HIRSCHMANN
A BELDEN BRAND

User Manual

Basic Configuration
Industrial ETHERNET (Gigabit-)Switch
PowerMICE, MACH 104, MACH 1040, MACH 4000

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

© 2015 Hirschmann Automation and Control GmbH

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

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

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

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

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

Rel. 9.0 - 02/2015 – 22.01.2015

Contents

Safety Information 9

About this Manual 11

Key 13

Introduction 15

1 Access to the user interfaces 17

1.1 System Monitor 18

1.2 Command Line Interface 21

1.3 Graphical User Interface 24

2 Entering the IP Parameters 27

2.1 IP Parameter Basics 29
2.1.1 IP Address (Version 4) 29
2.1.2 Netmask 30
2.1.3 Classless Inter-Domain Routing 34

2.2 Entering IP parameters via CLI 36

2.3 Entering the IP Parameters via HiDiscovery 39

2.4 Loading the system configuration from the ACA 41

2.5 System configuration via BOOTP 43

2.6 System Configuration via DHCP 48

2.7 System Configuration via DHCP Option 82 51

2.8 Graphical User Interface IP Configuration 52

2.9 Faulty Device Replacement 55

3 Loading/saving settings 57

3.1 Loading settings 58
3.1.1 Loading from the local non-volatile memory 59
3.1.2 Loading from a file 60
3.1.3 Resetting the configuration to the default settings 62

3.1.4 Loading from the AutoConfiguration Adapter 63
3.1.5 Using the offline configurator 64
3.2 Saving settings 67
3.2.1 Saving locally (and on the ACA) 67
3.2.2 Saving in a binary file or a script file on a URL 69
3.2.3 Saving to a binary file on the PC 70
3.2.4 Saving as a script on the PC 70
3.2.5 Saving as an offline configuration file on the PC 71
3.3 Configuration Signature 72

4 Loading Software Updates 73

4.1 Loading the Software manually from the ACA 75
4.1.1 Selecting the software to be loaded 76
4.1.2 Starting the software 77
4.1.3 Performing a cold start 78
4.2 Automatic software update by ACA 79
4.3 Loading the software from the TFTP server 81
4.4 Loading the Software via File Selection 83
4.5 Bootcode Update via TFTP 84
4.5.1 Updating the Bootcode file 84

5 Configuring the Ports 87

6 Assistance in the Protection from Unauthorized Access 93

6.1 Protecting the device 94
6.2 Password for SNMP access 95
6.2.1 Description of password for SNMP access 95
6.2.2 Entering the password for SNMP access 96
6.3 Telnet/internet/SSH access 100
6.3.1 Description of Telnet Access 100
6.3.2 Description of Web Access (http) 100
6.3.3 Description of SSH Access 101
6.3.4 Switching Telnet/Internet/SSH access on/off 102
6.3.5 Web access through HTTPS 103
6.4 Restricted Management Access 106
6.5 HiDiscovery Access 109
6.5.1 Description of the HiDiscovery Protocol 109
6.5.2 Enabling/disabling the HiDiscovery function 109

6.6 Port access control 110
6.6.1 Description of the port access control 110
6.6.2 Application Example for Port Access Control 111
6.7 Port Authentication IEEE 802.1X 113
6.7.1 Description of Port Authentication according to IEEE 802.1X 113
6.7.2 Authentication Process according to IEEE 802.1X 114
6.7.3 Preparing the Device for the IEEE 802.1X Port Authentication 114
6.7.4 IEEE 802.1X Settings 115
6.8 Access Control Lists (ACL) 116
6.8.1 Description of prioritizing with ACLs 117
6.8.2 Description of IP-based ACLs 118
6.8.3 Description of MAC-based ACLs 119
6.8.4 Configuring IP ACLs 121
6.8.5 Configuring MAC ACLs 123
6.8.6 Configuring Priorities with IP ACLs 123
6.8.7 Specifying the Sequence of the Rules 125
6.8.8 ACLs for Layer 4 fragments 126
6.9 Login Banner 128
6.10 CLI Banner 129

7 Synchronizing the System Time in the Network 131

7.1 Setting the time 132
7.2 SNTP 134
7.2.1 Description of SNTP 134
7.2.2 Preparing the SNTP Configuration 135
7.2.3 Configuring SNTP 136
7.3 Precision Time Protocol 139
7.3.1 Description of PTP Functions 139
7.3.2 Preparing the PTP Configuration 145
7.3.3 Application Example 147
7.4 Interaction of PTP and SNTP 152

8 Network Load Control 155

8.1 Direct Packet Distribution 156
8.1.1 Store and Forward 156
8.1.2 Multi-Address Capability 156
8.1.3 Aging of learned MAC addresses 157
8.1.4 Entering Static Addresses 158
8.1.5 Disabling the Direct Packet Distribution 159

8.2 Multicast Application 161
8.2.1 Description of the Multicast Application 161
8.2.2 Example of a Multicast Application 162
8.2.3 Description of IGMP Snooping 163
8.2.4 Setting IGMP Snooping 164
8.2.5 Description of GMRP 169
8.2.6 Setting GMRP 171

8.3 Rate Limiter 173
8.3.1 Description of the Rate Limiter 173
8.3.2 Rate limiter settings 174

8.4 QoS/Priority 175
8.4.1 Description of Prioritization 175
8.4.2 VLAN tagging 176
8.4.3 IP ToS / DiffServ 178
8.4.4 Management prioritization 181
8.4.5 Handling of Received Priority Information 181
8.4.6 Handling of traffic classes 182
8.4.7 Setting prioritization 184

8.5 Flow Control 191
8.5.1 Description of Flow Control 191
8.5.2 Setting the Flow Control 193

8.6 VLANs 194
8.6.1 VLAN Description 194
8.6.2 Examples of VLANs 195
8.6.3 Double VLAN Tagging 208

9 Operation Diagnosis 213

9.1 Sending Traps 214
9.1.1 List of SNMP traps 215
9.1.2 SNMP Traps when Booting 216
9.1.3 Configuring Traps 217

9.2 Monitoring the Device Status 219
9.2.1 Configuring the Device Status 220
9.2.2 Displaying the Device Status 221

9.3 Out-of-band Signaling 222
9.3.1 Controlling the Signal Contact 223
9.3.2 Monitoring the Device Status via the Signal Contact 224
9.3.3 Monitoring the Device Functions via the Signal Contact 224
9.3.4 Monitoring the Fan 225

9.4 Port Status Indication 228

9.5 Event Counter at Port Level 230
9.5.1 Detecting Non-matching Duplex Modes 231
9.5.2 TP Cable Diagnosis 233
9.5.3 Port Monitor 235
9.5.4 Auto Disable 238
9.6 Displaying the SFP Status 240
9.7 Topology Discovery 241
9.7.1 Description of Topology-Detection 241
9.7.2 Displaying the Topology Discovery Results 242
9.8 Detecting IP Address Conflicts 244
9.8.1 Description of IP Address Conflicts 244
9.8.2 Configuring ACD 245
9.8.3 Displaying ACD 245
9.9 Detecting Loops 246
9.10 Reports 247
9.11 Monitoring Data Traffic on the Ports (Port Mirroring) 249
9.12 Syslog 253
9.13 Trap log 256
9.14 MAC Notification 257

A Setting up the Configuration Environment 259

A.1 Setting up a DHCP/BOOTP Server 260
A.2 Setting up a DHCP Server with Option 82 266
A.3 TFTP Server for Software Updates 270
A.3.1 Setting up the TFTP Process 271
A.3.2 Software Access Rights 274
A.4 Preparing access via SSH 275
A.4.1 Generating a key 275
A.4.2 Loading a key onto the device 277
A.4.3 Access through an SSH 277
A.5 HTTPS Certificate 280
A.6 Service Shell 281

B General Information 283

B.1 Management Information Base (MIB) 284

B.2 Abbreviations used 287

B.3 Technical Data 288

B.4 Readers' Comments 289

C Index 291

D Further Support 295

Safety Information

⚠ WARNING

UNCONTROLLED MACHINE ACTIONS
To avoid uncontrolled machine actions caused by data loss, configure all the data transmission devices individually.
Before you start any machine which is controlled via data transmission, be sure to complete the configuration of all data transmission devices.

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

About this Manual

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

The following thematic sequence has proven itself in practice:

- Set up device access for operation by entering the IP parameters
- Check the status of the software and update it if necessary
- Load/store any existing configuration
- Configure the ports
- Set up protection from unauthorized access
- Optimize the data transmission with network load control
- Synchronize system time in the network
- Perform an operation diagnosis
- Store the newly created configuration in the non-volatile memory

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

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

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

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

The “GUI” reference manual contains detailed information on using the graphical interface to operate the individual functions of the device.

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

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

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

Maintenance

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

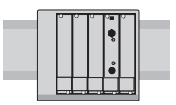
Key

The designations used in this manual have the following meanings:

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

Symbols used:

	WLAN access point
	Router with firewall
	Switch with firewall
	Router
	Switch

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

Introduction

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

Note: The changes you make in the dialogs are copied into the volatile memory of the device when you click on "Set".
To save the changes to the device into permanent memory, select the saving location in the `Basic Settings:Load/Save` dialog box and click on "Save".

1 Access to the user interfaces

The device has 3 user interfaces, which you can access via different interfaces:

- System monitor via the V.24 interface (out-of-band)
- Command Line Interface (CLI) via the V.24 connection (out-of-band) as well as Telnet or SSH (in-band)
- Graphical User Interface via Ethernet (in-band).

1.1 System Monitor

The system monitor enables you to

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

Starting the System Monitor

Prerequisites

- Terminal cable for connecting the device to your PC (available as an optional accessory).
- PC with VT100 terminal emulation (such as PuTTY) or serial terminal

Perform the following work steps:

☐ Use the terminal cable to connect the V.24 port of the device with the “COM” port of the PC.
☐ Start the VT100 terminal emulation on the PC.
☐ Define the following transmission parameters:
  – Speed: 9600 Baud
  – Data: 8 bit
  – Parity: None
  – Stopbit: 1 bit
  – Flow control: None

Speed	9600 Baud
Data	8 bit
Parity	None
Stopbit	1 bit
Handshake	Off

Table 1: Data transfer parameters

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

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

```
< Device Name  (Boot) Release: 1.00 Build: 2005-09-17 15:36 >

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

Figure 1: Screen display during the boot process

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

```
System Monitor

(Selected OS: L3P-06.0.00 (2010-09-09 09:09))

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




sysMon1>
```

Figure 2: System monitor 1 screen display

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

1.2 Command Line Interface

The Command Line Interface enables you to use the functions of the device via a local or remote connection.
The Command Line Interface provides IT specialists with a familiar environment for configuring IT devices.
The script compatibility of the Command Line Interface enables you, among other things, to feed multiple devices with the same configuration data, to create and use partial configurations, or to compare 2 configurations using 2 script files.

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

You can access the Command Line Interface via:

- the V.24 port (out-of-band)
- Telnet (in-band)
- SSH (in-band)

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

Opening the Command Line Interface

☐ Connect the device to a terminal or to a “COM” port of a PC using terminal emulation based on VT100, and press any key (see on page 18 “System Monitor”) or
call up the Command Line Interface via Telnet.
A window for entering the user name appears on the screen.
Up to 5 users can access the Command Line Interface.

```
        Copyright (c) 2004-2010 Hirschmann Automation and Control GmbH

                             All rights reserved

                          PowerMICE Release L3P-06.0.00

                          (Build date 2010-09-09 12:13)



                        System Name:   PowerMICE
                        Mgmt-IP     :  10.0.1.105
                        1.Router-IP:   0.0.0.0
                        Base-MAC    :  00:80:63:51:74:00
                        System Time:   2010-09-09 13:14:15


User:
```

Figure 3: Logging in to the Command Line Interface program

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

The start screen appears.

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


(Hirschmann Product) >
```

Figure 4: CLI screen after login

1.3 Graphical User Interface

The graphical user Interface (GUI) allows you to conveniently define and monitor the settings of the device from a computer on the network.

You reach the graphical user interface (GUI) with the following programs:
- HiView
- Web browser

System requirements

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

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

Starting the graphical user interface

The prerequisite for starting the graphical user interface, first configure the IP parameters of the device correctly.

Starting the graphical user interface in HiView:

☐ Start HiView.

☐ In the URL field of the start window, enter the IP address of your device.

☐ Click "Open".

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

Start the graphical user interface in the Web browser:

– This requires that Java is enabled in the security settings of your Web browser.

☐ Start your Web browser.

☐ Write the IP address of the device in the address field of the Web browser. Use the following form: `https://xxx.xxx.xxx.xxx`

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

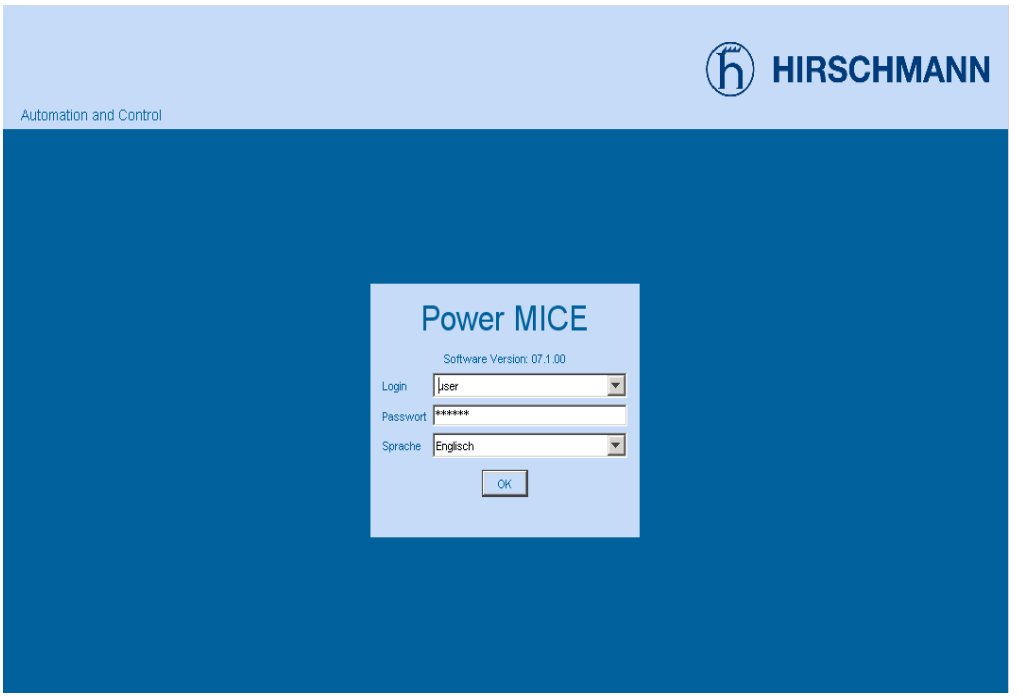


Figure 5: Login window

☐ Select the user name and enter the password.
  – Select the user name `user` to have read access to the device.
  – Select the user name `admin` to have read and write access to the device.

☐ Select the language in which you want to use the graphical user interface.

☐ Click "Ok".

The Web browser displays the graphical user interface.

2 Entering the IP Parameters

When you install the device for the first time enter the IP parameters.

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

- Entry using the Command Line Interface (CLI).
  You choose this “out of band” method if
  - you preconfigure your device outside its operating environment, or
  - you need to restore network access (“in-band”) to the device
- Entry using the HiDiscovery protocol.
  You choose this “in-band” method on a previously installed network device or if you have another Ethernet connection between your PC and the device
- Configuration using the AutoConfiguration Adapter (ACA).
  You choose this method if you are replacing a device with a device of the same type and have already saved the configuration on anACA.
- Using BOOTP.
  You choose this “in-band” method to configure the installed device using BOOTP. You need a BOOTP server for this method. The BOOTP server assigns the configuration data to the device using its MAC address. The DHCP mode is the default mode for the configuration data reference, set the parameter to the BOOTP mode for this method.
- Configuration via DHCP.
  You choose this “in-band” method to configure the installed device using DHCP. You need a DHCP server for this method. The DHCP server assigns the configuration data to the device using its MAC address or its system name.

- Configuration via DHCP Option 82.
  You choose this “in-band” method if you want to configure the installed device using DHCP Option 82. You need a DHCP server with Option 82 for this. The DHCP server assigns the configuration data to the device using its physical connection (see on page 51 “System Configuration via DHCP Option 82”).
- Configuration using the graphical user interface.
  If the device already has an IP address and is reachable via the network, then the graphical user interface provides you with another option for configuring the IP parameters.

2.1 IP Parameter Basics

2.1.1 IP Address (Version 4)

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

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

Class	Network address	Host address	Address range
A	1 byte	3 bytes	0.0.0.0 to 127.255.255.255
B	2 bytes	2 bytes	128.0.0.0 to 191.255.255.255
C	3 bytes	1 byte	192.0.0.0 to 223.255.255.255
D			224.0.0.0 to 239.255.255.255
E			240.0.0.0 to 255.255.255.255

Table 2: IP address classes

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

- APNIC (Asia Pacific Network Information Center) - Asia/Pacific Region
- ARIN (American Registry for Internet Numbers) - Americas and Sub-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

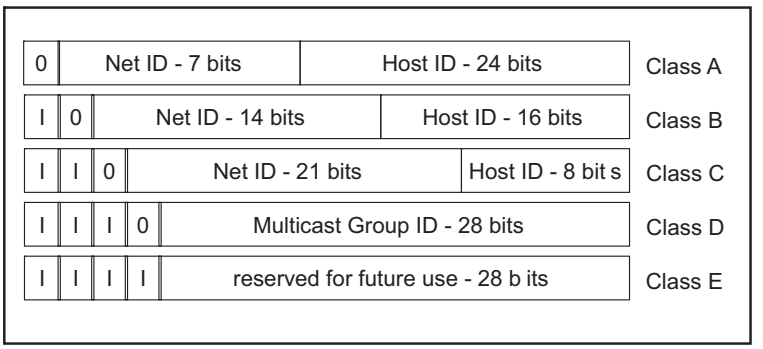


Figure 6: Bit representation of the IP address

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

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

2.1.2 Netmask

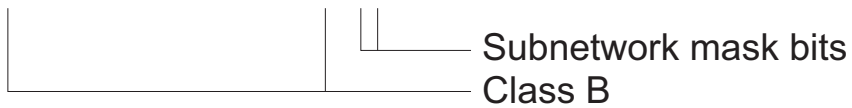
Routers and gateways subdivide large networks into subnetworks. The netmask assigns the IP addresses of the individual devices to a particular subnetwork.

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

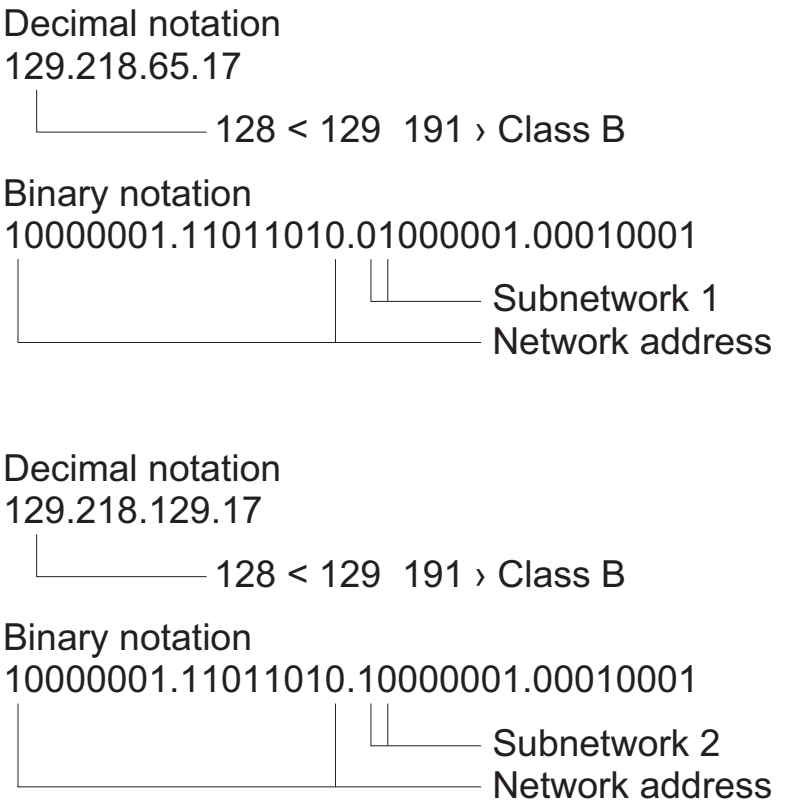
The bits of the host address (host id) that represent the mask are set to one. The remaining bits of the host address in the netmask are set to zero (see the following examples).
Example of a netmask:

Decimal notation
255.255.192.0

Binary notation
11111111.11111111.11000000.00000000



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


Decimal notation
129.218.65.17
128 < 129 191 › Class B
Binary notation
10000001.11011010.01000001.00010001
Subnetwork 1
Network address
Decimal notation
129.218.129.17
128 < 129 191 › Class B
Binary notation
10000001.11011010.10000001.00010001
Subnetwork 2
Network address

Example of how the network mask is used

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

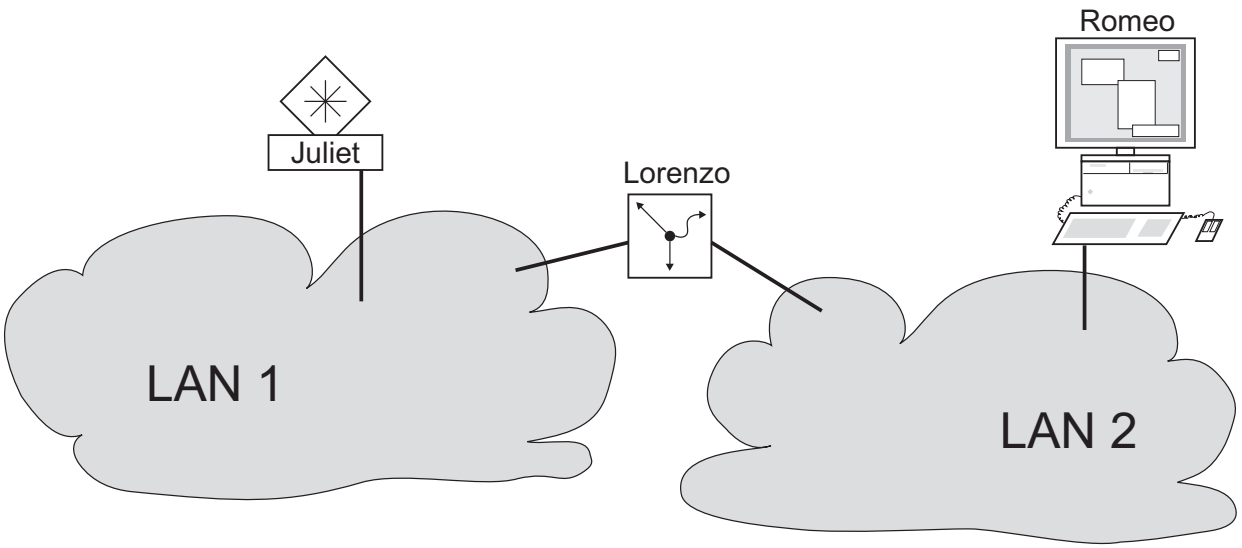


Figure 7: Management agent that is separated from its management station by a router

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

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

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

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

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

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

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

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

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

2.1.3 Classless Inter-Domain Routing

Class C with a maximum of 254 addresses was too small, and class B with a maximum of 65,534 addresses was too large for most users. This resulted in ineffective usage of the class B addresses available.
Class D contains reserved multicast addresses. Class E is reserved for experimental purposes. A gateway not participating in these experiments ignores datagrams with these destination addresses.

Since 1993, RFC 1519 has been using Classless Inter-Domain Routing (CIDR) to provide a solution. CIDR overcomes these class boundaries and supports classless address ranges.

With CIDR, you enter the number of bits that designate the IP address range. You represent the IP address range in binary form and count the mask bits that designate the netmask. The netmask indicates the number of bits that are identical to the network part for the IP addresses in a given address range. Example:

IP address, decimal	Network mask, decimal	IP address, binary
149.218.112.1	255.255.255.128	10010101 11011010 01110000 00000001
149.218.112.127		10010101 11011010 01110000 01111111

25 mask bits

CIDR notation: 149.218.112.0/25

Mask bits

The combination of a number of class C address ranges is known as “supernetting”. This enables you to subdivide class B address ranges to a very fine degree.

2.2 Entering IP parameters via CLI

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

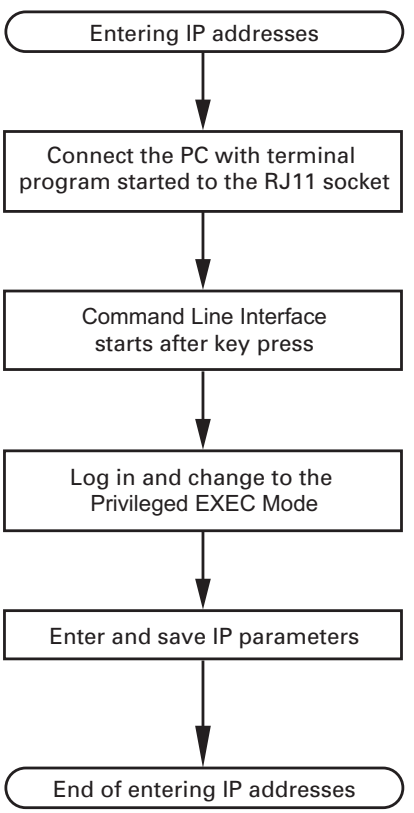


Figure 8: Flow chart for entering IP addresses

Note: If a terminal or PC with terminal emulation is unavailable in the vicinity of the installation location, you can configure the device at your own workstation, then take it to its final installation location.

☐ Set up a connection to the device (see on page 18 “Starting the System Monitor”).

The start screen appears.

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


(Hirschmann PowerMICE) >
```

☐ Deactivate DHCP.

☐ Enter the IP parameters.

- Local IP address
  On delivery, the device has the local IP address `0.0.0.0`.
- Netmask
  If you divided your network into subnetworks, and if these are identified with a netmask, then enter the netmask here.

The default setting of the netmask is `0.0.0.0`.

- IP address of the gateway.
  You require this entry when installing the device in a different subnetwork as the management station or TFTP server (see on page 33 “Example of how the network mask is used”).
  Enter the IP address of the gateway between the subnetwork with the device and the path to the management station.
  The default setting of the IP address is `0.0.0.0`.

☐ Save the configuration entered using
`copy system:running-config nvram:startup-config`.

`enable`	Switch to the privileged EXEC mode.
`network protocol none`	Deactivate DHCP.
`network parms 10.0.1.23 255.255.255.0`	Assign the device the IP address 10.0.1.23 and the netmask 255.255.255.0. You have the option of also assigning a gateway address.
`copy system:running-config nvram:startup-config`	Save the current configuration to the non-volatile memory.

After entering the IP parameters, you easily configure the device via the graphical user interface (see the “GUI” reference manual).

2.3 Entering the IP Parameters via HiDiscovery

The HiDiscovery protocol enables you to assign IP parameters to the device via the Ethernet.
You can easily configure other parameters via the graphical user interface (see the "GUI" Graphic User Interface reference manual).

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

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

☐ Start the HiDiscovery program.
When you start HiDiscovery, it automatically searches the network for those devices which support the HiDiscovery protocol.
HiDiscovery uses the first network interface found for the PC. If your computer has several network cards, you select the one you desire in the HiDiscovery toolbar.

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

HiDiscovery enables you to identify the devices displayed.
☐ Select a device line.
☐ Click the „Signal“ symbol on the tool bar to set the LEDs for the selected device to flashing on. To switch off the flashing, click on the symbol again.
☐ By double-clicking a line, you open a window in which you enter the device name and the IP parameters.

Note: When the IP address is entered, the device copies the local configuration settings (see on page 57 “Loading/saving settings”).

Note: For security reasons, switch off the HiDiscovery function for the device in the graphical user interface, after you have assigned the IP parameters to the device (see on page 52 “Graphical User Interface IP Configuration”).

Note: Save the settings so that you will still have the entries after a restart (see on page 57 “Loading/saving settings”).

2.4 Loading the system configuration from the ACA

The AutoConfiguration Adapter (ACA) is a device for

- for saving the device configuration data and
- saving the device software.

If a device becomes inoperative, the ACA allows you to transfer the configuration data to a replacement device of the same type.

When you start the device, it checks to see whether an ACA is present. If an ACA is present with a valid password and valid software, the device loads the configuration data from the ACA.

The password is valid if

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

To save the configuration data in the ACA, See 67 “Saving locally (and on the ACA)”.

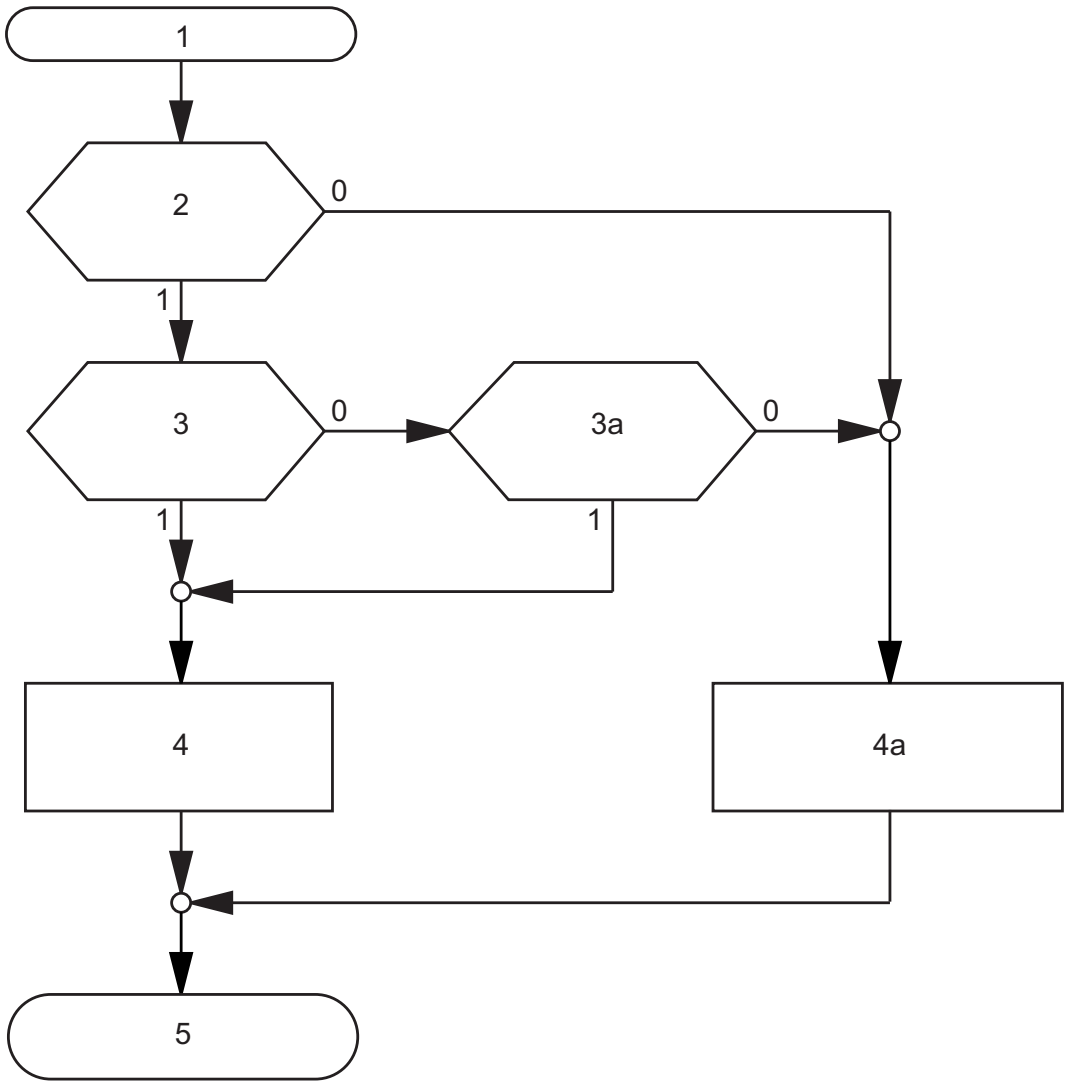


Figure 9: Flow chart of loading configuration data from the ACA
1 – Device start-up
2 – ACA plugged-in?
3 – Password in device and ACA identical?
3a – Default password in device?
4 – Load configuration from ACA,
ACA LEDs flashing synchronously
4a –Load configuration from local memory,
ACA LEDs flashing alternately
5 – Configuration data loaded

2.5 System configuration via BOOTP

When it is started up via BOOTP (bootstrap protocol), a device receives its configuration data in accordance with the “BOOTP process” flow chart (see figure 10).

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

☐ Activate BOOTP to receive the configuration data (see on page 52 “Graphical User Interface IP Configuration”), or see the CLI:

`enable`	Switch to the privileged EXEC mode.
`network protocol bootp`	Activate BOOTP.
`copy system:running-config 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=10.1.112.83:tc=.global:
switch_02:ht=ethernet:ha=008063086502:ip=10.1.112.84:tc=.global:
.
.
```

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

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

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

In the appendix, you will find an example for the configuration of a BOOTP/DHCP server.
See "Setting up a DHCP/BOOTP Server" on page 260.

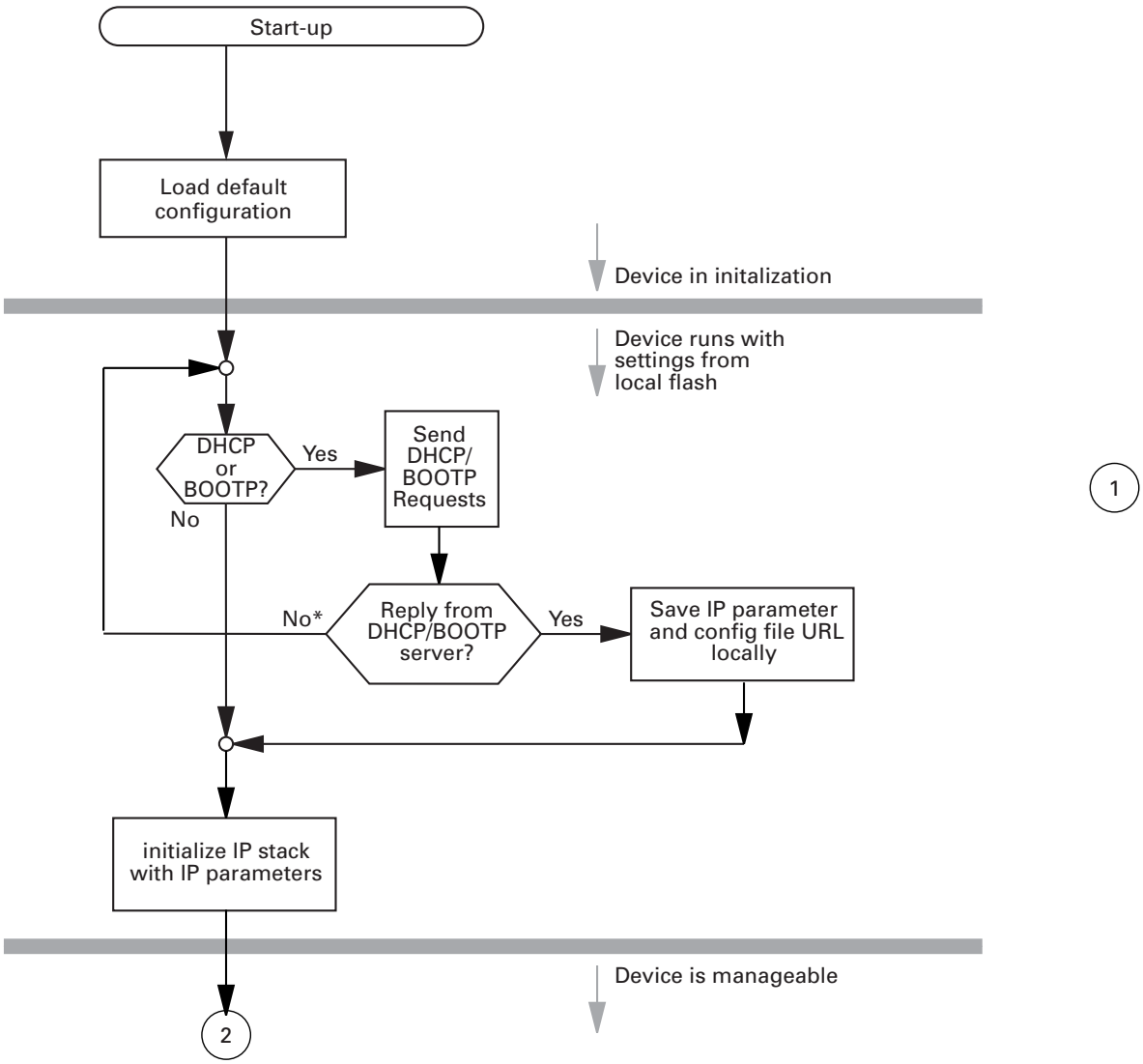


Figure 10: Flow chart for the BOOTP/DHCP process, part 1
** see note figure 11*

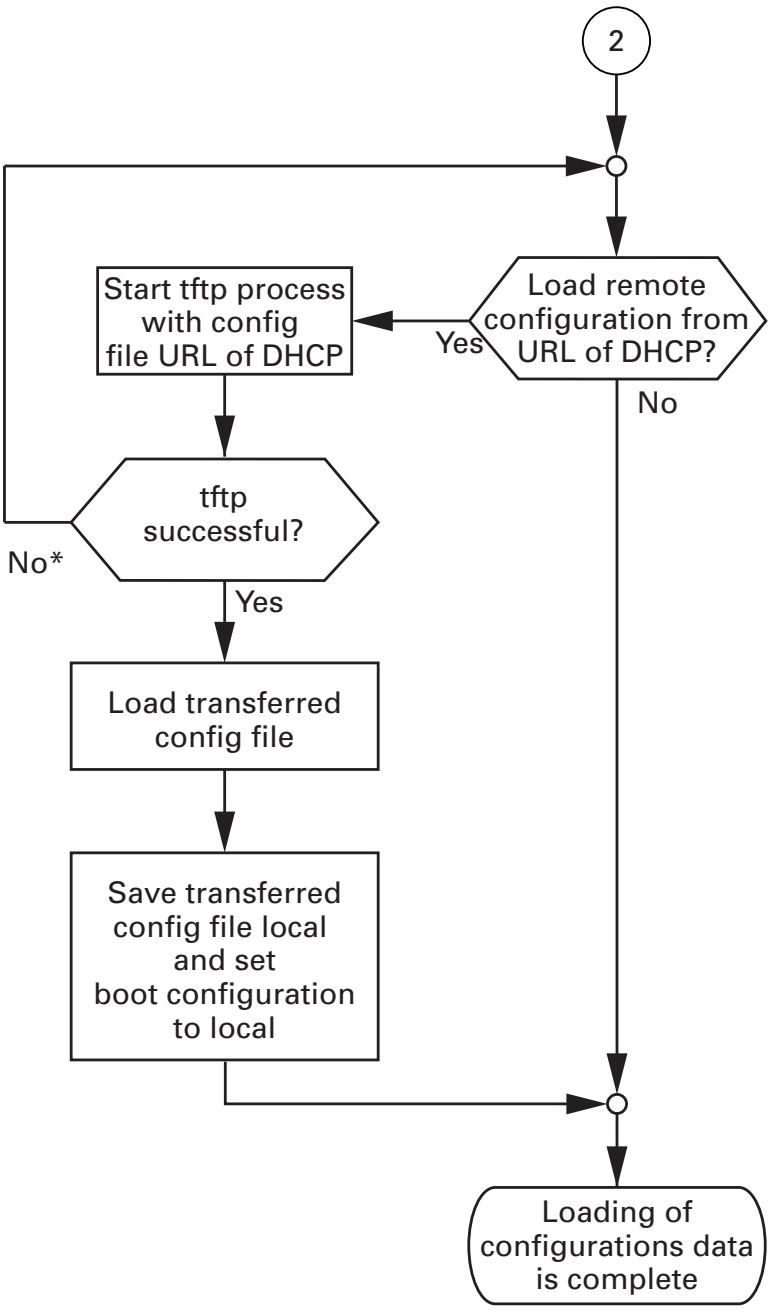


Figure 11: Flow chart for the BOOTP/DHCP process, part 2

Note: The loading process started by DHCP/BOOTP (see on page 43 “System configuration via BOOTP”) shows the selection of “from URL & save locally” in the “Load” frame. If you get an error message when saving a configuration, this could be due to an active loading process. DHCP/BOOTP only finishes a loading process when a valid configuration has been loaded. If DHCP/BOOTP does not find a valid configuration, then finish the loading process by loading the local configuration in the “Load” frame.

2.6 System Configuration via DHCP

The DHCP (Dynamic Host Configuration Protocol) is a further development of BOOTP, which it has replaced. The DHCP additionally allows the configuration of a DHCP client via a name instead of via the MAC address. For the DHCP, this name is known as the “client identifier” in accordance with RFC 2131.
The device uses the name entered under sysName in the system group of the MIB II as the client identifier. You can enter this system name directly via SNMP, the Web-based management (see system dialog), or the Command Line Interface.

During startup operation, a device receives its configuration data according to the “DHCP process” flowchart (see figure 10).

The device sends its system name to the DHCP server. The DHCP server can then use the system name to allocate an IP address as an alternative to the MAC address.

In addition to the IP address, the DHCP server sends

- the netmask
- the default gateway (if available)
- the tftp URL of the configuration file (if available)

The device accepts this data as configuration parameters (see on page 52 “Graphical User Interface IP Configuration”). If an IP address was assigned by a DHCP server, it will be permanently saved locally.

Option	Meaning
1	Subnet Mask
2	Time Offset
3	Router
4	Time server

Table 3: DHCP options which the device requests

Option	Meaning
12	Host Name
42	NTP server
61	Client Identifier
66	TFTP Server Name
67	Bootfile Name

Table 3: DHCP options which the device requests

The advantage of using DHCP instead of BOOTP is that the DHCP server can restrict the validity of the configuration parameters (“Lease”) to a specific time period (known as dynamic address allocation). Before this period (“Lease Duration”) elapses, the DHCP client can attempt to renew this lease. Alternatively, the client can negotiate a new lease. The DHCP server then allocates a random free address.
To help avoid this, DHCP servers provide the explicit configuration option of assigning a specific client the same IP address based on a unique hardware ID (known as static address allocation).

On delivery, DHCP is activated. As long as DHCP is activated, the device attempts to obtain an IP address. If it cannot find a DHCP server after restarting, it will not have an IP address. Activate or deactivate DHCP in the `Basic Settings:Network:Global` dialog.

Note: When using Industrial HiVision network management, the user checks to see that DHCP allocates the original IP address to each device every time.

The appendix contains an example configuration of the BOOTP/DHCP-server .(see on page 260 “Setting up a DHCP/BOOTP Server”)

Example of a DHCP-configuration file:

```
# /etc/dhcpd.conf for DHCP Daemon
#
subnet 10.1.112.0 netmask 255.255.240.0 {
option subnet-mask 255.255.240.0;
option routers 10.1.112.96;
```

```
}
#
# Host berta requests IP configuration
# with her MAC address
#
host berta {
hardware ethernet 00:80:63:08:65:42;
fixed-address 10.1.112.82;
}
#
# Host hugo requests IP configuration
# with his client identifier.
#
host hugo {
#
option dhcp-client-identifier "hugo";
option dhcp-client-identifier 00:68:75:67:6f;
fixed-address 10.1.112.83;
server-name "10.1.112.11";
filename "/agent/config.dat";
}
```

Lines that begin with the #-character contain comments.
The lines that precede the individual devices indicate settings that apply to the following device.
The fixed-address line assigns a fixed IP address to the device.
Please refer to your DHCP-Server manual for more details.

2.7 System Configuration via DHCP Option 82

As with the classic DHCP, on startup an agent receives its configuration data according to the “BOOTP/DHCP process” flow chart (see figure 10).

While the system configuration is based on the classic DHCP protocol on the device being configured (see on page 48 “System Configuration via DHCP”), Option 82 is based on the network topology. This procedure gives you the option of assigning the same IP address to any device which is connected to a particular location (port of a device) on the LAN.
The installation of a DHCP server is described in the chapter “Setting up a DHCP Server with Option 82” on page 266.

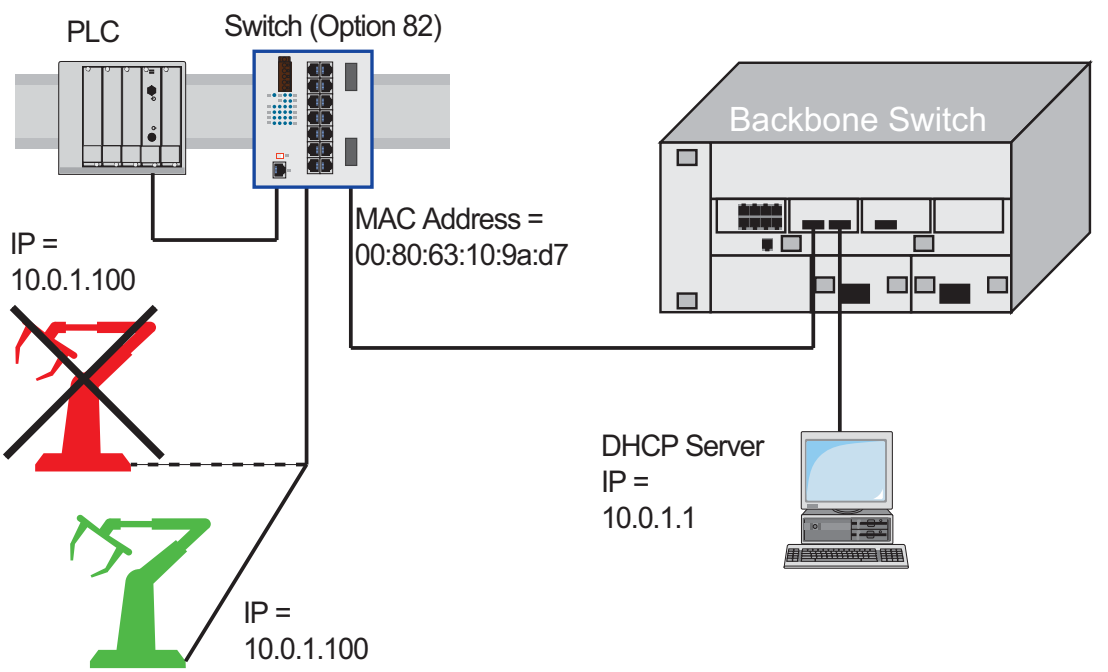


Figure 12: Application example of using Option 82

2.8 Graphical User Interface IP Configuration

Use the `Basic Settings:Network` dialog to define the source from which the device receives its IP parameters after startup, assign the IP parameters and VLAN ID, and configure the HiDiscovery access.

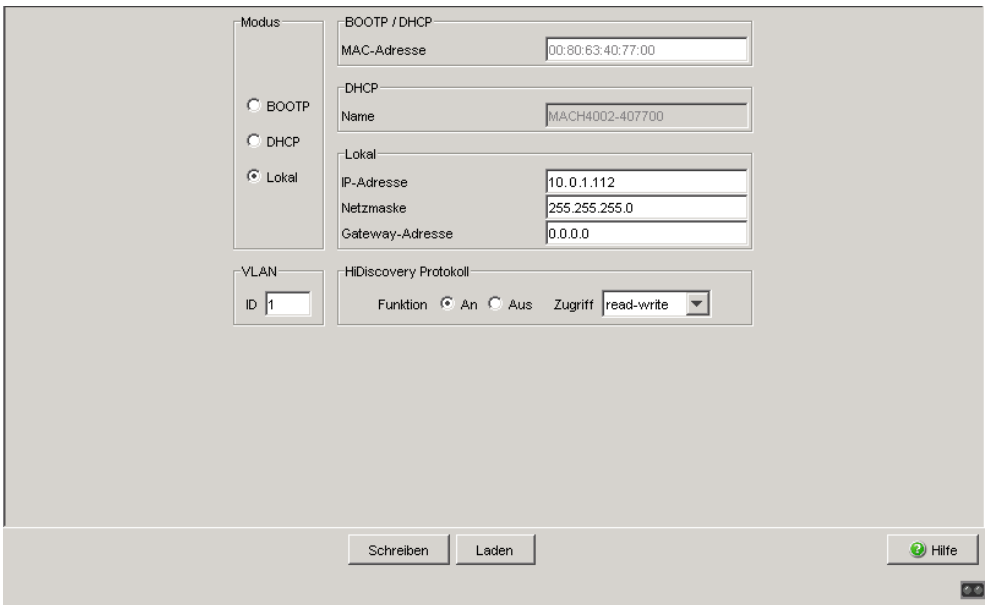


Figure 13: Network parameters dialog

☐ Under “Mode”, you enter where the device gets its IP parameters:
- ▶ In the BOOTP mode, the configuration is via a BOOTP or DHCP server on the basis of the MAC address of the device.
  See “Setting up a DHCP/BOOTP Server” on page 260.
- ▶ In the DHCP mode, the configuration is via a DHCP server on the basis of the MAC address or the name of the device.
  See “Setting up a DHCP Server with Option 82” on page 266.
- ▶ In the “local” mode the net parameters in the device memory are used.

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

☐ You enter the name applicable to the DHCP protocol in the “Name” line in the `Basic Settings:System` dialog of the graphical user interface.

☐ The “VLAN” frame enables you to assign a VLAN to the management CPU of the device. If you enter 0 here as the VLAN ID (not included in the VLAN standard version), the management CPU will then be accessible from all VLANs.

☐ The HiDiscovery protocol allows you to allocate an IP address to the device. Activate the HiDiscovery protocol if you want to allocate an IP address to the device from your PC with the enclosed HiDiscovery software (default setting: "Operation" `On`, "Access" `read-write`).

Note: Save the settings so that you will still have the entries after a restart (see on page 57 “Loading/saving settings”).

2.9 Faulty Device Replacement

The device provides 2 plug-and-play solutions for replacing a faulty device with a device of the same type (faulty device replacement):

- Configuring the new device using an AutoConfiguration Adapter (see on page 41 “Loading the system configuration from the ACA”) or
- configuration via DHCP Option 82 (see on page 266 “Setting up a DHCP Server with Option 82”)

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

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

Note: If you want to access the device via SSH, you also need an SSH key. To transfer the SSH key of the old device to the new one, you have the following options:

- If you have already created the key and saved it outside the device (e.g. on your administration workstation), load the saved key onto the new device (see on page 277 “Loading a key onto the device”).

- Otherwise create a new SSH key and load it onto the new device (see on page 275 “Preparing access via SSH”). Note that the new device now identifies itself by means of another key.

3 Loading/saving settings

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

- Load settings from a non-volatile memory into the temporary memory
- Save settings from the temporary memory in a non-volatile memory

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

3.1 Loading settings

When it is restarted, the device loads its configuration data from the local non-volatile memory. The prerequisites for this are:

- You have not connected an AutoConfiguration Adapter (ACA) and
- the IP configuration is “local”.

During a restart, the device also allows you to load settings from the following sources:

- a binary file of the AutoConfiguration Adapter. If an ACA is connected to the device, the device automatically loads its configuration from the ACA during the boot procedure.
- from a script file of the AutoConfiguration Adapter. If an ACA is connected to the device, the device automatically loads its configuration from the script file of the ACA during the boot procedure (see on page 63 “Loading a script from the ACA”).

Note: Details of times required for a reboot:

- The time required for a cold start is the time taken by the device from the moment power is switched on until it is fully connected and its Management-CPU is fully accessible.
- Depending on the device type and the extent of the configuration settings, a cold start takes at least about 10 seconds.
- Extensive configuration settings will increase the time required for a reboot, especially if they contain a high number of VLANs. In extreme cases, a reboot can take up to about 200 seconds.
- A warm start is quicker, since in this case the device skips the software loading from NVRAM.

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

- the local non-volatile memory
- a file in the connected network (setting on delivery)
- a binary file or an editable and readable script on the PC and
- the firmware (restoration of the configuration on delivery).

Note: When loading a configuration, hold off any accesses to the device until it has loaded the configuration file and applied the new configuration settings. Depending on the device type and the extent of the configuration settings, this process can take between 10 and 200 seconds.

3.1.1 Loading from the local non-volatile memory

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

☐ Select the `Basics: Load/Save` dialog.
☐ In the “Load” frame, click “from Device”.
☐ Click “Restore”.

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

Switch to the privileged EXEC mode.
The device loads the configuration data from the local non-volatile memory.

3.1.2 Loading from a file

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

☐ Select the `Basics: Load/Save` dialog.
☐ In the “Load” frame, click
- “from URL” if you want the device to load the configuration data from a file and retain the locally saved configuration.
- “from URL & save to Switch” if you want the device to load the configuration data from a file and save this configuration locally.
- “via PC” if you want the device to load the configuration data from a file on the PC and retain the locally saved configuration.

☐ In the “URL” frame, enter the path under which the device will find the configuration file, if you want to load from the URL.
☐ Click “Restore”.

Note: When restoring a configuration using one of the options in the “Load” frame, note the following particulars:
- The device can restore the configuration from a binary or script file:
  - The option “from Device” restores the configuration exclusively from the device-internal binary file.
  - The 3 options “from URL”, “from URL and save to Device” or “via PC” can restore the configuration both from a binary file and from a script file. The script file can be an offline configuration file (*.ocf) or a CLI script file (*.cli). The device determines the file type automatically.
- When restoring the configuration from a script file, you first delete the device configuration so that the default settings are overwritten correctly. For further information (see on page 62 “Resetting the configuration to the default settings”)

The URL identifies the path to the tftp server from which the device loads the configuration file. The URL is in the format tftp://IP address of the tftp server/path name/file name (e.g. `tftp://10.1.112.5/switch/config.dat`).

Example of loading from a tftp server

☐ Before downloading a file from the tftp server, you have to save the configuration file in the corresponding path of the tftp servers with the file name, e.g. `switch/switch_01.cfg` (see on page 69 “Saving in a binary file or a script file on a URL”).

☐ In the “URL” line, enter the path of the tftp server, e.g. `tftp://10.1.112.214/switch/switch_01.cfg`.

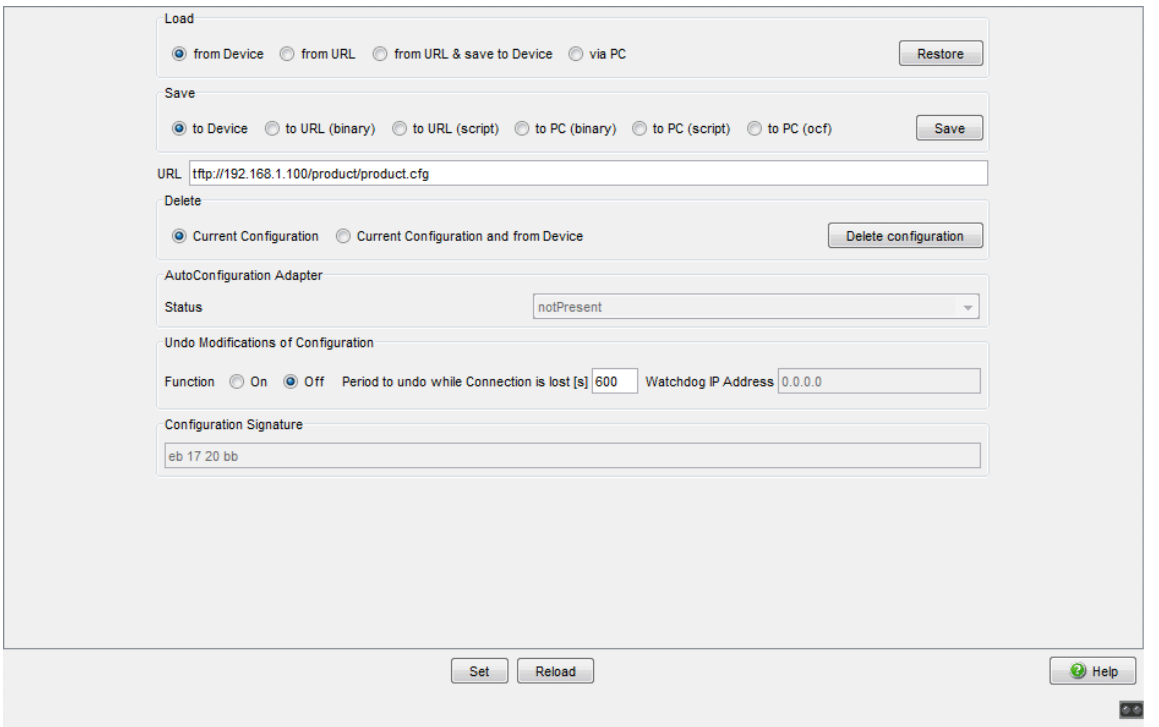


Figure 14: Load/Save dialog

```
enable
copy
tftp://10.1.112.159/switch/c
onfig.dat
  nvram:startup-config
```

Switch to the privileged EXEC mode.

The device loads the configuration data from a tftp server in the connected network.

Note: The loading process started by DHCP/BOOTP (see on page 43 “System configuration via BOOTP”) shows the selection of “from URL & save locally” in the “Load” frame. If you get an error message when saving a configuration, this could be due to an active loading process. DHCP/BOOTP only finishes a loading process when a valid configuration has been loaded. If DHCP/BOOTP does not find a valid configuration, then finish the loading process by loading the local configuration in the “Load” frame.

3.1.3 Resetting the configuration to the default settings

The device enables you to

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

☐ Select the `Basics: Load/Save` dialog.
☐ Make your selection in the "Delete" frame.
☐ Click "Delete configuration". The device will delete its configuration immediately.

Resetting the device using the system monitor

☐ Select `5` “Erase main configuration file”
This menu item allows you to reset the current configuration, stored in non volatile memory, to its default setting. The device also stores a backup configuration, and a configuration associated with the firmware, in its Flash memory.
☐ Press the Enter key to delete the configuration file.

3.1.4 Loading from the AutoConfiguration Adapter

Loading a configuration during the boot procedure

If you connect an ACA to the device and if the passwords on the device are in the default setting, missing, or the same as those on the ACA, the device automatically loads its configuration from the ACA during the boot procedure. After booting, the device updates its configuration in the local non-volatile memory with the configuration from the ACA.

Note: During the boot procedure, the configuration on the ACA has priority over the configuration in the local non-volatile memory.

The chapter “Saving locally (and on the ACA)” on page 67 describes how you can save a configuration file on an ACA.

Loading a script from the ACA

If the ACA contains a script file, the device automatically loads its configuration from the script file on the ACA during the boot procedure. The prerequisites for this are:

- The ACA is connected during the boot procedure.
- There is no binary configuration in the main directory of the ACA.
- The main directory of the ACA contains a file with the name “autoupdate.txt”.
- The file “autoupdate.txt” is a text file and contains a line whose content has the format `script=<file_name>`. Here `<file_name>` stands for the name of the script file to be loaded, e.g. `custom.cli`.
- The file specified using `script=<file_name>`, e.g. `custom.cli`, is located in the main directory of the ACA and is a valid script file.

If the local non-volatile memory of the device contains a configuration, the device ignores this.
After applying the script, the device updates the configuration in the local non-volatile memory with the configuration from the script.
In the process, it also writes the current binary configuration to the ACA.

Note: During the boot procedure, a binary configuration on the ACA has priority over a script on the ACA.

The chapter “Saving locally (and on the ACA)” describes how you can save a script file on an ACA.

- **Reporting configuration differences**
  The device allows you to trigger the following events when the configuration stored on the ACA does not match the configuration on the device:
  - send a trap (see on page 217 “Configuring Traps”),
  - update the device status (see on page 220 “Configuring the Device Status”),
  - update the status of the signal contacts (see on page 223 “Controlling the Signal Contact”).

3.1.5 Using the offline configurator

The offline configurator allows you to create configurations for devices in advance. You create the configuration virtually on your PC and load it onto your device in a 2nd step.

In this way you can prepare and manage the device configuration efficiently, thus saving time and effort both when creating the configuration and loading it to the devices.

For more details on using the offline configurator, see the chapter “Loading a configuration from the offline configurator” in the “GUI” Reference Manual.

Example of using the offline configurator

An IT employee already creates the configuration files for the devices of a production cell during the planning phase. In doing so, he uses existing configuration files for a similar production cell and modifies these.
He makes the offline configuration files available to the field service employee, who mounts the devices on site and then loads the configuration to the devices. All that is required for this is for the devices to be reachable and have received an IP address, e.g. via HiDiscovery.

Data format

The offline configurator reads and writes configuration data in an XML-based format. The file name extension of these files is ".ocf" (Offline Configurator Format).

You can use the graphical user interface of the devices to load these files and thus configure your devices very quickly.

The XML format also allows you to use other tools to create, edit and manage the offline configuration files and thus optimize your administration processes.

Installation and operating requirements

A requirement for the installation is a PC with a Windows™ XP operating system (with Service Pack 3) or higher.
You install the offline configurator from the product CD included with the device. To do so, start the "Setup.exe" installation file from the "ocf_setup" folder.

The offline configurator - like the graphical user interface - uses Java software 6 ("Java™ Runtime Environment (JRE) Version 1.6.x").
Install the software from www.java.com.

Using the offline configurator

Start the offline configurator by double-clicking the "Offline Management" desktop symbol.

For more details on using the offline configurator, see the chapter “Loading a configuration from the offline configurator” in the “GUI” Reference Manual.

3.2 Saving settings

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

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

3.2.1 Saving locally (and on the ACA)

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

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

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

Switch to the privileged EXEC mode.

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

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

Note: The device allows you to trigger the following events when the configuration stored on the ACA does not match the configuration on the device:

- send a trap (see on page 217 “Configuring Traps”),
- update the device status (see on page 220 “Configuring the Device Status”),
- update the status of the signal contacts (see on page 223 “Controlling the Signal Contact”).

Skip ACA21 during the boot phase

The device allows you to skip the ACA21 AutoConfiguration Adapter (if connected) during the boot phase. In this case, the device ignores the ACA21 during the boot phase. This shortens the boot phase of the device by 1 to 4 seconds. If you have enabled this function, ACA21-functionality becomes available as usual after the boot phase. The device simply skips the ACA21-loading procedures during the boot phase.

`enable`	Switch to Privileged EXEC mode..
`configure`	Switch to Global Configure mode.
`#boot skip-aca-on-boot enable`	Skip ACA during the boot phase. (default setting: disabled).
`#boot skip-aca-on-boot disable`	Include the ACA during the boot phase.
`#show boot skip-aca-on-boot`	Show whether the "Skip ACA during boot phase"function is enabled.

3.2.2 Saving in a binary file or a script file on a URL

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

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

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

The URL identifies the path to the tftp server on which the device saves the configuration file. The URL is in the format tftp://IP address of the tftp server/path name/file name (e.g. `tftp://10.1.112.5/switch/config.dat`).

☐ Click "Save".

`enable`	Switch to the privileged EXEC mode.
`copy nvram:startup-config tftp://10.1.112.159/ 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.

Note: If you save the configuration in a binary file, the device saves all configuration settings in a binary file.
In contrast to this, the device only saves those configuration settings that deviate from the default setting when saving to a script file.

When loading script files, these are only intended for overwriting the default setting of the configuration.

3.2.3 Saving to a binary file on the PC

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

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

3.2.4 Saving as a script on the PC

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

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

3.2.5 Saving as an offline configuration file on the PC

The device allows you to save the current configuration data for the offline configurator in XML form in a file on your PC.

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

3.3 Configuration Signature

The device assigns a checksum or signature to identify a configuration so that changes to that configuration are visible. Every time you save a configuration, the device generates a random sequence of numbers and/or letters for the configuration signature. This signature changes every time you change the configuration. Each configuration has a unique identifier.

The device stores the random generated signature with the configuration to verify that the device maintained the configuration after a reboot.

The signature consists of a configuration file checksum and a random number. The device checks the signature to verify that it is different from previous generated numbers.

4 Loading Software Updates

Hirschmann is working constantly to improve the performance of their procucts. Therefore, on the Hirschmann web page (www.hirschmann.com) you may find a newer release of the device software than the one installed on your device.

Checking the installed Software Release

☐ Open the `Basic Settings:Software` dialog.
☐ This dialog indicates the Release Number of the software installed in the device.

```
enable                                  Switch to Privileged EXEC mode.
show sysinfo                            Show system information.

Alarm..................................... None

System Description........................ Hirschmann Railswitch
System Name............................... RS-1F1054
System Location........................... Hirschmann Railswitch
System Contact............................ Hirschmann Automation
  and Control GmbH
System Up Time............................ 0 days 0 hrs 45 mins
  57 secs
System Date and Time (local time zone)..... 2009-11-12 14:15:16
System IP Address......................... 10.0.1.13
Boot Software Release..................... L2B-05.2.00
Boot Software Build Date.................. 2009-11-12 13:14
OS Software Release....................... L2B-03.1.00
OS Software Build Date.................... 2009-11-12 13:14
Hardware Revision......................... 1.22 / 4 / 0103
Hardware Description...................... RS20-1600T1T1SDAEHH
Serial Number............................. 943434023000001191
Base MAC Address.......................... 00:80:63:1F:10:54
Number of MAC Addresses................... 32 (0x20)
```

Loading the software

The device gives you 4 options for loading the software:

- manually from the ACA (out-of-band),
- automatically from the ACA (out-of-band),
- via TFTP from a tftp server (in-band) and
- via a file selection dialog from your PC.

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

4.1 Loading the Software manually from the ACA

You can connect the AutoConfiguration Adapter (ACA) to a USB port of your PC like a conventional USB stick and copy the device software into the main directory of the ACA.

☐ Copy the device software from your computer to the ACA.

☐ Now connect the ACA to the device‘s USB port.

☐ Open the system monitor (see on page 18 “Starting the System Monitor”).

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

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

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

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

4.1.1 Selecting the software to be loaded

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

```
Select Operating System Image

(Available OS: Selected: 05.0.00 (2009-08-07 06:05), Backup: 04.2.00
 (2009-07-06 06:05 (Locally selected: 05.0.00 (2009-08-07 06:05))

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

Figure 15: Update operating system screen display

Swap OS images
The memory of the device provides space for two images of the software. This allows you, for example, to load a new version of the software without deleting the existing version.
☐ Select 1 to load the other software in the next booting process.

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

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

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

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

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

4.1.2 Starting the software

This menu item (Start Selected Operating System) of the system monitor

allows you to start the software selected.

4.1.3 Performing a cold start

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

4.2 Automatic software update by ACA

☐ For a software update via the ACA, first copy the new device software into the main directory of the AutoConfiguration Adapter. If the version of the software on the ACA is newer or older than the version on the device, the device performs a software update.

Note: Software versions with release 06.0.00 and higher in the non-volatile memory of the device support the software update via the ACA. If the device software is older, you have the option of loading the software manually from the ACA. See “Loading the Software manually from the ACA” on page 75.

☐ Give the file the name that matches the device type and the software variant, e.g. rsL2P.bin for device type RS2 with the software variant L2P. Please note the case-sensitivity here.
If you have copied the software from a product CD or from a Web server of the manufacturer, the software already has the correct file name.

☐ Also create an empty file with the name “autoupdate.txt” in the main directory of the ACA. Please note the case-sensitivity here.

☐ Connect the AutoConfiguration Adapter to the device and restart the device.

☐ The device automatically performs the following steps:
- During the booting process, it checks whether an ACA is connected.
- It checks whether the ACA has a file with the name “autoupdate.txt” in the main directory.
- It checks whether the ACA has a software file with a name that matches the device type in the main directory.
- If compares the software version stored on the ACA with the one stored on the device.
- If these conditions are fulfilled, the device loads the software from the ACA to its non-volatile memory as the main software.
- The device keeps a backup of the existing software in the non-volatile memory.
- The device then performs a cold start, during which it loads the new software from the non-volatile memory.

One of the following messages in the log file indicates the result of the update process:

- S_watson_AUTOMATIC_SWUPDATE_SUCCESSFUL: Update completed successfully.
- S_watson_AUTOMATIC_SWUPDATE_FAILED_WRONG_FILE: Update failed. Reason: incorrect file.
- S_watson_AUTOMATIC_SWUPDATE_FAILED_SAVING_FILE: Update failed. Reason: error when saving.

☐ In your browser, click on “Reload” so that you can use the graphical user interface to access the device again after it is booted.

4.3 Loading the software from the TFTP server

For a software update via TFTP, you need a TFTP server on which the software to be loaded is stored (see on page 270 “TFTP Server for Software Updates”).

☐ Select the `Basics:Software` dialog.

The URL identifies the path to the software stored on the tftp server. The URL is in the format
tftp://IP address of the tftp server/path name/file name
(e.g. `tftp://192.168.1.1/device/device.bin`).

☐ Enter the path of the device software.

☐ Click on “tftp Update” to load the software from the tftp server to the device.

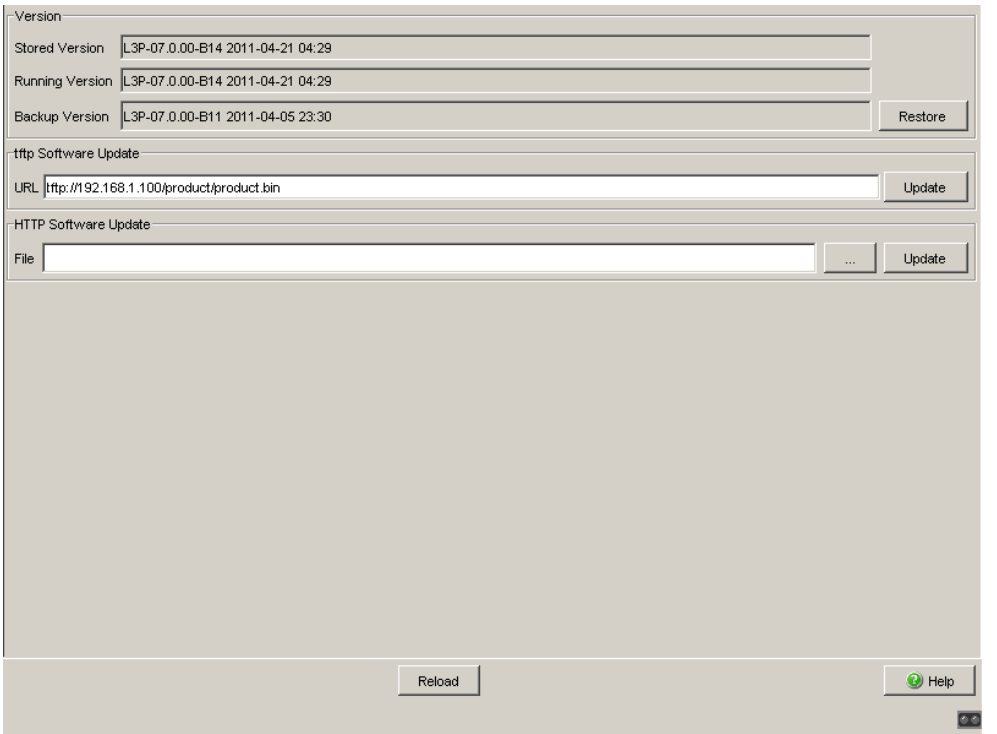


Figure 16: Software update dialog

☐ After successfully loading it, you activate the new software:
Select the dialog `Basic Settings:Restart` and perform a cold start.
In a cold start, the device reloads the software from the permanent memory, restarts, and performs a self-test.

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

`enable`	Switch to the privileged EXEC mode.
`copy tftp://10.0.1.159/product.bin system:image`	Transfer the “product.bin” software file to the device from the tftp server with the IP address 10.0.1.159.

4.4 Loading the Software via File Selection

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

- ☐ Select the `Basics:Software` dialog.
- ☐ In the file selection frame, click on “...”.
- ☐ In the file selection window, select the device software (name type: *.bin, e.g. device.bin) and click on “Open”.
- ☐ Click on “Update” to transfer the software to the device.

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

- ▶ Update finished.
- ▶ Update aborted. Reason: incorrect file.
- ▶ Update aborted. Reason: saving unsuccessful.
- ▶ File not found (reason: file name not found or does not exist).
- ▶ Unsuccessful Connection (reason: path without file name).

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

4.5 Bootcode Update via TFTP

In very rare cases, a bootcode with an expanded functionality is required to perform a software update. In such a case the service desk requests that you update the bootcode before performing the software update.

4.5.1 Updating the Bootcode file

For a tftp update, you need a tftp server to store the bootcode.
The URL identifies the path to the bootcode stored on the tftp server. The URL is in the format
tftp://IP address of the tftp server/path name/file name
(for example:).`tftp://192.168.1.1/device/device_bootrom.img`

- ☐ Open the `Basic Settings:Software` dialog.
- ☐ In the "tftp Software Update" frame, click the "Bootcode" radio button.
- ☐ Enter the path to the bootcode bin file in the "URL" text box.
- ☐ To start the update, click "Update".
- ☐ To start the new bootcode after loading, open the `Basic Settings:Restart` dialog and click "Cold start...".

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

`enable`	Change to the privileged EXEC mode.

`configure`	Change to the Configuration mode.
`copy <url> system:bootcode`	Copy the bootcode bin file from the tftp server to the device.

5 Configuring the Ports

The port configuration consists of:

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

Switching the port on and off

In the default setting, every port is switched on. For a higher level of access security, switch off the ports for which you are not making any connection.

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

Selecting the operating mode

In the default setting, the ports are set to "Automatic Configuration" operating mode.

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

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

Disable unused module slots

This function is available for the MS, PowerMICE, MACH102 and MACH4000 devices.

When you plug a module in an empty slot on modular devices, the device configures the module with the default settings. The default settings allow access to the network. To help prevent network access, the feature adds the possibility to disable an unused slot.

- ☐ Open the `Basics:Modules` dialog.
- ☐ Deactivate the unused slots in the "Enabled" column.

Displaying detected loss of connection

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

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

Power over Ethernet konfigurieren

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

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

Nominal power for MACH 4000:
The device provides the nominal power for the sum of all PoE ports plus a surplus. Should the connected devices require more PoE power than is provided, the device then switches PoE off at the ports. Initially, the device switches PoE off at the ports with the lowest PoE priority. If multiple ports have the same priority, the device first switches PoE off at the ports with the higher port number.

☐ **Global settings**
- For devices with **PoE** select the `Basic Settings:Power over Ethernet` dialog.
- For devices with **PoE** select the `Basic Settings:Power over Ethernet Plus:Global` dialog.

Frame "Operation":

☐ With “Function On/Off” you turn the PoE on or off.

Frame "Configuration":

☐ With “Send Trap” you can get the device to send a trap in the following cases:
- If a value exceeds/falls below the performance threshold.
- If the PoE supply voltage is switched on/off on at least one port.

☐ Enter the power threshold in “Threshold”. When the device exceeds or is below this value, the device will send a trap, provided that you enable the “Send Trap” function. For the power threshold you enter the power yielded as a percentage of the nominal power.

☐ “Budget [W]” displays the power that the device nominally provides to the PoE ports.

☐ “Reserved [W]” displays the maximum power that the device provides to the connected PoE devices on the basis of their classification.

☐ “Delivered [W]” shows how large the current power requirement is on the PoE ports.

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

☐ **Port settings**

– For devices with **PoE** select the `Basic Settings:Power over Ethernet` dialog.
– For devices with **PoE+** select the `Basic Settings:Power over Ethernet Plus:Port` dialog.

The table only shows ports that support PoE.

☐ In the “POE on” column, you can enable/disable PoE at this port.
☐ The “Status” column indicates the PoE status of the port.
☐ In the “Priority” column (MACH 4000), set the PoE priority of the port to “low”, “high” or “critical”.
☐ The "Class" column indicates the class of the connected device:
Class: Maximum delivered power
0: 15.4 W = As-delivered state
1: 4.0 W
2: 7.0 W
3: 15.4 W
4: reserved, treated as Class 0
☐ The column „Consumption [W]“ displays the current power delivered at the respective port.
☐ The “Name” column indicates the name of the port, see `Basic settings:Port configuration`.

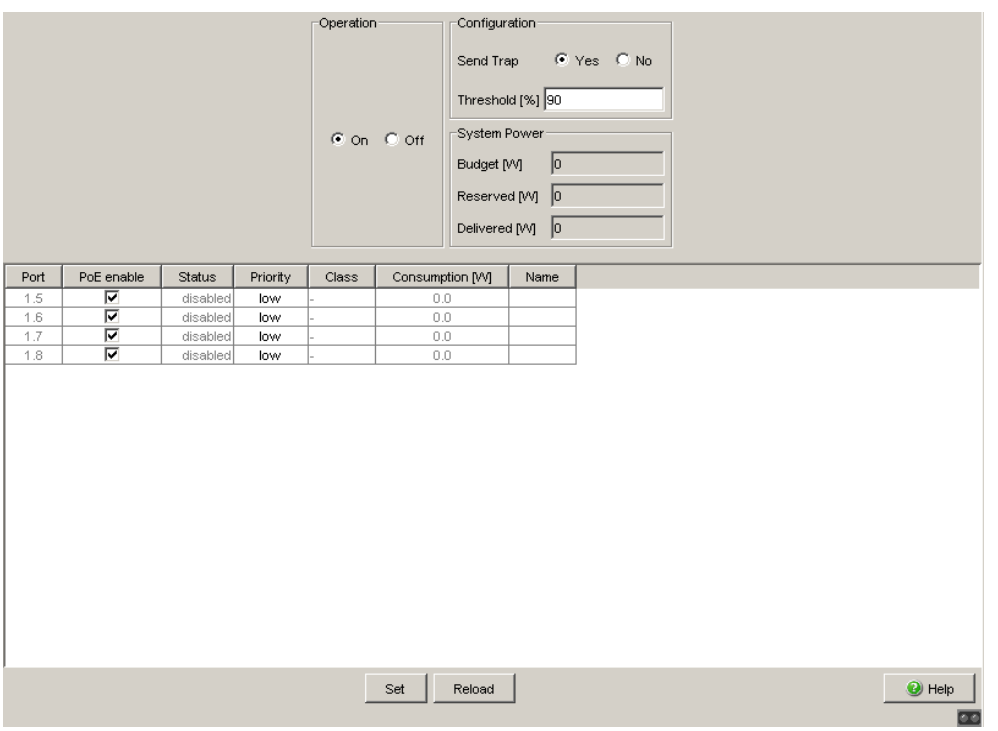


Figure 17: Power over Ethernet dialog

Switch on PoE power supply

OCTOPUS PoE devices let you switch on the PoE power supply before loading and starting the software. This means that the connected PoE devices (powered devices) are supplied with the PoE voltage more quickly and the start phase of the whole network is shorter.

`enable`	Switch to Privileged EXEC mode.
`configure`	Switch to Global Configure mode.
`#inlinepower fast-startup enable`	Switch on Inline Power Fast Startup (disabled in the as-delivered state).
`#inlinepower fast-startup disable`	Switch off Inline Power Fast Startup.
`#show inlinepower`	Show Power over Ethernet System Information (Fast Startup and other information).

Cold start with detected errors

This function lets you reset the device automatically with a cold start in the following cases:

- if an error is detected
  (selftest reboot-on-error enable)
  or
- only if a serious error is detected
  (selftest reboot-on-error seriousOnly)

If the function `selftest reboot-on-error seriousOnly` is enabled, the device behaves as follows:

- If an error is detected in a subsystem (for example, if an HDX/FDX mismatch is detected on a port), cold starts of the device are dropped.
- However, if an error affecting the function of the entire device is detected, the device still carries out a cold start.
- The device sends a trap (see on page 214 “Sending Traps”).

Note: If the `selftest reboot-on-error seriousOnly` function is enabled and the device detects an HDX/FDX mismatch, automatic cold starts of the device are dropped. In this case, to return the affected port(s) to a usable condition, open the `Basic Settings:Reboot` dialog and carry out a cold start of the device.

`enable`	Switch to Privileged EXEC mode.
`configure`	Switch to Global Configure mode.

`#selftest reboot-on-error enable`	Switch on the "Cold start if error detected“ function.
`#selftest reboot-on-error seriousOnly`	Switch on the "Cold start only if serious error detected“ function.
`#selftest reboot-on-error disable`	Switch off the "Cold start if error detected“ function (enabled in the as-delivered state).
`#show selftest`	Show status of the "Cold start if error detected" function (Enabled/Disabled/seriousOnly).

6 Assistance in the Protection from Unauthorized Access

The device provides the following functions to help prevent unauthorised accesses.

- Password for SNMP access
- Telnet/internet/SSH access can be switched off
- Restricted Management access
- HiDiscovery-Function can be switched off
- Port access control by IP or MAC address
- IEEE 802.1X standard port authentication
- Access Control Lists (ACL)
- Login Banner

6.1 Protecting the device

If you want to maximize the protection of the device against unauthorized access in just a few steps, you can perform the following steps on the device as required:

- ☐ Deactivate SNMPv1 and SNMPv2 and select a password for SNMPv3 access other than the standard password (see on page 96 “Entering the password for SNMP access”).
- ☐ Deactivate the Web access after you have downloaded the applet for the graphical user interface onto your management station. You can start the applet as an independent program in order to have SNMPv3 access to the device.
  Deactivate Telnet access.
  If necessary, deactivate SSH access.
  See “Switching Telnet/Internet/SSH access on/off” on page 102.
- ☐ Deactivate HiDiscovery access.

Note: Retain at least one option to access the device. Connecting to the device via V.24 serial access is possible, since it cannot be deactivated.

6.2 Password for SNMP access

6.2.1 Description of password for SNMP access

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

The device receives the SNMP packet and compares the IP address of the sending computer and the password with the entries in the device MIB.
If the password has the appropriate access right, and if the IP address of the sending computer has been entered, then the device will allow access.

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

To help protect your device from unwanted access:

- ☐ First define a new password with which you can access from your computer with all rights.
- ☐ Treat this password as confidential, because everyone who knows the password can access the device MIB with the IP address of your computer.
- ☐ Limit the access rights of the known passwords or delete their entries.

6.2.2 Entering the password for SNMP access

☐ Select the `Security:Password/SNMP Access` dialog.
This dialog gives you the option of changing the read and read/write passwords for access to the device via the graphical user interface, via the CLI, and via SNMPv3 (SNMP version 3).
Set different passwords for the read password and the read/write password so that a user that only has read access (user name “user”) does not know, or cannot guess, the password for read/write access (user name “admin”).
If you set identical passwords, when you attempt to write this data the device reports a general error.

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

Note: Passwords are case-sensitive.

☐ Select “Modify Read-Only Password (User)” to enter the read password.
☐ Enter the new read password in the “New Password” line and repeat your entry in the “Please retype” line.
☐ Select “Modify Read-Write Password (Admin)” to enter the read/write password.
☐ Enter the read/write password and repeat your entry.
☐ The "Accept only encrypted requests" function encrypts the data of the Web-based management that is transferred between your PC and the device with SNMPv3. You can set the funtion differently for access with a read password and access with a read/write password.
☐ When you activate the "Synchronize password to v1/v2 community" function, when the password is changed the device synchronizes the corresponding community name.
  – When you change the password for the read/write access, the device updates the readWrite community for the SNMPv1/v2 access to the same value.
  – When you change the password for the read access, the device updates the readOnly community for the SNMPv1/v2 access to the same value.

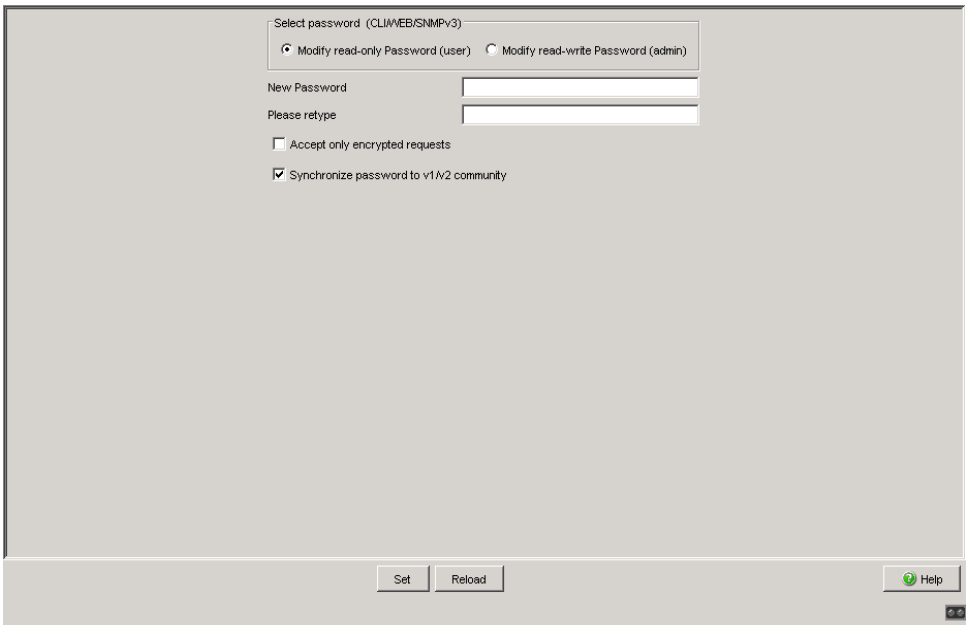


Figure 18: Password/SNMP Access dialog

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

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

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

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

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

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

Index	Serial number for this table entry
Community Name	Password with which this computer can access the device. This password is independent of the SNMPv3 password. If you activate the "Synchronize community to v3 password" function in the "Configuration" frame, the device synchronizes the corresponding SNMPv3 password when you change the community name.
IP Address	IP address of the computer that can access the device.
IP Mask	IP mask for the IP address
Access Mode	The access mode determines whether the computer has read-only or read-write access.
Active	Enable/disable this table entry.

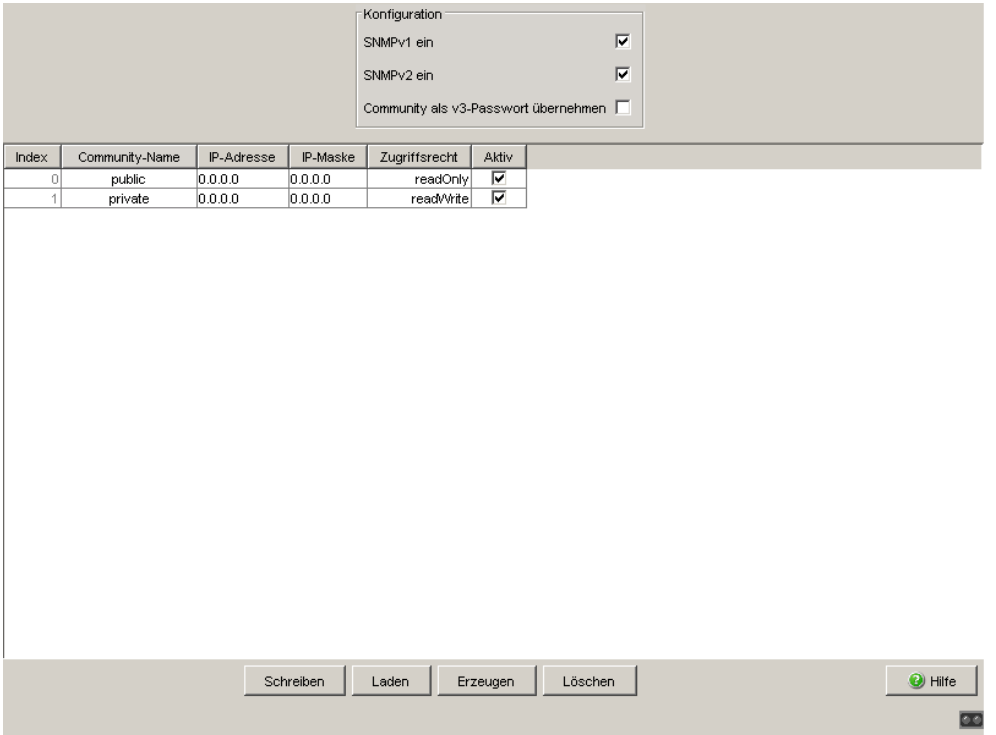


Figure 19: SNMPv1/v2 access dialog

☐ To create a new line in the table click “Create”.
☐ To delete an entry, select the line in the table and click “Remove”.

6.3 Telnet/internet/SSH access

6.3.1 Description of Telnet Access

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

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

6.3.2 Description of Web Access (http)

The device's Web server allows you to configure the device by using the graphical user interface. You can deactivate the Web server to prevent Web access to the device.
The server is activated in its default setting.

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

6.3.3 Description of SSH Access

The device's SSH server allows you to configure the device using the Command Line Interface (in-band). You can deactivate the SSH server to prevent SSH access to the device.
The server is deactivated in its default setting.
After the SSH server has been deactivated, you will no longer be able to access the device via a new SSH connection. If an SSH connection already exists, it is retained.

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

Note: To be able to access the device via SSH, you require a key that has to be installed on the device. See “Preparing access via SSH” on page 275.

The device supports SSH version 1 and version 2. You have the option to define the protocol to be used.

- ☐ Open the `Security:Telnet/Web/SHH Access` dialog.
- ☐ Select the protocol to be used in the "Configuration" frame, "SSH Version" field.

`enable`	Change to the privileged EXEC mode.
`no ip ssh`	Deactivates the SSH server.
ip ssh protocol 2	The SSH server uses SSH version 2.
ip ssh protocol 1	The SSH server uses SSH version 1.
ip ssh protocol 1 2	The SSH server uses SSH versions 1 and 2.
`ip ssh`	Activates the SSH server.

6.3.4 Switching Telnet/Internet/SSH access on/off

The Web server copies a Java applet for the graphical user interface onto your computer. The applet then communicates with the device by SNMPv3 (Simple Network Management Protocol). The Web server of the device allows you to configure the device using the graphical user interface. You can switch off the Web server in order to prevent the applet from being copied.

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

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

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`lineconfig`	Switch to the configuration mode for CLI.
`transport input telnet`	Enable Telnet server.
`no transport input telnet`	Disable Telnet server.
`exit`	Switch to the Configuration mode.
`exit`	Switch to the privileged EXEC mode.
`ip http server`	Enable Web server.
`no ip http server`	Disable Web server.
`ip ssh`	Enable SSH function on Switch
`no ip ssh`	Disable SSH function on Switch

6.3.5 Web access through HTTPS

The HTTPS communication protocol (HyperText Transfer Protocol Secure) helps protect data transfers from interception. The device uses the HTTPS protocol to encrypt and authenticate the communications between web server and browser.
The Web server uses HTTP to load a Java applet for the graphical user interface onto your computer. This applet then communicates with the device by SNMP (Simple Network Management Protocol). If you have enabled the `Web Server (HTTPS)` function, the Java applet starts setting up a connection to the device via HTTPS. The device creates an HTTPS tunnel through the SNMP. It uses DES encoding on 56 bits. You can upload HTTPS certificates to the device.

Certificate

An X.509/PEM Standard certificate (Public Key Infrastructure) is required for the encryption. In the as-delivered state, a self-generated certificate is already present on the device.

- ☐ You can create an X509/PEM certificate using the following CLI command: `# ip https certgen`
- ☐ You can upload a new certificate using the following CLI command:
  `copy tftp://<server_ip>/<path_to_pem> nvram:httpscert`
- ☐ You can switch the HTTPS server off and on again using the following CLI command sequence:
  ```
  # no ip https server
  # ip https server
  ```

Note: If you upload a new certificate, reboot the device or the HTTPS server in order to activate the certificate.

HTTPS connection

Note: The standard port for HTTPS connection is 443. If you change the number of the HTTPS port, reboot the device or the HTTPS server in order to make the change effective.

☐ You can change the HTTPS port number using the following CLI-command (where <port_no> is the number of the HTTPS port):
`#ip https port <port_no>`

Note: If you want to use HTTPS, switch on both HTTPS and HTTP. This is required in order to load the applet. In the as-delivered state, HTTPS is switched off.

☐ Open the `Security:Telnet/Internet/SSH Access` dialog.

☐ Tick the boxes `Telnet Server active`, `Web Server(http)` and `Web Server(https)`. In the `HTTPS Port Number` box, enter the value `443`.

☐ To access the device by HTTPS, enter HTTPS instead of HTTP in your browser, followed by the IP address of the device.

`enable`	Switch to Privileged EXEC mode.
`# ip https server`	Switch on HTTPS-server.
`# ip https port <port_no>`	Set the HTTPS port number for a secure HTTP connection. - As-delivered state: 443. - Value range: 1-65535
`# no ip https server` `# ip https server`	If you change the HTTPS port number, switch the HTTPS server off and then on again in order to make the change effective.
`# show ip https`	Optional: Show the status of the HTTPS server and HTTPS port number.
`# ip https certgen`	Create X509/PEM certificates.
`# copy tftp://<server_ip>/<path_to_pem> nvram:httpscert`	Upload an X509/PEM certificate for HTTPS using TFTP.
`# no ip https server` `# ip https server`	After uploading the HTTPS certificate, switch the HTTPS server off and then on again in order to activate the certificate.:

The device uses HTTPS protocol and establishes a new connection. When the session is ended and the user logs out, the device terminates the connection.

Note: The device allows you to open HTTPS- and HTTP connections at the same time. The maximum number of HTTP(S) connections that can be open at the same time is 16.

6.4 Restricted Management Access

The device allows you to differentiate the management access to the device based on IP address ranges, and to differentiate these in turn based on management services (http, snmp, telnet, ssh). You thus have the option to set finely differentiated management access rights.

If you only want the device, which is located, for example, in a production plant, to be managed from the network of the IT department via the Web interface, but also want the administrator to be able to access it remotely via SSH, you can achieve this with the “Restricted management access” function.

You can configure this function using the graphical user interface or the CLI. The graphical user interface provides you with an easy configuration option. Make sure you do not unintentionally block your access to the device. The CLI access to the device via V.24 provided at all times is excluded from the function and cannot be restricted.

In the following example, the IT network has the address range 192.168.1.0/24 and the remote access is from a mobile phone network with the IP address range 109.237.176.0 - 109.237.176.255.

The device is already prepared for the SSH access (see on page 275 “Preparing access via SSH”) and the SSH client application already knows the fingerprint of the host key on the device.

Parameter	IT network	Mobile phone network
Network address	192.168.1.0	109.237.176.0
Netmask	255.255.255.0	255.255.255.0
Desired management access	http, snmp	ssh

Table 4: Example parameter for the restricted management access

☐ Select the `Security:Restricted Management Access` dialog.

- ☐ Leave the existing entry unchanged and use the “Create” button to create a new entry for the IT network.
- ☐ Enter the IP address 192.168.1.0.
- ☐ Enter the netmask 255.255.255.0.
- ☐ Leave the HTTP and SNMP management services activated and deactivate the Telnet and SSH services by removing the checkmarks from the respective boxes.
- ☐ Use the “Create” button to create a new entry for the mobile phone network.
- ☐ Enter the IP address 109.237.176.0.
- ☐ Enter the netmask 255.255.255.0.
- ☐ Deactivate the HTTP, SNMP and Telnet services and leave SSH activated.
- ☐ Make sure you have CLI access to the device via V.24.
- ☐ Deactivate the preset entry, because this allows everything and would cause your subsequent entries to have no effect.
- ☐ Activate the function.
- ☐ Click on “Write” to temporarily save the data.
- ☐ If your current management station is also located in the IT network, you continue to have access to the graphical user interface. Otherwise the device ignores operations via the graphical user interface, and it also rejects a restart of the graphical user interface.
- ☐ Check whether you can access the device from the IT network via http and snmp: Open the graphical user interface of the device in a browser, login on the start screen, and check whether you can read data (as user “user”) or read and write data (as user “admin”).
  Check whether the device rejects connections via telnet and ssh.
- ☐ Check whether you can access the device from the mobile phone network via ssh: Open an SSH client, make a connection to the device, login, and check whether you can read data, or read and write data.
  Check whether the device rejects connections via http, snmp and telnet.
- ☐ When you have successfully completed both tests, save the settings in the non-volatile memory. Otherwise check your configuration. If the device rejects access with the graphical user interface, use the CLI of the device to initially deactivate the function via V.24.

`enable`	Switch to the privileged EXEC mode.
`show network mgmt-access`	Display the current configuration.
`network mgmt-access add`	Create an entry for the IT network. This is given the smallest free ID - in the example, 2.
`network mgmt-access modify 2 ip 192.168.1.0`	Set the IP address of the entry for the IT network.
`network mgmt-access modify 2 netmask 255.255.255.0`	Set the netmask of the entry for the IT network.
`network mgmt-access modify 2 telnet disable`	Deactivate telnet for the entry of the IT network.
`network mgmt-access modify 2 ssh disable`	Deactivate SSH for the entry of the IT network.
`network mgmt-access add`	Create an entry for the mobile phone network. In the example, this is given the ID 3.
`network mgmt-access modify 3 ip 109.237.176.0`	Set the IP address of the entry for the mobile phone network.
`network mgmt-access modify 3 netmask 255.255.255.0`	Set the netmask of the entry for the mobile phone network.
`network mgmt-access modify 3 http disable`	Deactivate http for the entry of the mobile phone network.
`network mgmt-access modify 3 snmp disable`	Deactivate snmp for the entry of the mobile phone network.
`network mgmt-access modify 3 telnet disable`	Deactivate telnet for the entry of the mobile phone network.
`network mgmt-access status 1 disable`	Deactivate the **preset** entry.
`network mgmt-access operation enable`	Activate the function **immediately**.
`show network mgmt-access`	Display the current configuration of the function.
`copy system:running-config nvram:startup-config`	Save the entire configuration in the non-volatile memory.

6.5 HiDiscovery Access

6.5.1 Description of the HiDiscovery Protocol

The HiDiscovery protocol allows you to allocate an IP address to the device (see on page 39 “Entering the IP Parameters via HiDiscovery”). HiDiscovery v1 is a Layer 2 protocol. HiDiscovery v2 is a Layer 3 protocol.

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

6.5.2 Enabling/disabling the HiDiscovery function

☐ Select the `Basic settings:Network` dialog.

☐ Disable the "HiDiscovery function in the “HiDiscovery Protocol v1/v2" frame or limit the access to `read-only`.

`enable`	Switch to the privileged 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

6.6 Port access control

6.6.1 Description of the port access control

You can configure the device in such a way that it helps to protect every port from unauthorized access. Depending on your selection, the device checks the MAC address or the IP address of the connected device.
The following functions are available for monitoring every individual port:

- The device can distinguish between authorized and unauthorized access and supports 2 types of access control:
  - Access for all:
    – No access restriction.
    – MAC address 00:00:00:00:00:00 or
    – IP address 0.0.0.0.
  - Access exclusively for defined MAC and IP addresses:
    – Only devices with defined MAC or IP addresses have access.
    – You can define up to 10 IP addresses and up to 50 MAC addresses or maskable MAC addresses.
- The device reacts to an unauthorized access with the following selectable actions:
  - none: no reaction
  - trapOnly: message by sending a trap
  - portDisable: message by sending a trap and disabling the port
  - autoDisable: disabling the port via the AutoDisable function with the option to enable the port again after a definable time has elapsed.

6.6.2 Application Example for Port Access Control

You have a LAN connection in a room that is accessible to everyone. To set the device so that only defined users can use this LAN connection, activate the port access control on this port. An unauthorized access attempt will cause the device to shut down the port and alert you with an alarm message. The following is known:

Parameter	Value	Explanation
Allowed IP Addresses	10.0.1.228 10.0.1.229	The defined users are the device with the IP address 10.0.1.228 and the device with the IP address 10.0.1.229
Action	portDisable	Disable the port with the corresponding entry in the port configuration table (see on page 87 “Configuring the Ports”) and send an alarm

Prerequisites for further configuration:

- The port for the LAN connection is enabled and configured correctly (see on page 87 “Configuring the Ports”)
- Prerequisites for the device to be able to send an alarm (trap) (see on page 217 “Configuring Traps”):
  - You have entered at least one recipient
  - You have set the flag in the “Active” column for at least one recipient
  - In the “Selection” frame, you have selected “Port Security”

☐ Configure the port security.

☐ Select the `Security:Port Security` dialog.

☐ In the “Configuration” frame, select “IP-Based Port Security”.

☐ In the table, click on the row of the port to be protected, in the “Allowed IP addresses” cell.
☐ Enter in sequence:
– the IP subnetwork group: 10.0.1.228
– a space character as a separator
– the IP address: 10.0.1.229
Entry: `10.0.1.228 10.0.1.229`
☐ In the table, click on the row of the port to be protected, in the “Action” cell, and select `portDisable`.

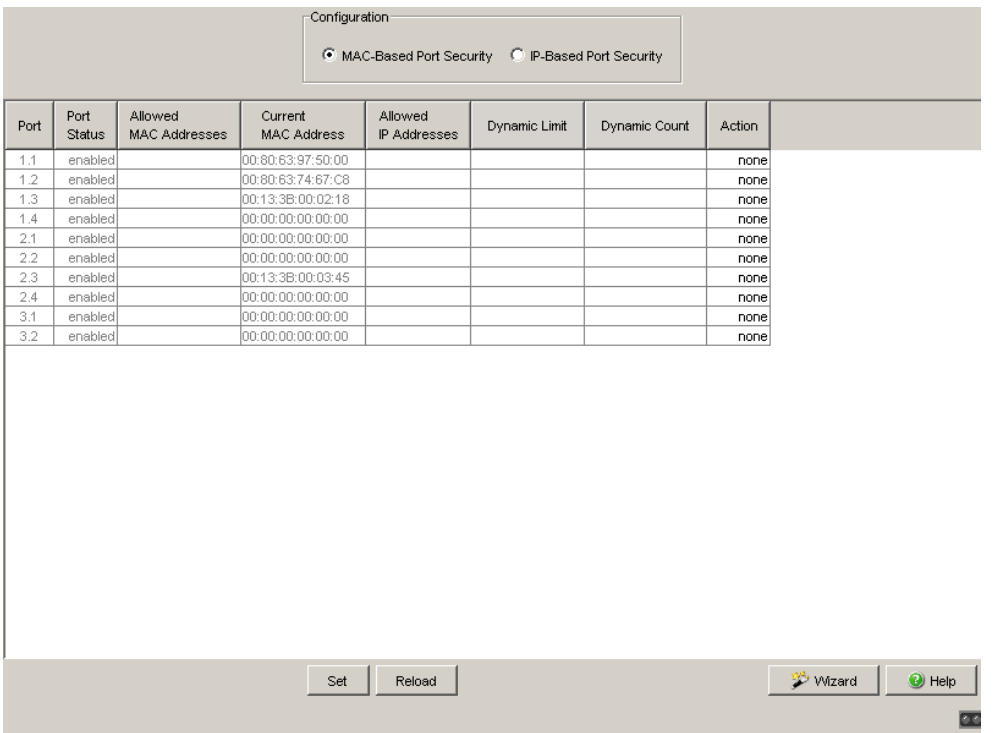


Figure 20: Port Security dialog

☐ Save the settings in the non-volatile memory.

☐ Select the dialog `Basic Settings:Load/Save`.
☐ In the “Save” frame, select “To Device” for the location and click “Save” to permanently save the configuration in the active configuration.

6.7 Port Authentication IEEE 802.1X

6.7.1 Description of Port Authentication according to IEEE 802.1X

The port-based network access control is a method described in norm IEEE 802.1X to help protect IEEE 802 networks from unauthorized access. The protocol controls the access to this port by authenticating and authorizing a terminal device that is connected to one of the device's ports.
The authentication and authorization is carried out by the authenticator, in this case the device. The device authenticates the supplicant (the querying device, e.g. a PC, etc.), which means that it permits the access to the services it provides (e.g. access to the network to which the device is connected) or denies it. In the process, the device accesses an external authentication server (RADIUS server), which checks the authentication data of the supplicant. The device exchanges the authentication data with the supplicant via the Extensible Authentication Protocol over LANs (EAPOL), and with the RADIUS server via the RADIUS protocol.

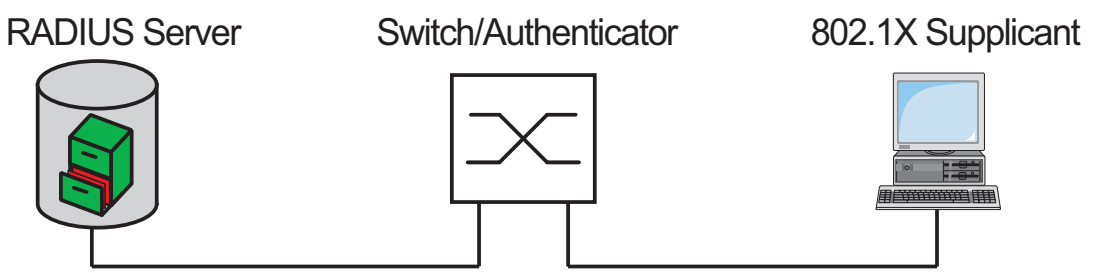


Figure 21: Radius server connection

6.7.2 Authentication Process according to IEEE 802.1X

A supplicant attempts to communicate via a device port.

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

6.7.3 Preparing the Device for the IEEE 802.1X Port Authentication

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

6.7.4 IEEE 802.1X Settings

Configurating the RADIUS Server

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

This dialog allows you to enter the data for 1, 2 or 3 RADIUS servers.

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

Selecting Ports

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

Activating Access Control

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

6.8 Access Control Lists (ACL)

You can use Access Control Lists (ACL) to filter out, forward, divert or prioritize data packets as they are received. The device provides

- MAC-based ACLs and
- IP-based ACLs.

The device considers the ACLs when it receives a package. This is why the lists are called Ingress ACLs.

You configure Access Control Lists via the Command Line Interface. You will find details on this in the document “Reference Manual Command Line Interface“.

The device provides the following ACL capabilities:

- Up to 100 ACLs
- 10 rules per ACL,
- Up to 100 rules per interface,
- Up to 1000 rules on all interfaces combined
- Possible actions:
  - permit and deny,
  - in combination with permit: assign queue and redirect - i.e. if a rule applies, the packet is forwarded to the specific interface.
- “Deny everything” is always the (invisible) final rule. It comes into effect if no other rules apply to this interface.

The configuration of ACLs consists of the following steps:

☐ First define ACL and then
☐ attach the ACL to one or all interfaces.
You can attach ACLs to all physical ports and to all link aggregation interfaces.

Note: You configure Access Control Lists via the Command Line Interface. You will find details on this in the document “Reference Manual Command Line Interface“.

The sequence used in defining the rules of a list and the sequence in which these lists are connected to an interface determines the sequence in which the rules and lists are used (see on page 125 “Specifying the Sequence of the Rules”).

Note: With PowerMICE and MACH 4000, you can use either MAC-based or IP-based ACLs for each interface.
With MACH 4002-24G/48G, you can use both MAC-based and IP-based ACLs for each interface.

6.8.1 Description of prioritizing with ACLs

Prioritizing with ACLs provides you with an extension of the prioritizing function. Using the “assign queue” ACL action, you can perform extended prioritizing using protocols, source and destination addresses, VLAN ID, and so on (see on page 118 “Description of IP-based ACLs”),(see on page 119 “Description of MAC-based ACLs”).

If an ACL rule containing an assign queue action applies to a packet received, the device modifies the priority information in the data packet (see on page 175 “QoS/Priority”) according to the specified (see table 5) assign queue parameter. This procedure is known as ACL remarking. The device sends the data packets with the modified priority information.

Assign queue parameter	VLAN priority	DSCP
0	0	CS0 (0)
1	1	CS1 (8)
2	2	CS2 (16)
3	3	CS3 (24)
4	4	CS4 (32)
5	5	CS5 (40)
6	6	CS6 (48)
7	7	CS7 (56)

Table 5: Assigning the assign queue parameters to the modified VLAN priority and to the modified DSCP value

6.8.2 Description of IP-based ACLs

The device differentiates between standard and extended IP-based ACLs. ACLs with an ID number (ACL ID)

- 1 to 99 are standard IP-based ACLs and
- 100 to 199 are extended IP-based ACLs.

Standard IP-based ACLs provide the following criteria for filtering:

- IP source address with netmask
- All data packets (match any)

Extended IP-based ACLs provide the following criteria for filtering:

- All data packets (every)
- Protocol number or protocol (IP, ICMP, IGMP, TCP, UDP)
- IP source address with netmask or all IP source addresses (any)
- Layer 4 protocol port number of the source (UDP port, TCP port)
- IP destination address with netmask or all IP destination addresses (any)
- Layer 4 protocol port number of the destination (UDP port, TCP port)
- ToS field with mask

- DSCP field
- IP precedence field

Note: If you are using IP ACLs at ports which are located in the HIPER-Ring or which participate in the Ring/network coupling, you add the following rule to the ACLs:

- PERMIT
- Protocol: UDP
- Source IP: ANY
- Destination IP: 0.0.0.0/32
- Source port: 0
- Destination port: 0
- CLI command (1xx stands for 100..199):

```
access-list 1xx permit udp any eq 0
0.0.0.0 0.0.0.0 eq 0
```

Note: IP address masks in the rules of ACLs are inverse.
This means that if you want to mask a single IP address, you select the netmask 0.0.0.0.

6.8.3 Description of MAC-based ACLs

While you use an ID number to identify IP-based ACLs, you use a unique name of your choice to identify MAC-based ACLs.

MAC-based ACLs provide the following criteria for filtering:

- Source MAC address with masks or all sources (any)
- Destination MAC address or all destinations (any)
- Ethernet type

- VLAN ID
- VLAN priority (COS)
- Secondary VLAN ID
- Secondary VLAN priority

Note: If you are using MAC ACLs at ports which are located in the HIPER-Ring or which participate in the Ring/network coupling, you add the following rule to the ACLs:

- PERMIT
- Source MAC: ANY
- Destination MAC: 00:80:63:00:00:00
- Destination MAC mask: 01:00:00:ff:ff:ff
- CLI command in Config-mac-access mode:
  `permit any 00:80:63:00:00:00 01:00:00:ff:ff:ff`

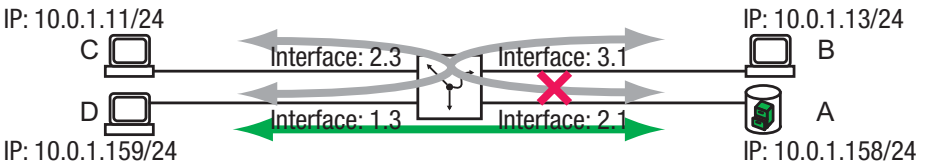
Note: If you are using MAC ACLs at ports located in the MRP-Ring, you add the following rule to the ACLs:

- PERMIT
- Source MAC: ANY
- Destination MAC: 01:15:4E:00:00:00
- Destination MAC mask: 00:00:00:00:00:03
- CLI command in the Config-mac-access mode:
  `permit any 01:15:4E:00:00:00 00:00:00:00:00:03`

Note: MAC address masks in the rules of ACLs are inverse.
This means that if you want to mask a single MAC address, you select the network mask 00:00:00:00:00:00.
If you want to mask MAC addresses in the range from 00:80:63:00:00:00 to 00:80:63:FF:FF:FF, you select the network mask 00:00:00:FF:FF:FF.

6.8.4 Configuring IP ACLs

Example: Extended ACL



B and C are not allowed to communicate with A.

`enable`	Change to the privileged EXEC mode.
`configure`	Change to the Configuration mode.
`access-list 100 deny ip 10.0.1.11 0.0.0.0 10.0.1.158 0.0.0.0`	Erzeugt die erweiterte ACL 100 mit der 1. Regel. Diese verweigert den Datenverkehr von der IP-Quelladresse 10.0.1.11 zur IP-Zieladresse 10.0.1.158.
`access-list 100 permit ip any any`	Fügt der ACL 100 eine weitere Regel hinzu. Diese erlaubt den Datenverkehr von jeder IP-Quelladresse zu jeder IP-Zieladresse.
`access-list 110 deny ip 10.0.1.13 0.0.0.0 10.0.1.158 0.0.0.0`	Erzeugt die erweiterte ACL 110 mit der 1. Regel. Diese verweigert den Datenverkehr von der IP-Quelladresse 10.0.1.13 zur IP-Zieladresse 10.0.1.158.
`access-list 110 permit ip any any`	Fügt der ACL 110 eine weitere Regel hinzu. Diese erlaubt den Datenverkehr von jeder IP-Quelladresse zu jeder IP-Zieladresse.
`exit`	Change to the privileged EXEC mode.
`show ip access-lists 100`	Zeigt die Regeln von ACL 100 an.

```
ACL ID: 100


Rule Number: 1
Action..................................... deny
Match All.................................. FALSE
Protocol................................... 255(ip)
Source IP Address.......................... 10.0.1.11
Source IP Mask............................. 0.0.0.0
Destination IP Address..................... 10.0.1.158
Destination IP Mask........................ 0.0.0.0

Rule Number: 2
Action..................................... permit
Match All.................................. TRUE
```

`configure`	Change to the Configuration mode.
`interface 2/3`	Change to the Interface Configuration mode of interface 2/3.
`ip access-group 100 in`	Bindet die ACL 100 für empfangene Daten an das Interface 2.3.
`exit`	Change to the Configuration mode.
`interface 3/1`	Wechsel in den Interface-Konfigurationsmodus von Interface 3.1.
`ip access-group 110 in`	Bindet die ACL 110 für empfangene Daten an das Interface 3.1.
`exit`	Change to the Configuration mode.
`exit`	Change to the privileged EXEC mode.

```
show access-lists interface 2/3 in

ACL Type             ACL ID                Sequence Number
-------- ------------------------------ ---------------
IP       100                            1
```

6.8.5 Configuring MAC ACLs

Example: MAC ACL
Filtering AppleTalk and IPX from the entire network.

```
enable                                  Switch to the privileged EXEC mode.
configure                               Switch to the Configuration mode.
mac access-list extended                Create the extended ACL “ipx-apple”.
  ipx-apple
  deny any any ipx                      Add the rule “deny IPX” to the list.
  deny any any appletalk                Add the rule “deny AppleTalk” to the list.
  permit any any                        Add the rule “permit all other data” to the list.
exit                                    Switch to the Configuration mode.

mac access-group ipx-apple              Attach the ACL “ipx-apple” to all interfaces.
  in
exit                                    Switch to the privileged EXEC mode.

show mac access-lists                   Display the ACLs..
     MAC ACL Name                    Rules Direction      Interface(s)
------------------------------- ----- --------- ------------------
ipx-apple                          3     inbound   1/1,1/2,1/3,1/4,2/
                                                   1,2/2,2/3,2/4,3/1,3/2
show access-lists interface             Display the ACLs of interface 1.1.
  1/1 in
ACL Type             ACL ID              Sequence Number
-------- ------------------------------ ---------------
MAC      ipx-apple                      1
```

6.8.6 Configuring Priorities with IP ACLs

Example: Prioritizing Multicast streams.

- Assign priority 6 to the Multicast streams with the IP Multicast destination addresses 239.1.1.1 to 239.1.1.255 and
- Assign priority 5 to the Multicast streams with the IP Multicast destination addresses 237.1.1.1 to 237.1.1.255 and

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`access-list 102 permit ip any 239.1.1.1 0.0.0.255 assign-queue 6`	Create the extended ACL 102 with the first rule. This rule assigns priority 6 to the IP Multicast destination addresses 239.1.1.1 with the mask 0.0.0.255.
`access-list 102 permit ip any 237.1.1.1 0.0.0.255 assign-queue 5`	Add another rule to the ACL 102. This rule assigns priority 5 to the IP Multicast destination addresses 237.1.1.1 with the mask 0.0.0.255.
`exit`	Switch to the privileged EXEC mode.
`show ip access-lists 102`	Displays the rules of ACL 102.

```
ACL ID: 102

Rule Number: 1
Action..................................... permit
Match All.................................. FALSE
Protocol................................... 255(ip)
Destination IP Address..................... 239.1.1.1
Destination IP Mask........................ 0.0.0.255
Assign Queue............................... 6

Rule Number: 2
Action..................................... permit
Match All.................................. FALSE
Protocol................................... 255(ip)
Destination IP Address..................... 237.1.1.1
Destination IP Mask........................ 0.0.0.255
Assign Queue............................... 5
```

Example: Extended ACL with prioritizing using the Simple Network Management Protocol (SNMP, Layer 4)

`enable`	Change to the privileged EXEC mode.
`configure`	Change to the Configuration mode.
`access-list 104 permit udp any any eq snmp assign-queue 5`	Create the extended ACL 104 with the first rule. This rule assigns priority 5 to all SNMP packets with the UDP destination port (=161). This rule overwrites any priority contained in a VLAN tag with the value 5, and also overwrites the IP-DSCP value with cs5.
`exit`	Change to the privileged EXEC mode.
`show ip access-lists 104`	Displays the rules of ACL 104.

```
ACL ID: 104


Rule Number: 1
Action..................................... permit
Match All.................................. FALSE
Protocol................................... 17(udp)
Destination L4 Port Keyword................ 161(snmp)
Assign Queue............................... 5
```

`configure`	Change to the Configuration mode.
`interface 2/1`	Switch to the Interface Configuration mode of interface 2/1.
`ip access-group 104 in`	Attaches ACL 104 to interface 2.1.
`exit`	Change to the Configuration mode.
`exit`	Change to the privileged EXEC mode.
`show access-lists interface 2/1 in`	Display the ACLs attached to interface 2.1 forreceived data packets.

```
ACL Type             ACL ID                 Sequence Number
-------- ------------------------------ ---------------
IP       100                            1
IP       102                            3
IP       104                            4
```

ACL 100 contains the rule “permit all” at the end. Thus the ACLs 102 and 104 are never applied. You can use the sequence number to alter the sequence for processing the ACLs (see on page 125 “Specifying the Sequence of the Rules”).

6.8.7 Specifying the Sequence of the Rules

The sequence of the ACLs determines their usage. The first list that applies is used, and all subsequent rules are ignored. You can influence the sequence by assigning the sequence number. A small sequence number has precedence over a higher one.

```
enable                          Switch to the privileged EXEC mode.
configure                       Switch to the Configuration mode.
ip access-group 100 in 30       Assign sequence number 30 to ACL 100.
ip access-group 102 in 10       Assign sequence number 10 to ACL 102.
ip access-group 104 in 20       Assign sequence number 20 to ACL 104.
exit                            Switch to the privileged EXEC mode.
show access-lists interface     Display the ACLs attached to interface 2.1 for
  2/1 in                        received data packets.

ACL Type             ACL ID                 Sequence Number
-------- ------------------------------ ---------------
IP       100                            30
IP       104                            20
IP       102                            10
```

6.8.8 ACLs for Layer 4 fragments

Splitting a long data packet into a number of shorter data packets is known as fragmenting. For example, some transferring routers fragment a Layer 4 data packet into a number of Layer 3 data packets if the length of the data packet is greater than the MTU (Maximum Transmission Unit) of the transferring interface.

Only the first Layer 3 data packet contains the Layer 4 header, e.g. TCP or UDP. The following data packets with the Layer 4 fragments do not contain any Layer 4 headers that can be evaluated. Therefore, ACLs drop these data packets. The MACH104, MACH1040 and MACH4002 24G/48G devices process Layer 4 fragments and allow you to forward these data packets also.

When you set up an ACL for Layer 4, the device uses the user-defined rule to automatically create a second rule for the fragments:

- The user-defined rule processes the data packet with the first Layer 4 fragment.
- The automatically created rule processes the data packets with the following Layer 4 fragments.

Therefore, when the fragment processing is activated, the maximum possible number of ACLs in the device is reduced.

You activate the processing of Layer 4 fragments globally in the device:

`enable`	Change to the privileged EXEC mode.
`configure`	Change to the Configuration mode.
`access-list fragments`	Activate the fragment processing in the device.
`exit`	Change to the privileged EXEC mode.
`show access-lists global`	Display the global ACL settings of the device.

```
L4 Fragment Processing..................... Enabled
```

6.9 Login Banner

The device gives you the option of displaying a greeting text to users before they login to the device. The users see this greeting text in the login dialog of the graphical user interface (GUI) and of the Command Line Interface (CLI).

Users logging in with SSH see the greeting text - depending on the client used - before or during the login.

Perform the following work steps:

- ☐ Open the `Security:Login Banner` dialog, "Login Banner" tab.
- ☐ Enter the greeting text in the "Banner Text" frame.
  Max. 255 characters allowed.
- ☐ To switch on the function, in the "Operation" frame, mark the "On" radio button.
- ☐ Click "Set" to save the changes temporarily.

`enable`	Change to the privileged EXEC mode.
`set pre-login-banner text "<string>"`	Assign the greeting text: – Put the text in quotation marks. – Max. 255 characters allowed. – Insert tab using string `\\t`. – Insert line break using string `\\n`.
`set pre-login-banner operation`	Switching the function on.
`logout`	Logout from device. The text is visible before you login again.

6.10 CLI Banner

In the default setting, the CLI start screen shows information about the device, such as the software version and the device settings. The "CLI Banner" function allows you to replace this information with an individual text.

Perform the following work steps:

- ☐ Open the `Security:Login/CLI Banner` dialog, "CLI Banner" tab.
- ☐ In the "Banner Text" frame, enter the text of your choice. Max. 2048 characters allowed.
- ☐ To switch on the function, in the "Operation" frame, mark the "On" radio button.
- ☐ Click "Set" to save the changes temporarily.

`enable`	Change to the privileged EXEC mode.
`set clibanner text "<string>"`	Assign the text to: – Put the text in quotation marks. – Max. 2048 characters allowed. – Insert tab using string `\\t`. – Insert line break using string `\\n`.
`set clibanner operation`	Switching the function on.
`logout`	Logout from device. The text is visible before you login again.

7 Synchronizing the System Time in the Network

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

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

The Simple Network Time Protocol (SNTP) is a simple solution for low accuracy requirements. Under ideal conditions, SNTP achieves an accuracy in the millisecond range. The accuracy depends on the signal delay.

IEEE 1588 with the Precision Time Protocol (PTP) achieves accuracies on the order of fractions of microseconds. This method is suitable even for demanding applications up to and including process control.

Examples of application areas include:
- Log entries
- Time stamping of production data
- Process control

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

7.1 Setting the time

If no reference clock is available, you have the option of entering the system time in a device and then using it like a reference clock (see on page 136 “Configuring SNTP”), (see on page 147 “Application Example”).

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

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

Thus the current time is available to you again, e.g. for log entries, when the device is started.
The hardware clock bridges a power supply downtime of 1 hour. The prerequisite is that the power supply of the device has been connected continually for at least 5 minutes beforehand.

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

☐ Open the `Time:Basic Settings` dialog.

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

- “System time (UTC)” displays the time determined using SNTP or PTP.
  The display is the same worldwide. Local time differences are not taken into account.

  Note: If the time source is PTP, consider that the PTP time uses the TAI time scale. TAI time is 34 s ahead of UTC time (as of 01.01.2011).
  If the UTC offset is configured correctly on the PTP reference clock, the device corrects this difference automatically when displaying “System time (UTC)”.
- The "System Time" uses "System Time (UTC)", allowing for the local time difference from "System Time (UTC)".
  "System Time" = "System Time (UTC)" + "Local Offset".
- Time Source displays the source of the following time data. The device automatically selects the source with the greatest accuracy. Possible sources are: `local`, `ptp` and `sntp`. The source is initially `local`.
  If PTP is activated and the device receives a valid PTP frame, it sets its time source to `ptp`. If SNTP is activated and if the device receives a valid SNTP packet, the device sets its time source to `sntp`. The device gives the PTP time source priority over SNTP.
- ☐ With "Set Time from PC", the device takes the PC time as the system time and calculates the "System Time (UTC)" using the local time difference.
  "System Time (UTC)" = "System Time" - "Local Offset"
- ☐ The "Local Offset" is for displaying/entering the time difference between the local time and the "System Time (UTC)".

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

`enable`	Switch to the privileged 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 "System Time (UTC)".

7.2 SNTP

7.2.1 Description of SNTP

The Simple Network Time Protocol (SNTP) enables you to synchronize the system time in your network.
The device supports the SNTP client and the SNTP server function.

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

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

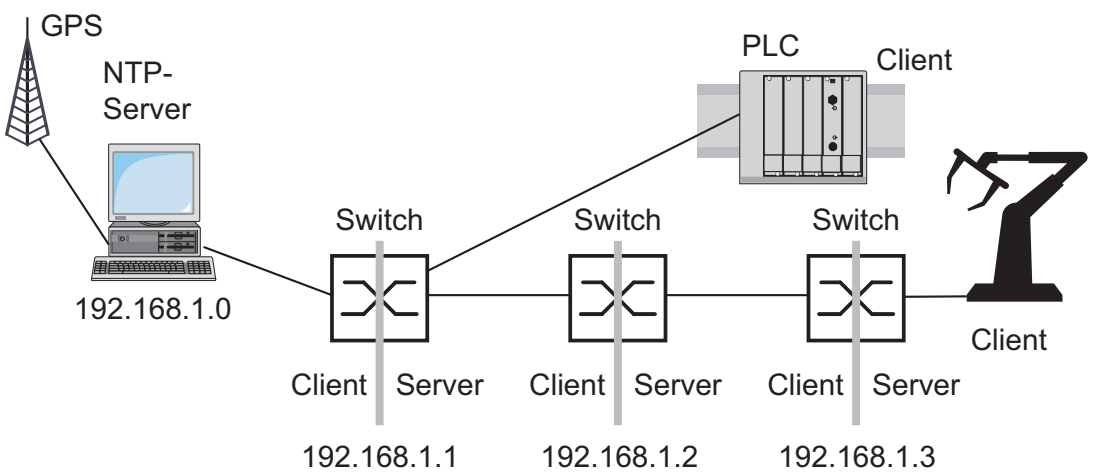


Figure 22: SNTP cascade

7.2.2 Preparing the SNTP Configuration

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

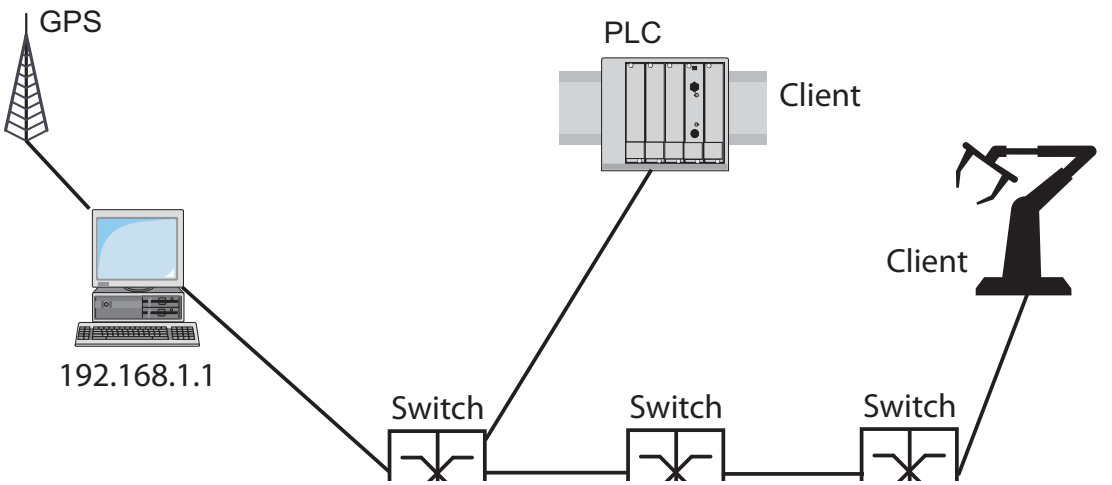


Figure 23: Example of SNTP cascade

☐ Enable the SNTP function on the devices whose time you want to set using SNTP.
The SNTP server of the device responds to Unicast requests as soon as it is enabled.

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

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

7.2.3 Configuring SNTP

☐ Select the `Time:SNTP` dialog.

▶ Operation

☐ In this frame you switch the SNTP function on/off globally.

▶ SNTP Status

☐ The “Status message” displays statuses of the SNTP client as one or more test messages, `e.g. Server 2 not responding`.

▶ Configuration SNTP Client

☐ In “Client status” you switch the SNTP client of the device on/off.

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

☐ In “Redundant server address” you enter the IP address of the SNTP server from which the device periodically requests the system time, if it does not receive a response to a request from the “External server address” within 1 second.

Note: If you are receiving the system time from an external/redundant server address, enter the dedicated server adress(es) and disable the setting `Accept SNTP Broadcasts` (see below). You thus ensure that the device uses the time of the server(s) entered and does not synchronize to broadcasts that might not be trustworthy.

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

☐ With “Accept SNTP Broadcasts” the device takes the system time from SNTP Broadcast/Multicast packets that it receives.

☐ With “Deactivate client after synchronization”, the device only synchronizes its system time with the SNTP server one time after the client status is activated, then it switches the client off.

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

SNTP server configuration

- ☐ In "Server-Status", switch the device's SNTP server on/off.
- ☐ In “Anycast destination address” you enter the IP address to which the SNTP server of the device sends its SNTP packets (see table 6).
- ☐ In "VLAN ID", enter the VLAN over which the device will be cyclically sending its SNTP packets.
- ☐ In “Anycast send interval” you specify the interval at which the device sends SNTP packets (valid entries: 1 s to 3600 s, on delivery: 120 s).
- ☐ With “Disable Server at local time source” the device disables the SNTP server function if the source of the time is `local` (see `Time` dialog).

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

Table 6: Destination address classes for SNTP and NTP packets

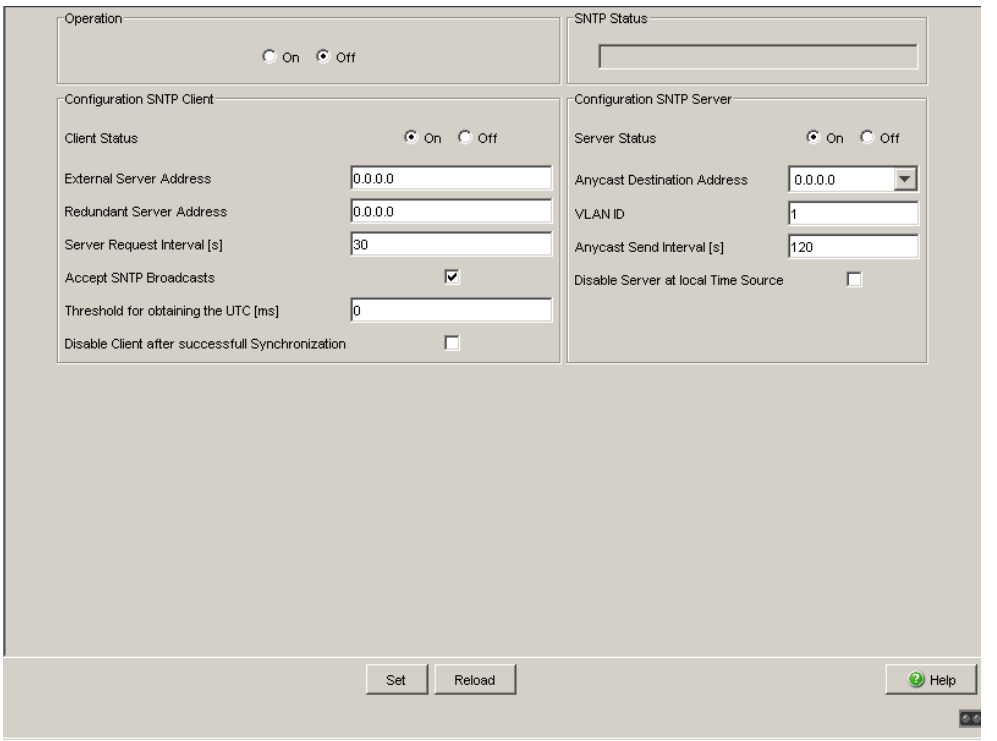


Figure 24: SNTP Dialog

Device	192.168.1.1	192.168.1.2	192.168.1.3
Operation	On	On	On
Server destination address	0.0.0.0	0.0.0.0	0.0.0.0
Server VLAN ID	1	1	1
Send interval	120	120	120
Client external server address	192.168.1.0	192.168.1.1	192.168.1.2
Request interval	30	30	30
Accept Broadcasts	No	No	No

Table 7: Settings for the example (see figure 23)

7.3 Precision Time Protocol

7.3.1 Description of PTP Functions

Precise time management is required for running time-critical applications via a LAN.
The IEEE 1588 standard with the Precision Time Protocol (PTP) describes a procedure that determines the best master clock in a LAN and thus enables precise synchronization of the clocks in this LAN.

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

Factors influencing precision are:

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

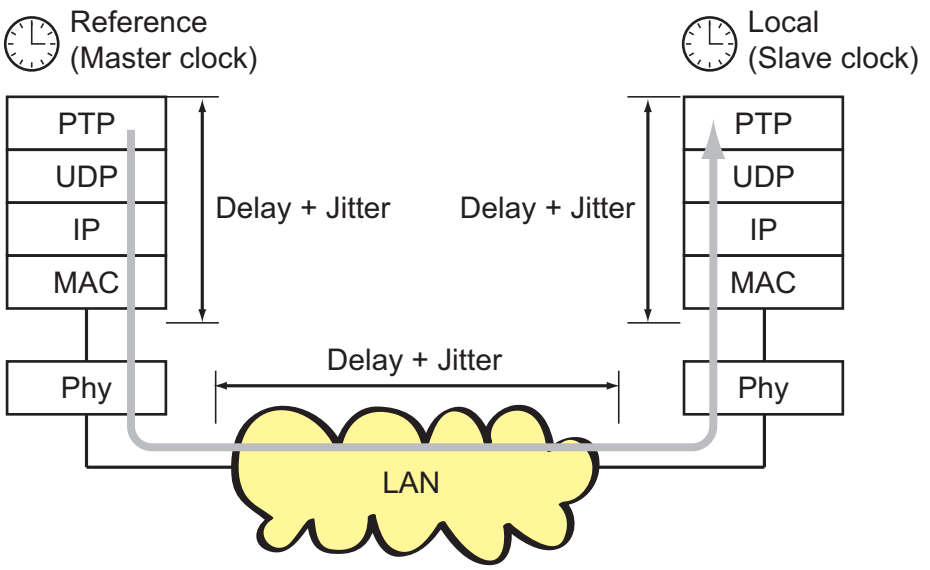
PTPv1 Stratum number	PTPv2 Clock class	Specification
0	– (priority 1 = 0)	For temporary, special purposes, in order to assign a higher accuracy to one clock than to all other clocks in the network.
1	6	Indicates the reference clock with the highest degree of accuracy. The clock can be both a boundary clock and an ordinary clock. Stratum 1/ clock class 6 clocks include GPS clocks and calibrated atomic clocks. A stratum 1 clock cannot be synchronized using the PTP from another clock in the PTP system.
2	6	Indicates the second-choice reference clock.

Table 8: Stratum – classifying the clocks

PTPv1 Stratum number	PTPv2 Clock class	Specification
3	187	Indicates the reference clock that can be synchronized via an external connection.
4	248	Indicates the reference clock that cannot be synchronized via an external connection. This is the standard setting for boundary clocks.
5–254	–	Reserved.
255	255	Such a clock should never be used as the so-called best master clock.

Table 8: Stratum – classifying the clocks

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



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

Figure 25: Delay and jitter for clock synchronization

To get around the delay and jitter in the protocol stack, IEEE 1588 recommends inserting a special hardware time stamp unit between the MAC and Phy layers.
Devices/modules with the “-RT” suffix in their names are equipped with this time stamp unit and support PTP version 1. Media modules MM23 and MM33 support PTP version 1 and PTP version 2.

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

With the introduction of PTP version 2, two procedures are available for the delay measurement:

- End-to-End (E2E)
  E2E corresponds to the procedure used by PTP version 1. Every slave clock measures only the delay to its master clock.
- Peer-to-Peer (P2P)
  With P2P, like in E2E, every slave clock measures the delay to its master clock. In addition, in P2P every master clock measures the delay to the slave clock. For example, if a redundant ring is interrupted, the slave clock can become the master clock and the master clock can become the slave clock. This switch in the synchronization direction takes place without any loss of precision, as with P2P the delay in the other direction is already known.

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

IEEE 1588 eliminates the inaccuracy caused by delays and jitter by defining boundary clocks. Boundary clocks are clocks integrated into devices. These clocks are synchronized on the one side of the signal path, and on the other side of the signal path they are used to synchronize the subsequent clocks (ordinary clocks).
PTP version 2 also defines what are known as transparent clocks. A transparent clock cannot itself be a reference clock, nor can it synchronize itself with a reference clock. However, it corrects the PTP messages it transmits by its own delay time and thus removes the jitter caused by the transmission. When cascading multiple clocks in particular, you can use transparent clocks to achieve greater time precision for the connected terminal devices than with boundary clocks

The Power Profile TLV Check is available on Mice, PowerMICE, MACH1040, MACH104 devices. When enabled this function checks for the presents of Power TLVs. Use the following worksteps to enable the device to check for announce messages containing Power Profile TLVs and use the TLVs for syntonization:

☐ Open the `Time:PTP:Version 2(TC):Global` dialog.

☐ Select the "Power TLV Check" checkbox

☐ Select the "Syntonize" checkbox

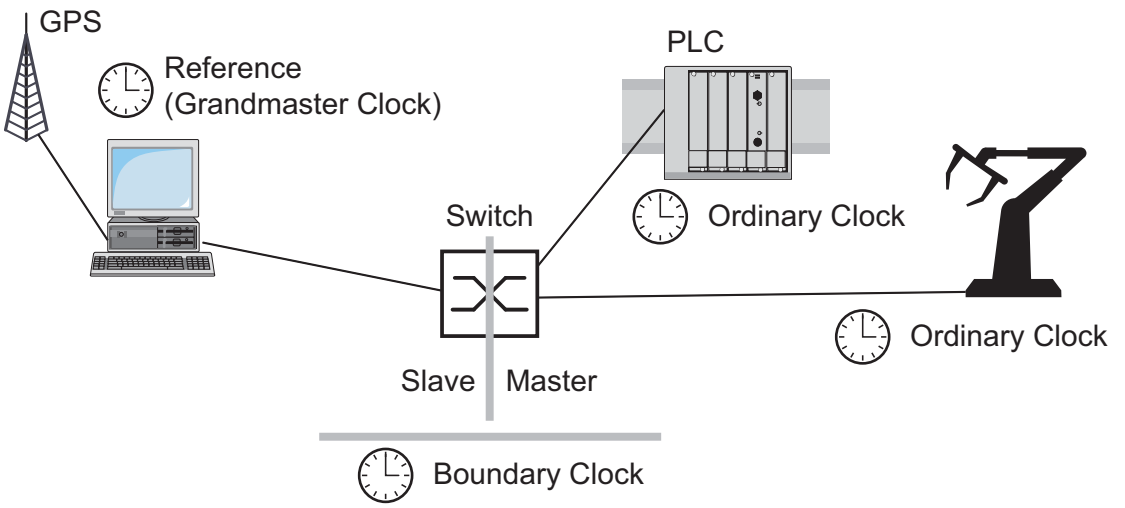


Figure 26: Position of the boundary clock in a network

Irrespective of the physical communication paths, the PTP allocates logical communication paths which you define by setting up PTP subdomains. The purpose of subdomains is to form groups of clocks which are chronologically independent from the other domains. The clocks in one group typically use the same communication paths as other clocks.

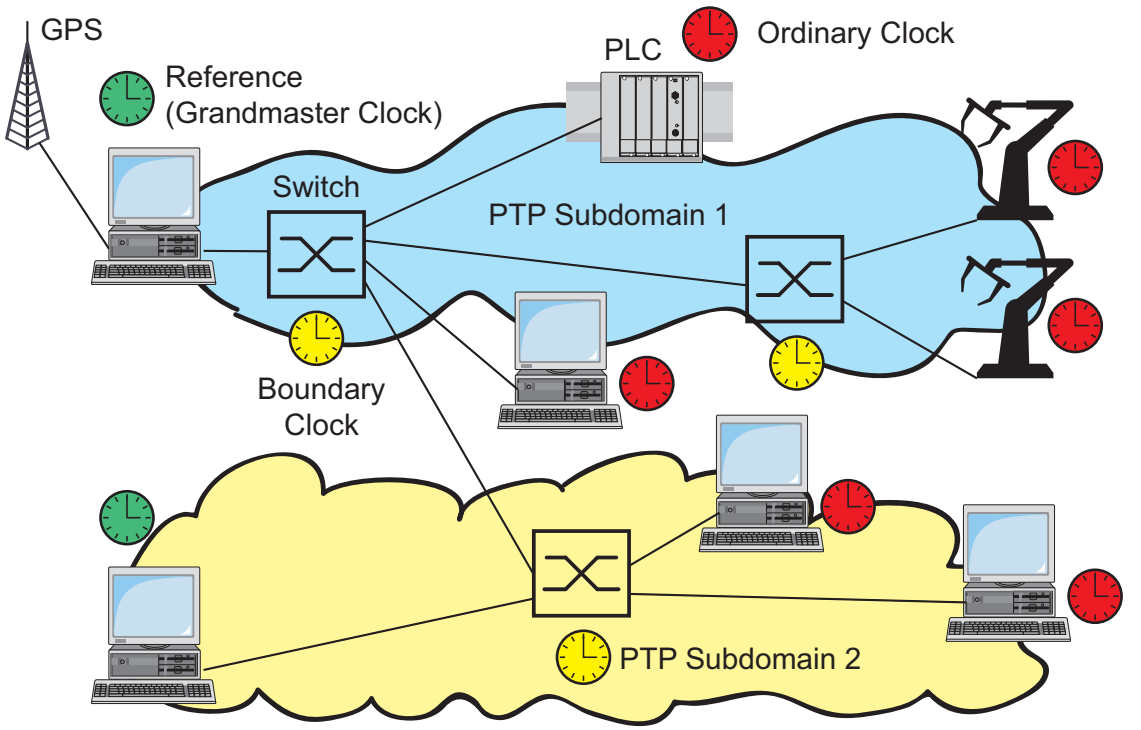


Figure 27: PTP subdomains

7.3.2 Preparing the PTP Configuration

After the function is activated, the PTP takes over the configuration automatically.

☐ To gain an overview of the distribution of clocks, draw a network plan with the devices involved in PTP.

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

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

☐ Select the PTP version and the PTP mode. Select the same PTP version for all the devices that you want to synchronize.

PTP mode	Application
v1-simple-mode	Support for PTPv1 without special hardware. The device synchronizes itself with received PTPv1 messages. Select this mode for devices without a timestamp unit (RT module).
v1-boundary-clock	Boundary Clock function based on IEEE 1588-2002 (PTPv1).
v2-boundary-clock-onestep	Boundary Clock function based on IEEE 1588-2008 (PTPv2) for devices with MM23 and MM33 media modules. The one-step mode determines the precise PTP time with one message.
v2-boundary-clock-twostep	Boundary Clock function based on IEEE 1588-2008 (PTPv2) for devices with RT modules. The two-step mode determines the precise PTP time with two messages.

Table 9: Selecting a PTP mode

PTP mode	Application
v2-simple-mode	Support for PTPv2 without special hardware. The device synchronizes itself with received PTPv2 messages. Select this mode for devices without a timestamp unit (RT module).
v2-transparent-clock	Transparent Clock (one-step) function based on IEEE 1588-2008 (PTPv2) for devices with MM23 and MM33 media modules.

Table 9: Selecting a PTP mode

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

7.3.3 Application Example

PTP is used to synchronize the time in the network. As an SNTP client, the left device (see figure 28) gets the time from the NTP server via SNTP. The device assigns PTP clock stratum 2 (PTPv1) or clock class 6 (PTPv2) to the time received from an NTP server. Thus the left device becomes the reference clock for the PTP synchronization and is the “preferred master”. The “preferred master” forwards the exact time signal via its connections to the RT module. The device with the RT module receives the exact time signal at a connection of its RT module and thus has the clock mode “v1-boundary-clock”. The devices without an RT module have the clock mode “v1-simple-mode”.

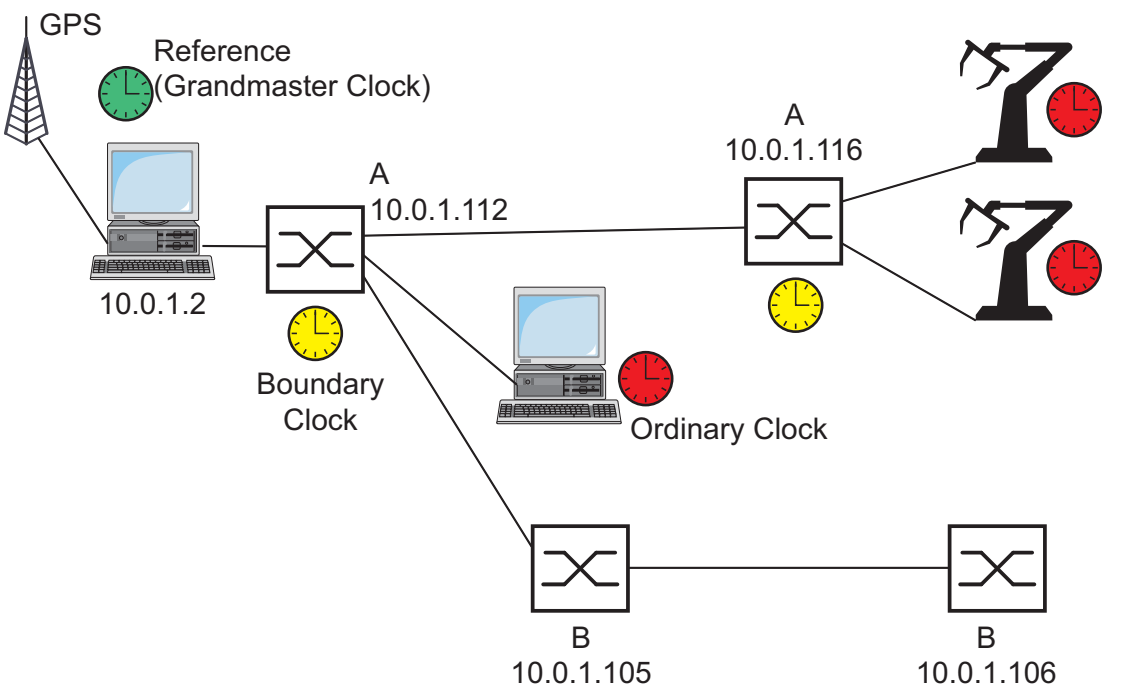


Figure 28: Example of PTP synchronization
A: Device with RT module
B: Device without RT module:

Device	10.0.1.112	10.0.1.116	10.0.1.105	10.0.1.106
PTP Global				
Operation	on	on	on	on
Clock Mode	v1-boundary-clock	v1-boundary-clock	v1-simple-mode	v1-simple-mode
Preferred Master	true	false	false	false
SNTP				
Operation	on	off	off	off
Client Status	on	off	off	off
External server address	10.0.1.2	0.0.0.0	0.0.0.0	0.0.0.0
Server request interval	30	any	any	any
Accept SNTP Broadcasts	No	any	any	any
Server status	on	off	off	off
Anycast destination address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
VLAN ID	1	1	1	1

Table 10: Settings for the example (see figure 28)

The following configuration steps apply to the device with the IP address 10.0.1.112. Configure the other devices in the same way with the values from the table above.

☐ Enter the SNTP parameters.

☐ Select the `Time:SNTP` dialog.
☐ Activate SNTP globally in the “Operation” frame.
☐ Activate the SNTP client (client status) in the “Configuration SNTP Client” frame.
☐ In the “Configuration SNTP Client” frame, enter:
– “External server address”: 10.0.1.2
– “Request interval”: 30
– “Accept SNTP Broadcasts”: No

☐ Activate the SNTP server (server status) in the “Configuration SNTP Server” frame.
☐ In the “Configuration SNTP Server” frame, enter:
– “Anycast destination address”: 0.0.0.0
– “VLAN ID”: 1
☐ Click "Set" to save the changes temporarily.

`enable`	Change to the privileged EXEC mode.
`configure`	Change to the Configuration mode.
`sntp operation on`	Switch on SNTP globally.
`sntp operation client on`	Switch on SNTP client.
`sntp client server primary 10.0.1.2`	Enter the IP address of the external SNTP server 10.0.1.2.
`sntp client request-interval 30`	Enter the value 30 seconds for the SNTP server request interval.
`sntp client accept-broadcast off`	Deactivate “Accept SNTP Broadcasts”.
`sntp operation server on`	Switch on SNTP server.
`sntp anycast address 0.0.0.0`	Enter the SNTP server Anycast destination address 0.0.0.0.
`sntp anycast vlan 1`	Enter the SNTP server VLAN ID 1.

☐ Enter the global PTP parameters.

☐ Select the `Time:PTP:Global` dialog.
☐ Activate the function in the “Operation IEEE 1588 / PTP” frame.
☐ Select `v1-boundary-clock` for “PTP version mode”.
☐ Click "Set" to save the changes temporarily.

`ptp operation enable`	Switch on PTP globally.
`ptp clock-mode v1-boundary-clock`	Select PTP version and clock mode.

☐ In this example, you have chosen the device with the IP address 10.0.1.112 as the PTP reference clock. You thus define this device as the “Preferred Master”.

☐ Select the `Time:PTP:Version1:Global` dialog.
☐ In the “Operation IEEE 1588 / PTP” frame, select `true` for the “Preferred Master”.
☐ Click "Set" to save the changes temporarily.

`ptp v1 preferred-master true` Define this device as the “Preferred Master”.

☐ Get PTP to apply the parameters.

☐ In the `Time:PTP:Version1:Global` dialog, click on “Reinitialize” so that PTP applies the parameters entered.

`ptp v1 re-initialize` Apply PTP parameters.

☐ Save the settings in the non-volatile memory.

☐ Select the `Basics: Load/Save` dialog.

☐ In the “Save” frame, select “To Device” for the location and click “Save” to permanently save the configuration in the active configuration.

`copy system:running-config nvram:startup-config`	Save the current configuration to the non-volatile memory.

7.4 Interaction of PTP and SNTP

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

Note: Configure the devices so that each device only receives the time from one source.
If the device gets its time via PTP, you enter the “External server address” 0.0.0.0 in the SNTP client configuration and do not accept SNTP Broadcasts.
If the device gets its time via SNTP, make sure that the “best” clock is connected to the SNTP server. Then both protocols will get the time from the same server. The example (see figure 29) shows such an application.

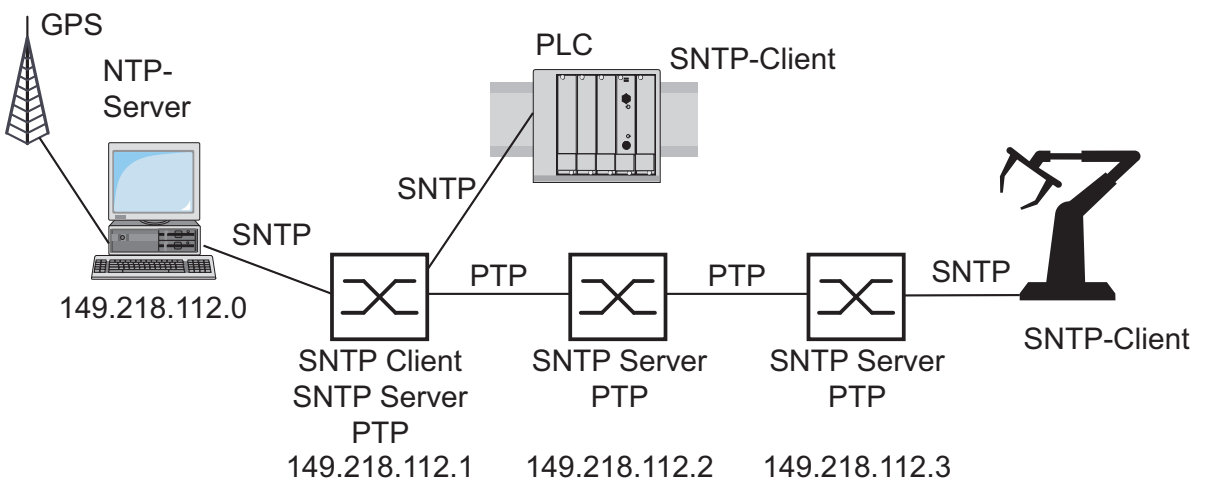


Figure 29: Example of the coexistence of PTP and SNTP

Application Example

The requirements with regard to the accuracy of the time in the network are quite high, but the terminal devices only support SNTP (see figure 29).

Device	149.218.112.1	149.218.112.2	149.218.112.3
PTP			
Operation	on	on	on
Clock Mode	v1-boundary-clock	v1-boundary-clock	v1-boundary-clock
Preferred Master	false	false	false
SNTP			
Operation	on	on	on
Client Status	on	off	off
External server address	149.218.112.0	0.0.0.0	0.0.0.0
Server request interval	any	any	any
Accept SNTP Broadcasts	No	No	No
Server status	on	on	on
Anycast destination address	224.0.1.1	224.0.1.1	224.0.1.1
VLAN ID	1	1	1
Anycast send interval	30	30	30

Table 11: Settings for the example

In the example, the left device, as an SNTP client, gets the time from the NTP server via SNTP. The device assigns PTP clock stratum 2 (PTPv1) or clock class 6 (PTPv2) to the time received from an NTP server. Thus the left device becomes the reference clock for the PTP synchronization. PTP is active for all 3 devices, thus enabling precise time synchronization between them. As the connectable terminal devices in the example only support SNTP, all 3 devices act as SNTP servers.

8 Network Load Control

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

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

8.1 Direct Packet Distribution

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

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

8.1.1 Store and Forward

The device stores receive data and checks the validity. The device rejects invalid and defective data packets (> 1522 bytes or CRC errors) as well as fragments (> 64 bytes). The device then forwards valid data packets.

8.1.2 Multi-Address Capability

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

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

in the destination address field are sent to this port. The device enters learned source addresses in its filter table (see on page 158 “Entering Static Addresses”).

The device can learn up to 8,000 addresses. This is necessary if more than one terminal device is connected to one or more ports. It is thus possible to connect several independent subnets to the device.

8.1.3 Aging of learned MAC addresses

The device monitors the age of the learned addresses. Address entries which exceed a particular age - the aging time - are deleted by the device from its address table.
Data packets with an unknown destination address are flooded by the device.
Data packets with known destination addresses are selectively transmitted by the device.

Note: A reboot deletes the learned address entries.

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

8.1.4 Entering Static Addresses

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

The following are valid filter criteria:

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

The individual filters are stored in the filter table (Forwarding Database, FDB). It consists of 3 parts: a static part and two dynamic parts.

- The management administrator describes the static part of the filter table (`dot1qStaticTable`).
- During operation, the device is capable of learning which of its ports receive data packets from which source address (see on page 156 “Multi-Address Capability”). This information is written to a dynamic part (`dot1qTpFdbTable`).
- Addresses learned dynamically from neighboring agents and those learned via GMRP are written to the other dynamic part.

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

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

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

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

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

- `learned`: The filter was created automatically by the device.
- `permanent`: The filter is stored permanently in the device or on the URL (see on page 67 “Saving settings”)
- `invalid`: With this status you delete a manually created filter.
- `gmrp`: The filter was created by GMRP.
- `gmrp/permanent`: GMRP added further port markings to the filter after it was created by the administrator. The port markings added by the GMRP are deleted by a restart.
- `igmp`: The filter was created by IGMP Snooping.

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

8.1.5 Disabling the Direct Packet Distribution

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

☐ Select the `Switching:Global` dialog.

- UnCheck "Address Learning" to observe the data at all ports.

8.2 Multicast Application

8.2.1 Description of the Multicast Application

The data distribution in the LAN differentiates between 3 distribution classes on the basis of the addressed recipients:

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

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

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

- MAC Multicast Address
  01:00:5E:00:00:00 - 01:00:5E:FF:FF:FF
  (in mask form 01:00:5E:00:00:00/24)
- Class D IP Multicast address
  224.0.0.0 - 239.255.255.255
  (in mask form 224.0.0.0/4)

8.2.2 Example of a Multicast Application

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

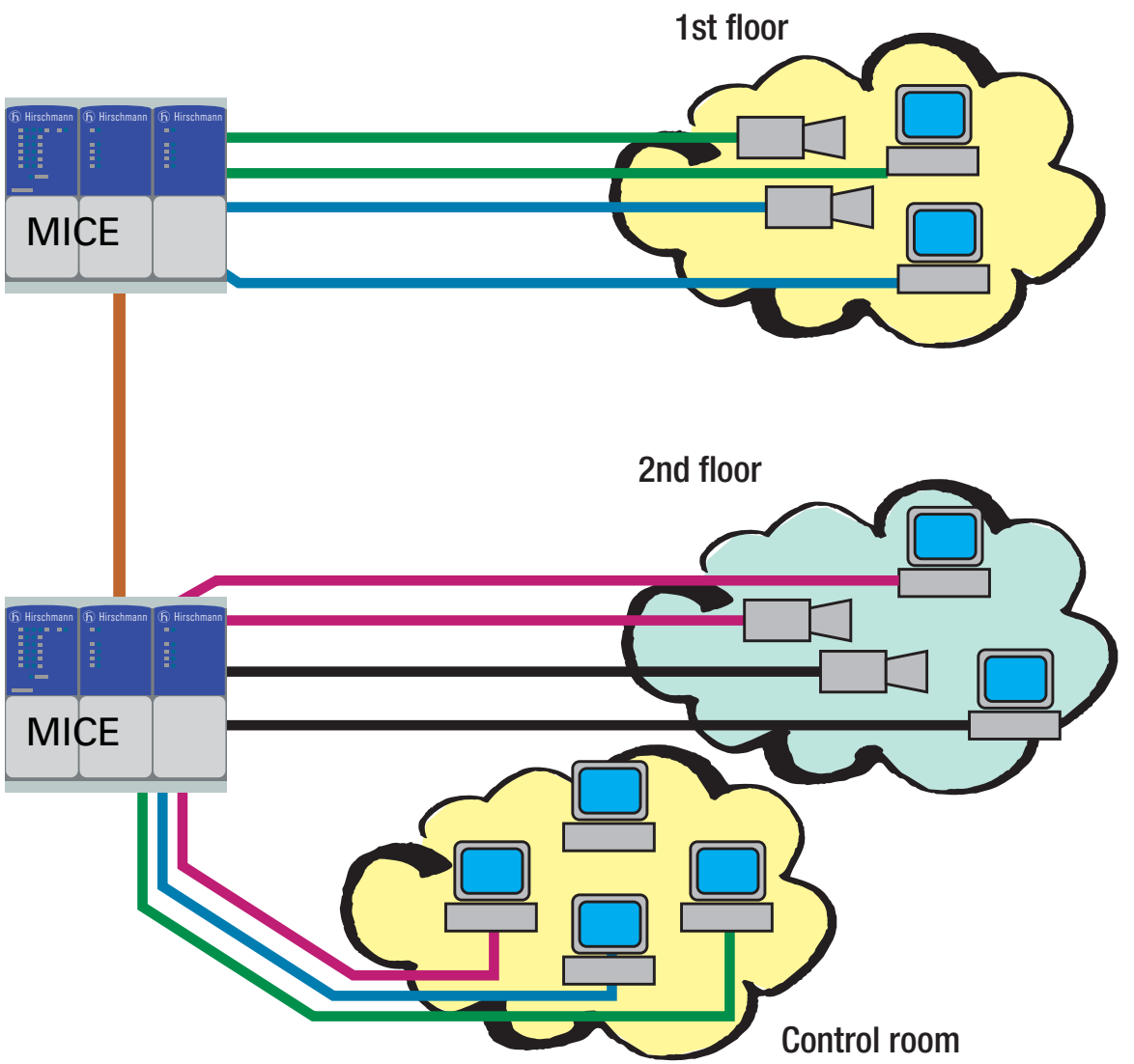


Figure 30: Example: Video surveillance in machine rooms

8.2.3 Description of IGMP Snooping

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

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

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

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

A Switch that connects a Multicast receiver with a router can evaluate the IGMP information using the IGMP Snooping procedure.

IGMP Snooping translates IP Multicast group addresses into MAC Multicast addresses, so that the IGMP functions can also be used by Layer 2 Switches. The Switch records the MAC addresses of the Multicast receivers, with are obtained via IGMP Snooping from the IP addresses, in the static address table. The Switch thus transmits these Multicast packets exclusively at the ports at which Multicast receivers are connected. The other ports are not affected by these packets.

A special feature of the device is that you can specify whether it should drop data packets with unregistered Multicast addresses, transmit them to all ports, or only to those ports at which the device received query packets. You also have the option of additionally sending known Multicast packets to query ports.

Default setting: “Off”.

8.2.4 Setting IGMP Snooping

☐ Select the `Switching:Multicast:IGMP` dialog.

Operation

The “Operation” frame allows you to enable/disable IGMP Snooping globally for the entire device.
If IGMP Snooping is disabled, then

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

Settings for IGMP Querier and IGMP

With these frames you can enter global settings for the IGMP settings and the IGMP Querier function.
Prerequisite: The IGMP Snooping function is activated globally.

IGMP Querier

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

“Protocol version” allow you to select IGMP version 1, 2 or 3.

In “Send interval [s]” you specify the interval at which the device sends query packets (valid entries: 2-3,599 s, default setting: 125 s).

Note the connection between the parameters Max. Response Time, Send Interval and Group Membership Interval (see on page 165 “Parameter Values”).

IGMP-capable terminal devices respond to a query with a report message, thus generating a network load.
Select large sending intervals if you want to reduce the load on your network and can accept the resulting longer switching times.
Select small sending intervals if you require short switching times and can accept the resulting network load.

IGMP Settings

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

In “Max. Response Time” you specify the period within which the Multicast group members respond to a query (valid values: 1-3,598 s, default setting: 10 s).

Note the connection between the parameters Max. Response Time, Send Interval and Group Membership Interval (see on page 165 “Parameter Values”).

The Multicast group members select a random value within the maximum response time for their response, to prevent all the Multicast group members responding to the query at the same time.
Select a large value if you want to reduce the load on your network and can accept the resulting longer switching times.
Select a small value if you require short switching times and can accept the resulting network load.
In “Group Membership Interval” you specify the period for which a dynamic Multicast group remains entered in the device if it does not receive any report messages (valid values: 3-3,600 s, default setting: 260 s).

Note the connection between the parameters Max. Response Time, Send Interval and Group Membership Interval (see on page 165 “Parameter Values”).

Parameter Values

The parameters
– Max. Response Time,
– Transmit Interval and
– Group Membership Interval
have a relationship to one another:

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

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

Parameter	Protocol Version	Value Range	Default Setting
Max. Response Time	1, 2 3	1-25 seconds 1-3,598 seconds	10 seconds
Transmit Interval	1, 2, 3	2-3,599 seconds	125 seconds
Group Membership Interval	1, 2, 3	3-3,600 seconds	260 seconds

Table 12: Value range for Max. Response Time, Transmit Interval and Group Membership Interval

Multicasts

With these frames you can enter global settings for the Multicast functions.
Prerequisite: The IGMP Snooping function is activated globally.

Unknown Multicasts

In this frame you can determine how the device in IGMP mode sends packets with known and unknown MAC/IP Multicast addresses that were not learned through IGMP Snooping..

“Unknown Muilticasts” allows you to specify how the device transmits unknown Multicast packets:

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

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

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

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

Settings per Port (Table)

- “IGMP on”
  This table column enables you to enable/disable the IGMP for each port when the global IGMP Snooping is enabled. Port registration will not occur if IGMP is disabled.

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

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

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

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

- "Static Query Port“
  The device sends IGMP Report messages to the ports on which it receives IGMP requests (disabled=as-delivered state).
  This table column also lets you send IGMP Report messages to:
  other selected ports (enable) or
  connected Hirschmann devices (automatic).

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

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

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

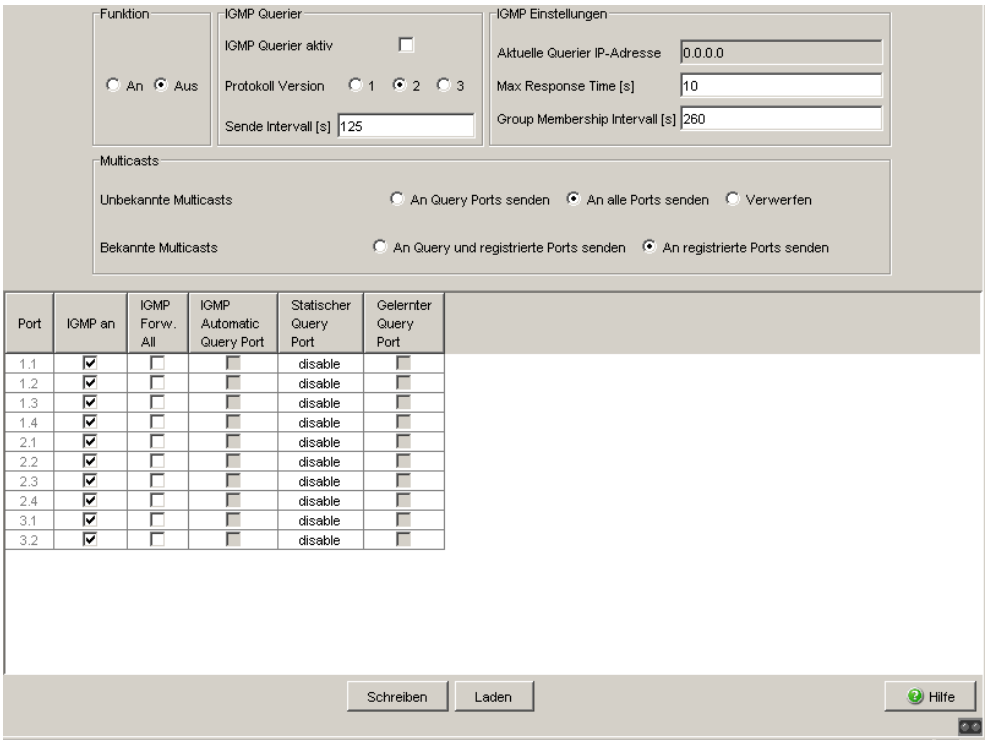


Figure 31: IGMP Snooping dialog

8.2.5 Description of GMRP

The GARP Multicast Registration Protocol (GMRP) describes the distribution of data packets with a multicast address as the destination address on Layer 2.

Devices that want to receive data packets with a multicast address as the destination address use the GMRP to perform the registration of the multicast address. For a switch, registration involves entering the multicast addresses in the filter table. When you enter a multicast address in the filter table, the switch sends this information in a GMRP packet to the ports. As a result, the connected switches forward the multicast address entered in the filter table to this switch. The GMRP sends packets with a Multicast address in the destination address field to the ports entered.

The feature is available on MS, RS, MACH102, MACH1020/30, Octopus, RSR and MACH1040, MACH104 devices. Depending on the configuration, the switch either discards unknown multicast addresses, or sends the data packets with unknown multicast addresses to the ports.

Default setting: “Off”.

8.2.6 Setting GMRP

☐ Select the `Switching:Multicasts:GMRP` dialog.

Operation

The “Operation” frame allows you to enable GMRP globally for the entire device.

If GMRP is disabled, then

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

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

Multicasts

The "Multicasts" frame allows you to configure GMRP to discard multicasts addresses or send them to the ports.

Enable GMRP, then:

- when you select "Discard", the device deletes unknown multicasts
- when you select "Send To All Ports", the device evaluates the GMRP packets received, and sends (floods) received data packets to the ports.

Settings per Port (Table)

- „GMRP”
  This table column enables you to enable/disable the GMRP for each port when the GMRP is enabled globally. When you switch off the GMRP at a port, no registrations can be made for this port, and GMRP packets cannot be forwarded at this port.

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

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

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

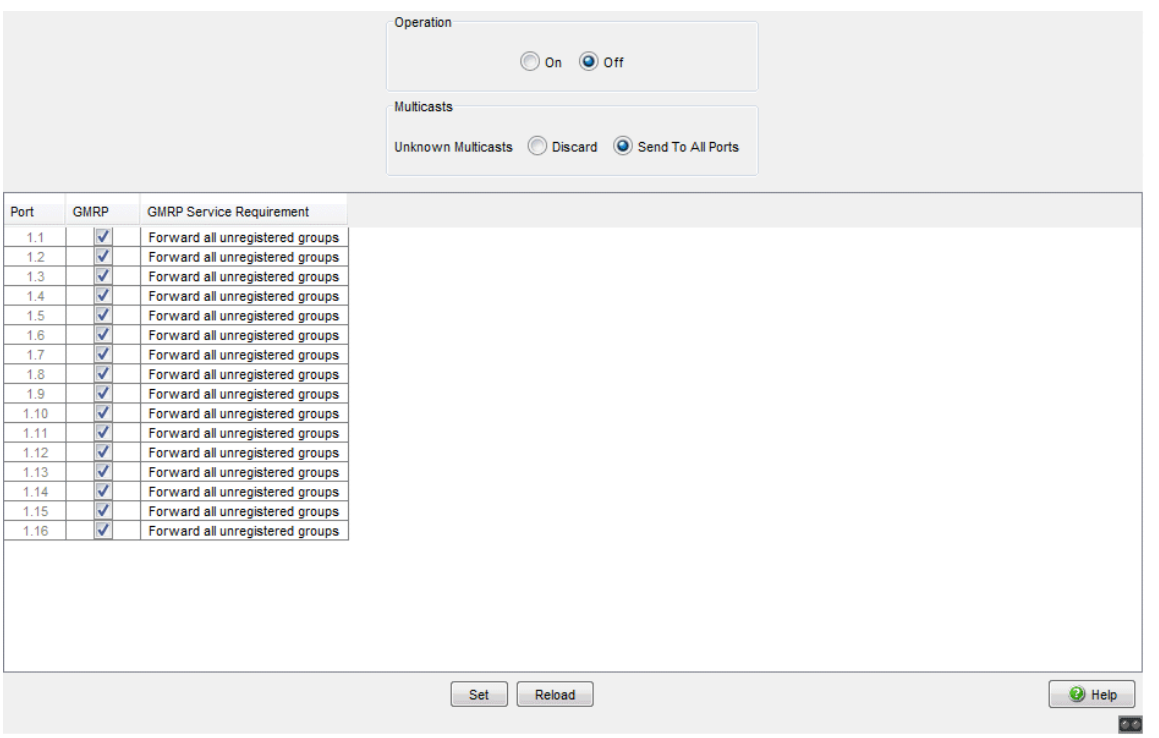


Figure 32: Multicasts dialog

8.3 Rate Limiter

8.3.1 Description of the Rate Limiter

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

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

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

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

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

To minimize these effects, use the following options:

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

8.3.2 Rate limiter settings

☐ Select the `Switching:Rate Limiter` dialog.

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

Setting options per port:

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

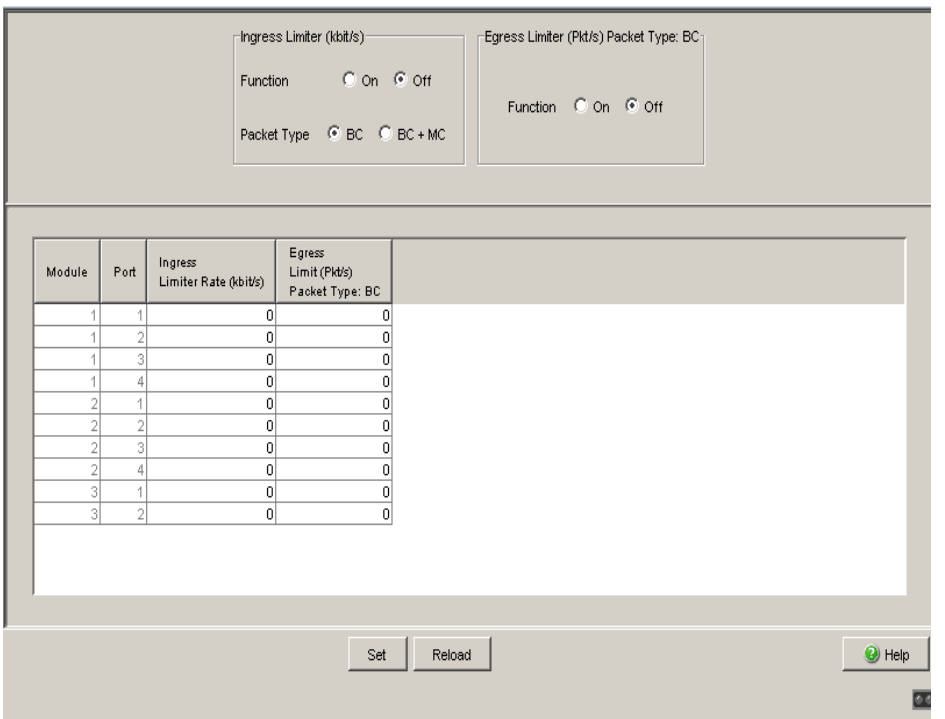


Figure 33: Rate Limiter dialog

8.4 QoS/Priority

8.4.1 Description of Prioritization

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

The device supports 8 priority queues (IEEE 802.1D standard traffic classes). Received data packets are assigned to these classes by

- Access Control Lists, MAC- or IP-based ACLs (see on page 116 “Access Control Lists (ACL)”).
- the priority of the data packet contained in the VLAN tag when the receiving port was configured to “trust dot1p”.
- the QoS information (ToS/DiffServ) contained in the IP header when the receiving port was configured to “trust ip-dscp”.
- the port priority when the port was configured to “untrusted”.
- the port priority when receiving non-IP packets when the port was configured to “trust ip-dscp”.
- the port priority when receiving data packets without a VLAN tag (see on page 87 “Configuring the Ports”) and when the port was configured to “trust dot1p”.
  Default setting: “trust dot1p”.

The device takes account of the classification mechanisms in the above order. This means that the Access-Control Lists always take priority over the following mechanisms. AccessControl Lists can classify the data packets relative to Layer 2, Layer 3 and Layer 4 (e.g. MAC addresses, IP addresses, protocols, TCP/UDP ports).

Data packets can contain prioritizing/QoS information:

- VLAN priority based on IEEE 802.1Q/ 802.1D (Layer 2)
- Type of Service (ToS) or DiffServ (DSCP) for IP packets (Layer 3)

8.4.2 VLAN tagging

The VLAN tag is integrated into the MAC data frame for the VLAN and Prioritization functions in accordance with the IEEE 802 1Q standard. The VLAN tag consists of 4 bytes. It is inserted between the source address field and the type field.

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

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

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

Table 13: Assignment of the priority entered in the tag to the traffic classes

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

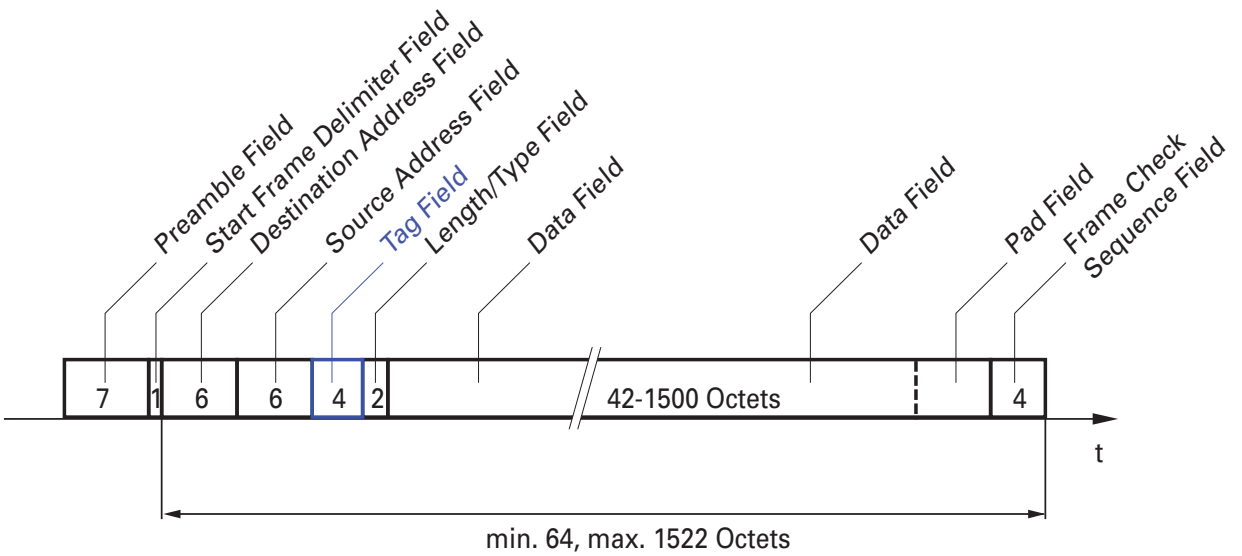


Figure 34: Ethernet data packet with tag

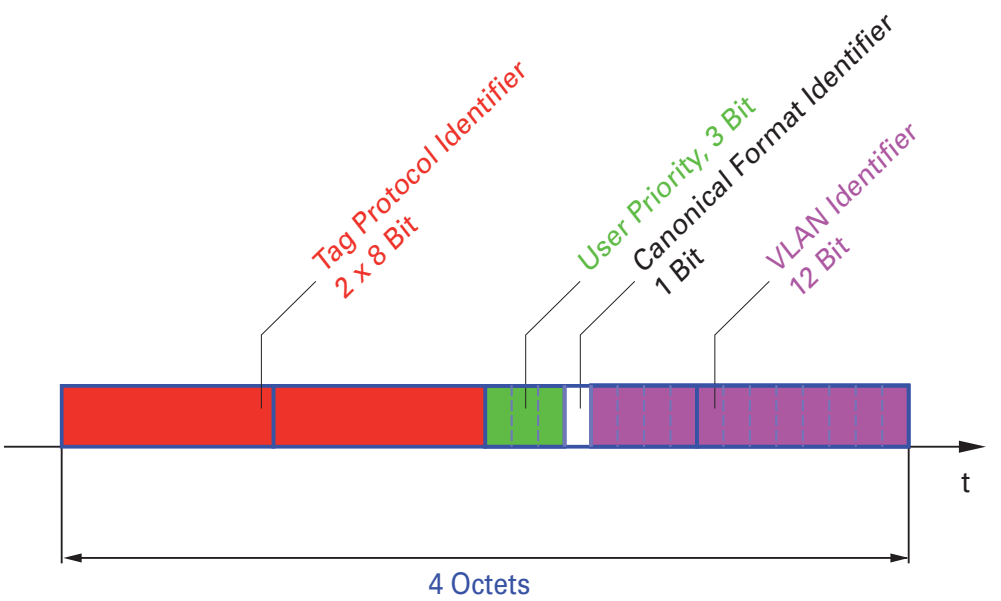


Figure 35: Tag format

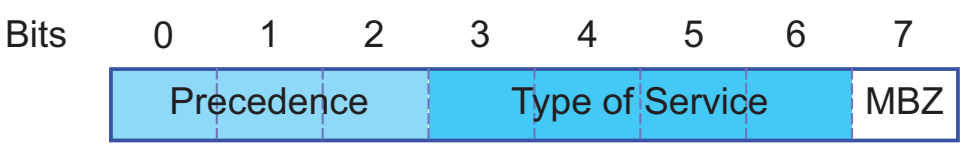
When using VLAN prioritizing, note the following special features:

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

8.4.3 IP ToS / DiffServ

TYPE of Service

The Type of Service (ToS) field in the IP header (see table 14) has been part of the IP protocol from the start, and it is used to differentiate various services in IP networks. Even back then, there were ideas about differentiated treatment of IP packets, due to the limited bandwidth available and the unreliable connection paths. Because of the continuous increase in the available bandwidth, there was no need to use the ToS field. Only with the real-time requirements of today's networks has the ToS field become significant again. Selecting the ToS byte of the IP header enables you to differentiate between different services. However, this field is not widely used in practice.



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

Table 14: ToS field in the IP header

Bits (0-2): IP Precedence Defined	Bits (3-6): Type of Service Defined	Bit (7)
010 - Immediate		
001 - Priority		
000 - Routine		

Table 14: ToS field in the IP header

Differentiated Services

The Differentiated Services field in the IP header (see figure 36) newly defined in RFC 2474 - often known as the DiffServ code point or DSCP - replaces the ToS field and is used to mark the individual packets with a DSCP. Here the packets are divided into different quality classes. The first 3 bits of the DSCP are used to divide the packets into classes. The next 3 bits are used to further divide the classes on the basis of different criteria. In contrast to the ToS byte, DiffServ uses 6 bits for the division into classes. This results in up to 64 different service classes.

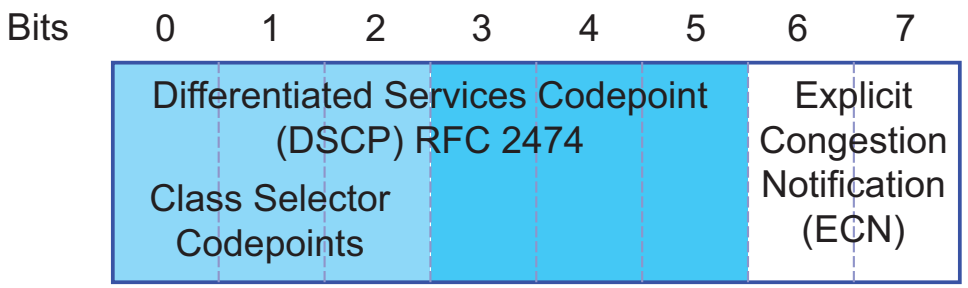


Figure 36: Differentiated Services field in the IP header

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

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

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

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

Table 15: Assigning the IP precedence values to the DSCP value

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

Table 16: Mapping the DSCP values onto the traffic classes

8.4.4 Management prioritization

To have full access to the management of the device, even in situations of high network load, the device enables you to prioritize management packets. In prioritizing management packets (SNMP, SSH, etc.), the device sends the management packets with priority information.

- On Layer 2 the device modifies the VLAN priority in the VLAN tag.
  For this function to be useful, the configuration of the corresponding ports must permit the sending of packets with a VLAN tag.
- On Layer 3 the device modifies the IP-DSCP value.

8.4.5 Handling of Received Priority Information

The device offers the following options for evaluating this priority information:

- trust dot1p
  The device assigns VLAN-tagged packets to the different traffic classes according to their VLAN priorities. The assignment is based on the pre-defined table (see on page 176 “VLAN tagging”). You can modify this assignment. The device assigns the port priority to packets that it receives without a tag.
- untrusted
  The device ignores the priority information in the packet and always assigns the packets the port priority of the receiving port.
- trust ip-dscp
  The device assigns the IP packets to the different traffic classes according to the DSCP value in the IP header, even if the packet was also VLAN-tagged. The assignment is based on the pre-defined values (see table 16). You can modify this assignment.
  The device prioritizes non-IP packets according to the port priority.

8.4.6 Handling of traffic classes

For the handling of traffic classes, the device provides:

- Strict Priority
- Weighted Fair Queuing
- Strict Priority combined with Weighted Fair Queuing

Default setting: Strict Priority.

Description of Strict Priority

With the Strict Priority setting, the device first transmits data packets that have a higher traffic class (higher priority) before transmitting a data packet with the next highest traffic class. The device transmits a data packet with the lowest traffic class (lowest priority) when there are no other data packets remaining in the queue. In unfortunate cases, the device never sends packets with a low priority if there is a high volume of high-priority traffic waiting to be sent on this port.
In applications that are time- or latency-critical, such as VoIP or video, Strict Priority enables high-priority data to be sent immediately(see on page 183 “Maximum bandwidth”).

Description of Weighted Fair Queuing

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

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

- A weighting of 0 is equivalent to a "no bandwidth" setting.
- The sum of the individual bandwidths may add up to 100%.

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

When you combine Weighted Fair Queuing with Strict Priority, make sure that the highest traffic class of Weighted Fair Queuing is smaller than the lowest traffic class of Strict Priority.
In this case, a high Strict Priority network load can significantly reduce the bandwidth available for Weighted Fair Queuing.

Maximum bandwidth

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

- Weighted Fair Queuing (see on page 182 “Description of Weighted Fair Queuing”) requires that the maximum bandwidth is at least as big as the minimum bandwidth.
- With “Strict Priority”, individual high-priority packets with low latency are processed (see on page 182 “Description of Strict Priority”). If the maximum bandwidth is configured to a value less than 100%, even data packets with lower traffic classes can be sent in periods of high-priority overloading.
  The weighting values range from 0% to 100% of the available bandwidth, in steps of 5%.

Description of Traffic Shaping

With Traffic Shaping you have the option of restricting the maximum bandwidth of an interface.

The values for the bandwidth restriction range from 0% to 95%, in steps of 5%.

- The value "0" is equivalent to a "no bandwidth restriction" setting.
- The value "95" means that 95% of the bandwidth is available.

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

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

8.4.7 Setting prioritization

Assigning the Port Priority

- ☐ Select the `QoS/Priority:Port Configuration` dialog.
- ☐ In the “Port Priority” column, you can specify the priority (0-7) with which the device sends data packets which it receives without a VLAN tag at this port.
- ☐ In the column "Trust Mode“, you have the option to control which criterion the the device uses to assign a traffic class to received data packets (see on page 175 “Description of Prioritization”).

Note: If you have set up VLANs, pay attention to the “VLAN 0 Transparent mode” (see `Switching:VLAN:Global`)

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`interface 1/1`	Switch to the Interface Configuration mode of interface 1/1.
`vlan priority 3`	Assigns port priority 3 to interface 1/1.
`exit`	Switch to the Configuration mode.

Assigning VLAN priority to a traffic class

- ☐ Select the `QOS/Priority:802.1D/p-Mapping` dialog.
- ☐ In the "Traffic Class" column, enter the desired values.

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`classofservice dot1p-mapping 0 2`	Assign traffic class 2 to VLAN priority 0.
`classofservice dot1p-mapping 1 2`	Also assign traffic class 2 to VLAN priority 1.
`exit`	Switch to the privileged EXEC mode.
`show classofservice dot1p-mapping`	Display the assignment.

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

Always assign port priority to received data packets (PowerMICE, MACH 104, MACH 1040 and MACH 4000)

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`interface 1/1`	Switch to the Interface Configuration mode of interface 1/1.
`no classofservice trust vlan 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 privileged 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

☐ Select the `QOS/Priority:IP DSCP Mapping` dialog.
☐ In the "Traffic Class" column, enter the desired values.

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

```
show classofservice ip-dscp-mapping

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

Always assign DSCP priority per interface to received IP data packets (PowerMICE, MACH 104, MACH 1040 and MACH 4000)

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`interface 6/1`	Switch to the interface configuration mode of interface 6/1.
`classofservice trust ip-dscp`	Assign the “trust ip-dscp” mode to the interface.
`exit`	Switch to the Configuration mode.
`exit`	Switch to the privileged EXEC mode.
`show classofservice trust 6/1`	Display the trust mode on interface 6/1.

```
Class of Service Trust Mode: IP DSCP

Non-IP Traffic Class: 2
```

Always assign the DSCP priority to received IP data packets globally

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

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

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

Configuration of Weighted Fair Queuing and Traffic Shaping

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`no cos-queue strict 0 1 2 3 4 5`	Switches off Strict Priority for traffic classes 0 to 5 and thus switches on Weighted Fair Queuing. Traffic classes 6 and 7 remain in Strict Priority mode.
`cos-queue min-bandwidth 10 10 15 15 20 30 0 0`	Assigns the weighting to the Weighted Fair Queuing traffic classes. In the case of Strict Priority, because the device first transmits all the data packets with a high priority, you can enter the weighting 0 for the Strict Priority traffic classes and distribute 100% among the remaining traffic classes. The device distributes the remaining bandwidth in accordance with the percentage weighting.
`cos-queue max-bandwidth 20 20 20 20 20 30 30 30`	Assign a maximum bandwidth to all traffic classes (Shaping). Because the two Strict Priority traffic classes are limited to a maximum of 30%, the remaining queues have at least 40% of the bandwidth at their disposal. The device immediately sends Strict Priority data up to a maximum bandwidth of 30%.
`exit`	Switch to the privileged EXEC mode.
`show interfaces cos-queue`	Display the configuration.

```
Global Configuration
Interface Shaping Rate..................... 0

Queue Id   Min. Bandwidth   Max. Bandwidth   Scheduler Type
--------   --------------   --------------   --------------
0          10               20               Weighted
1          10               20               Weighted
2          15               20               Weighted
3          15               20               Weighted
4          20               20               Weighted
5          30               30               Weighted
6          0                30               Strict
7          0                30               Strict
```

Configuring Traffic Shaping on a port

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`interface 1/2`	Switch to the interface configuration mode for port 1.2.

```
traffic-shape 50                    Restricts the maximum bandwidth of
                                    interface 1/2 to 50%.
exit                                Switch to the Configuration mode.
exit                                Switch to the privileged EXEC mode.
show interfaces cos-queue           Display the configuration of interface 1/2.
  1/2
Interface..................................... 1/2
Interface Shaping Rate........................ 50

Queue Id   Min. Bandwidth   Max. Bandwidth   Scheduler Type
--------   --------------   --------------   --------------
0          10               20               Weighted
1          10               20               Weighted
2          15               20               Weighted
3          15               20               Weighted
4          20               20               Weighted
5          30               30               Weighted
6          0                30               Strict
7          0                30               Strict
```

```
enable                              Switch to the privileged EXEC mode.
configure                           Switch to the Configuration mode.
interface 1/2                       Switch to the interface configuration mode for
                                    port 1.2.
traffic-shape 50                    Restricts the maximum bandwidth of
                                    interface 1/2 to 50%.
exit                                Switch to the Configuration mode.
exit                                Switch to the privileged EXEC mode.
show interfaces cos-queue           Display the configuration of interface 1/2.
  1/2
Interface..................................... 1/2
Interface Shaping Rate........................ 50

Queue Id   Min. Bandwidth   Max. Bandwidth   Scheduler Type
--------   --------------   --------------   --------------
0          10               20               Weighted
1          10               20               Weighted
2          15               20               Weighted
3          15               20               Weighted
4          20               20               Weighted
5          30               30               Weighted
6          0                30               Strict
7          0                30               Strict
```

Configuring Layer 2 management priority

☐ Configure the VLAN ports to which the device sends management packets as a member of the VLAN that sends data packets with a tag (see on page 195 “Examples of VLANs”).

☐ Open the `QoS/Priority:Global` dialog.
☐ In the "VLAN Priority for Management packets" field, you enter the value of the VLAN priority.

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

```
System IP Address.............................. 10.0.1.116
Subnet Mask.................................... 255.255.255.0
Default Gateway................................ 10.0.1.200
Burned In MAC Address.......................... 00:80:63:51:7A:80
Network Configuration Protocol (BootP/DHCP).... None
DHCP Client ID (same as SNMP System Name)...... "PowerMICE-517A80"
Network Configuration Protocol HiDiscovery..... Read-Write
HiDiscovery Version............................ v1, v2
Management VLAN ID............................. 1
Management VLAN Priority....................... 7
Management IP-DSCP Value....................... 0(be/cs0)
Web Mode....................................... Enable
```

Configuring Layer 3 management priority

☐ Open the `QoS/Priority:Global` dialog.
☐ In the "IP DSCP Value for Management packets" field, you enter the IP DSCP value with which the device sends management packets.

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

```
System IP Address.............................. 10.0.1.116
Subnet Mask.................................... 255.255.255.0
Default Gateway................................ 10.0.1.200
Burned In MAC Address.......................... 00:80:63:51:7A:80
Network Configuration Protocol (BootP/DHCP).... None
DHCP Client ID (same as SNMP System Name)...... "PowerMICE-517A80"
Network Configuration Protocol HiDiscovery..... Read-Write
HiDiscovery Version............................ v1, v2
Management VLAN ID............................. 1
Management VLAN Priority....................... 7
Management IP-DSCP Value....................... 56(cs7)
Web Mode....................................... Enable
```

8.5 Flow Control

8.5.1 Description of Flow Control

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

The example (see figure 37) shows a graphic illustration of how the flow control works. Workstations 1, 2 and 3 want to simultaneously transmit a large amount of data to Workstation 4. The combined bandwidth of Workstations 1, 2 and 3 to the device is larger than the bandwidth of Workstation 4 to the device. This leads to an overflow of the send queue of port 4. The funnel on the left symbolizes this status.

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

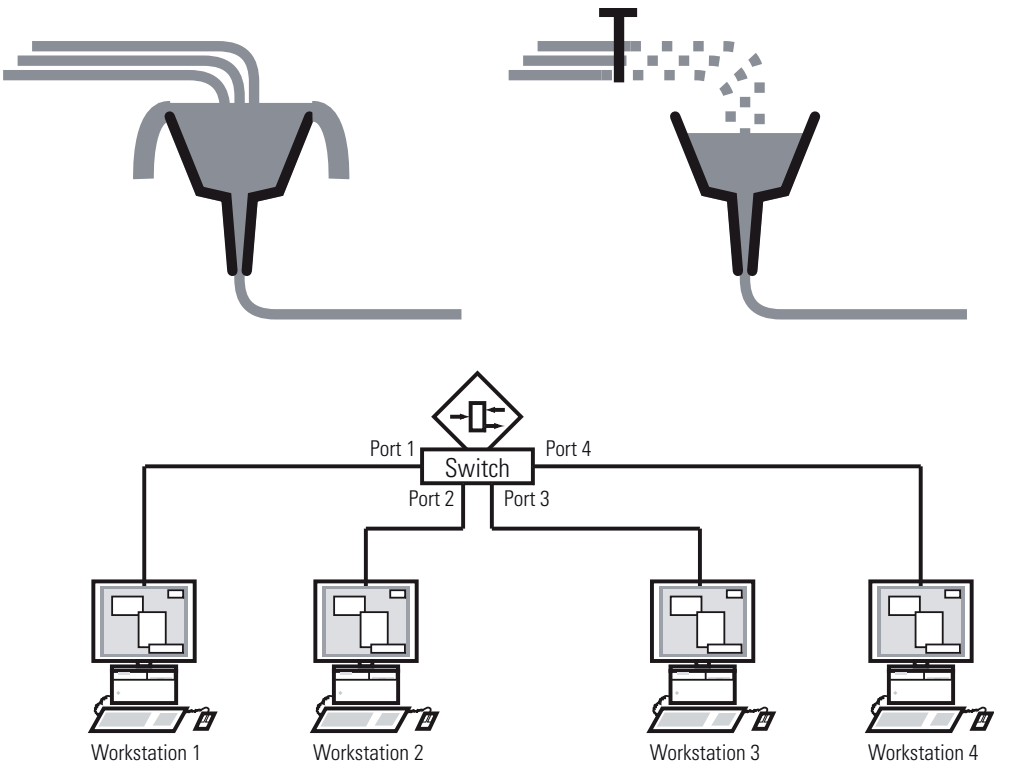


Figure 37: Example of flow control

Flow Control with a full duplex link

In the example (see figure 37) there is a full duplex link between Workstation 2 and the device.
Before the send queue of port 2 overflows, the device sends a request to Workstation 2 to include a small break in the sending transmission.

Note: The devices RS20/30/40, MS20/30, Octopus, MACH 100, RSR and MACH 1000 support flow control in full duplex mode only.

Flow Control with a half duplex link

In the example (see figure 37) there is a half duplex link between Workstation 2 and the device.
Before the send queue of port 2 overflows, the device sends data back so that Workstation 2 detects a collision and interrupts the sending process.

Note: The devices RS20/30/40, MS20/30, Octopus, MACH 100, RSR and MACH 1000 do not support flow control in half duplex mode.

8.5.2 Setting the Flow Control

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

☐ Select the `Switching:Global` dialog.
With this dialog you can

- switch off the flow control at all ports or
- switch on the flow control at those ports for which the flow control is selected in the port configuration table.

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

8.6 VLANs

8.6.1 VLAN Description

In the simplest case, a virtual LAN (VLAN) consists of a group of network participants in one network segment who can communicate with each other as if they belonged to a separate LAN.

More complex VLANs span out over multiple network segments and are also based on logical (instead of only physical) connections between network participants. Thus VLANs are an element of flexible network design, as you can reconfigure logical connections centrally more easily than cable connections.

The IEEE 802.1Q standard defines the VLAN function.

The most important benefits of VLANs are:

- Network load limiting
  VLANs reduce the network load considerably as the devices transmit broadcast, multicast, and unicast packets with unknown (unlearned) destination addresses exclusively inside the virtual LAN. The rest of the data network forwards traffic as normal.

- Flexibility
  You have the option of forming user groups flexibly based on the function of the participants and not on their physical location or medium.

- Clarity
  VLANs give networks a clear structure and make maintenance easier.

8.6.2 Examples of VLANs

The following practical examples provide a quick introduction to the structure of a VLAN.

Example 1

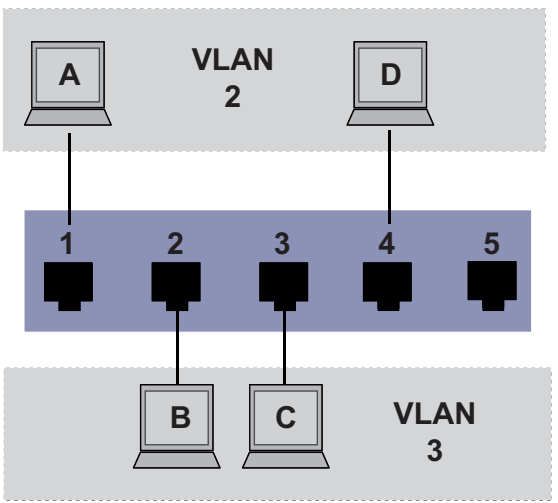


Figure 38: Example of a simple port-based VLAN

The example shows a minimal VLAN configuration (port-based VLAN). An administrator has connected multiple terminal devices to a transmission device and assigned them to 2 VLANs. This effectively prohibits any data transmission between the VLANs, whose members communicate only within their own VLANs.
When setting up the VLANs, you create communication rules for every port, which you enter in incoming (ingress) and outgoing (egress) tables. The ingress table specifies which VLAN ID a port assigns to the incoming data packets. Hereby, you use the port address of the terminal device to assign it to a VLAN.
The egress table specifies at which ports the Switch may send the frames from this VLAN. Your entry also defines whether the Switch marks (tags) the Ethernet frames sent from this port.

- `T` = with tag field (T = tagged, marked)
- `U` = without tag field (U = untagged, not marked)

For this example, the status of the TAG field of the data packets has no relevance, so you set it to "U“.

Terminal	Port	Port VLAN identifier (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
	5	1

Table 17: Ingress table

VLANID	Port				
	1	2	3	4	5
1					U
2	U			U	
3		U	U		

Table 18: Egress table

Proceed as follows to perform the example configuration:

☐ Configure VLAN

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

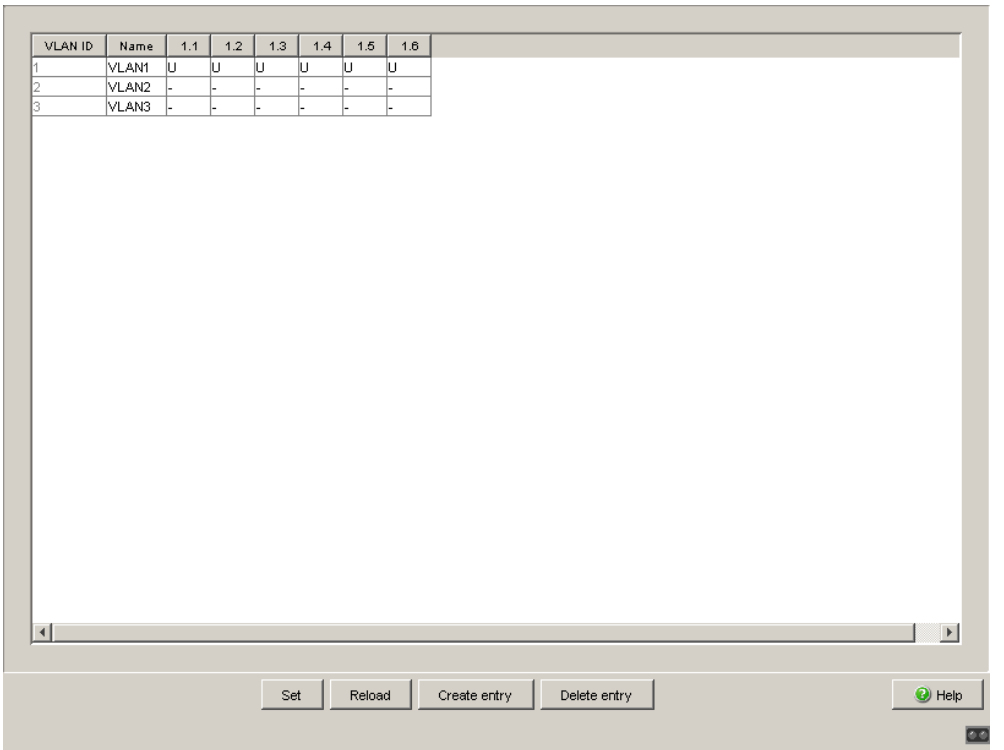


Figure 39: Creating and naming new VLANs

- ☐ Click on "Create" to open the window for entering the VLAN ID.
- ☐ Assign VLAN ID `2` to the VLAN.
- ☐ Click "OK".
- ☐ You give this VLAN the name VLAN2 by clicking on the field and entering the name. Also change the name for VLAN 1 from `Default` to `VLAN1`.
- ☐ Repeat the previous steps and create another VLAN with the VLAN ID `3` and the name `VLAN3`.

`enable`	Switch to the privileged EXEC mode.
`vlan database`	Switch to the VLAN configuration mode.
`vlan 2`	Create a new VLAN with the VLAN ID 2.
`vlan name 2 VLAN2`	Give the VLAN with the VLAN ID 2 the name VLAN2.
`vlan 3`	Create a new VLAN with the VLAN ID 3.
`vlan name 3 VLAN3`	Give the VLAN with the VLAN ID 3 the name VLAN3.
`vlan name 1 VLAN1`	Give the VLAN with the VLAN ID 1 the name VLAN1.
`exit`	Leave the VLAN configuration mode.

```
show vlan brief                    Display the current VLAN configuration.
Max. VLAN ID..................................... 4042
Max. supported VLANs.............................  255
Number of currently configured VLANs...........    3
VLAN 0 Transparent Mode (Prio. Tagged Frames).. Disabled
VLAN ID VLAN Name                       VLAN Type VLAN Creation Time
---- -------------------------------- --------- -------------------
1       VLAN1                           Default    0 days, 00:00:05
2       VLAN2                           Static     0 days, 02:44:29
3       VLAN3                           Static     0 days, 02:52:26
```

☐ Configuring the ports

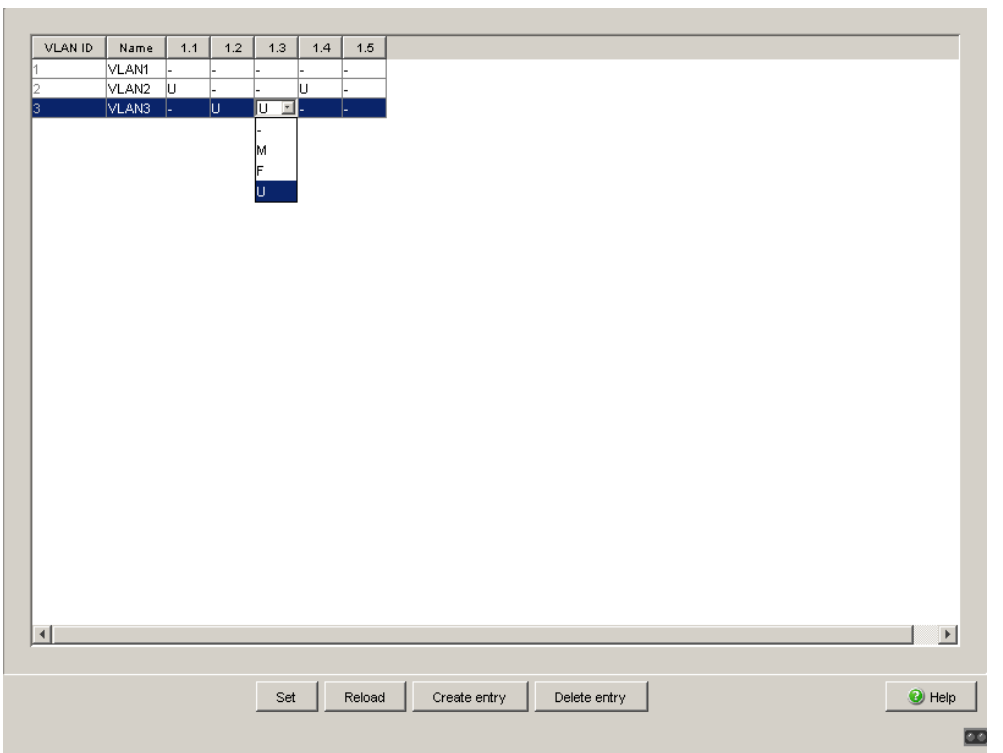


Figure 40: Defining the VLAN membership of the ports.

☐ Assign the ports of the device to the corresponding VLANs by clicking on the related table cell to open the selection menu and define the status. The selection options are:

- `-` = currently not a member of this VLAN (GVRP allowed)
- `T` = member of VLAN; send data packets with tag
- `U` = Member of the VLAN; send data packets without tag
- `F` = not a member of the VLAN (also disabled for GVRP)

Because terminal devices usually interpret untagged data packets exclusivly, you select the `U` setting here.

☐ To temporarily save the changes, click "Set".

☐ Open the `Switching:VLAN:Port` dialog.

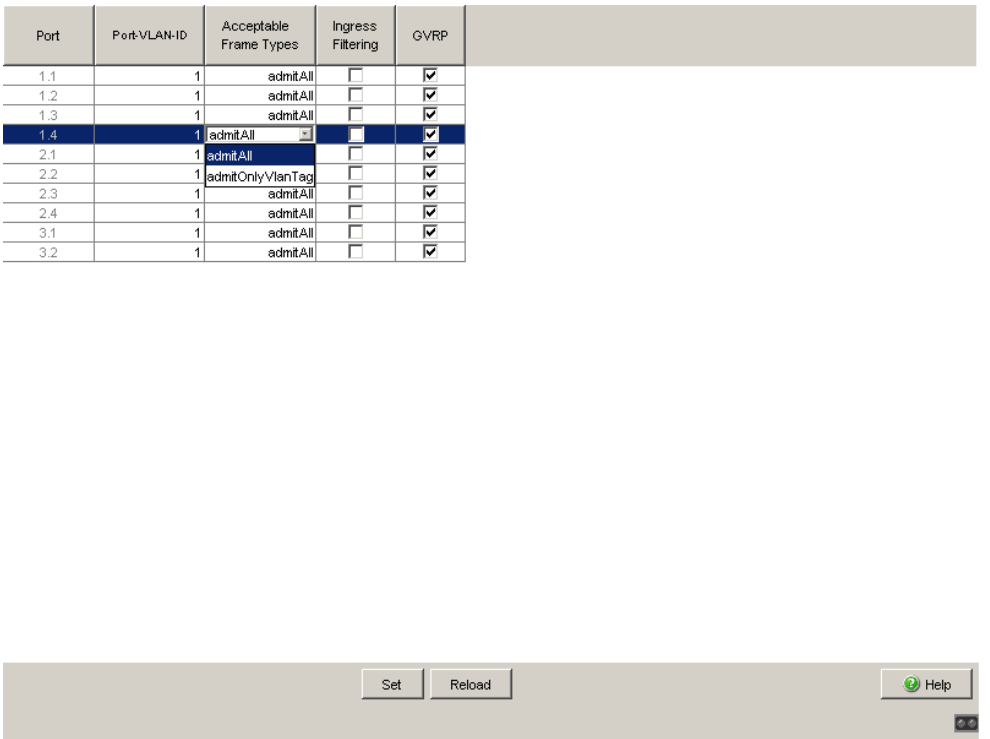


Figure 41: Assigning and saving "Port VLAN ID", "Acceptable Frame Types" and "Ingress Filtering"

- ☐ Assign the Port VLAN ID of the related VLANs (2 or 3) to the individual ports - see table.
- ☐ Because terminal devices usually send data packets as untagged, you select the `admitAll` setting for the "Acceptable Frame Types".
- ☐ The settings for `GVRP` and `Ingress Filter` do not affect how this example functions.
- ☐ Click "Set" to save the changes temporarily.
- ☐ Select the `Basics: Load/Save` dialog.
- ☐ In the “Save” frame, select “To Device” for the location and click “Save” to permanently save the configuration in the active configuration.

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`interface 1/1`	Switch to the Interface Configuration mode of interface 1/1.
`vlan participation include 2`	Port 1/1 becomes member untagged in VLAN 2.
`vlan pvid 2`	Port 1/1 is assigned the port VLAN ID 2.
`exit`	Switch to the Configuration mode.

```
interface 1/2                    Switch to the interface configuration mode for
                                 port 1.2.
vlan participation include 3     Port 1/2 becomes member untagged in VLAN 3.
vlan pvid 3                      Port 1/2 is assigned the port VLAN ID 3.
exit                             Switch to the Configuration mode.
interface 1/3                    Switch to the Interface Configuration mode of
                                 Interface 1/3.
vlan participation include 3     Port 1/3 becomes member untagged in VLAN 3.
vlan pvid 3                      Port 1/3 is assigned the port VLAN ID 3.
exit                             Switch to the Configuration mode.
interface 1/4                    Switch to the interface configuration mode of
                                 interface 1/4.
vlan participation include 2     Port 1/4 becomes member untagged in VLAN 2.
vlan pvid 2                      Port 1/4 is assigned the port VLAN ID 2.
exit                             Switch to the Configuration mode.
exit                             Switch to the privileged EXEC mode.
show VLAN 3                      Show details for VLAN 3.
VLAN ID           : 3
VLAN Name         : VLAN3
VLAN Type         : Static
VLAN Creation Time: 0 days, 02:52:26 (System Uptime)
Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1         Exclude   Autodetect   Tagged
1/2         Include   Include      Untagged
1/3         Include   Include      Untagged
1/4         Exclude   Autodetect   Tagged
1/5         Exclude   Autodetect   Tagged
```

Example 2

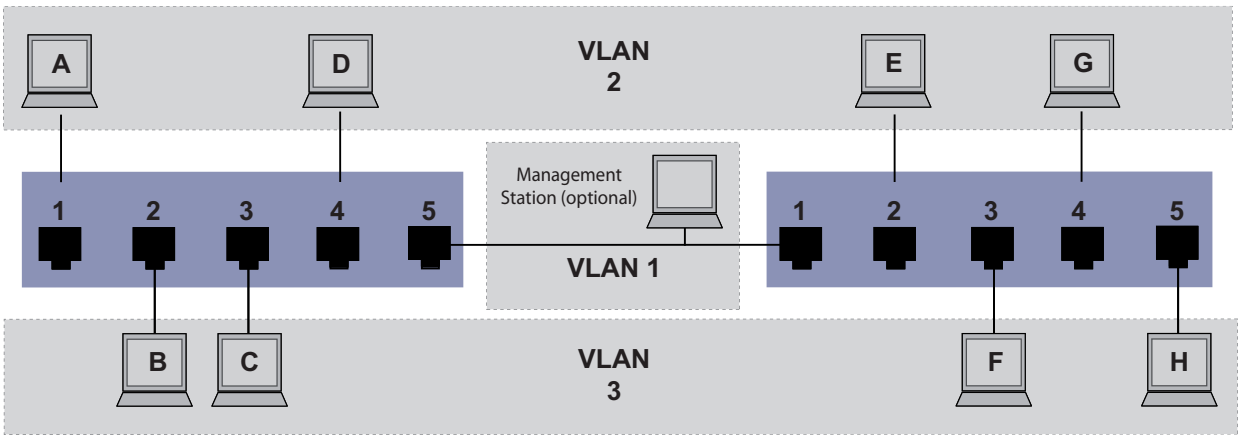


Figure 42: Example of a more complex VLAN configuration

The second example shows a more complex configuration with 3 VLANs (1 to 3). Along with the Switch from example 1, you use a 2nd Switch (on the right in the example).

The simple network divides the terminal devices, A - H, of the individual VLANs over 2 transmission devices (Switches). VLANs configured in this manner are „distributed VLANs“. When configured correctly the VLANs allow the optional Management Station to access the network components.

Note: In this case, VLAN 1 has no significance for the terminal device communication, but it is required for the administration of the transmission devices via what is known as the Management VLAN.

As in the previous example, uniquely assign the ports with their connected terminal devices to a VLAN. With the direct connection between the 2 transmission devices (uplink), the ports transport packets for both VLANs. To differentiate these uplinks you use “VLAN tagging”, which handles the frames accordingly. Thus, you maintain the assignment to the respective VLANs.

Proceed as follows to perform the example configuration:

Add Uplink Port 5 to the ingress and egress tables from example 1. Create new ingress and egress tables for the right switch, as described in the first example.

The egress table specifies at which ports the Switch may send the frames from this VLAN. Your entry also defines whether the Switch marks (tags) the Ethernet frames sent from this port.

- `T` = with tag field (T = tagged, marked)
- `U` = without tag field (U = untagged, not marked)

In this example, the devices use tagged frames in the communication between the transmission devices (uplink), the ports differentiate the frames for different VLANs.

Terminal	Port	Port VLAN identifier (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
Uplink	5	1

Table 19: Ingress table for device on left

Terminal	Port	Port VLAN identifier (PVID)
Uplink	1	1
E	2	2
F	3	3
G	4	2
H	5	3

Table 20: Ingress table for device on right

VLAN ID	Port				
	1	2	3	4	5
1					U
2	U			U	T
3		U	U		T

Table 21: Egress table for device on left

VLAN ID	Port				
	1	2	3	4	5
1	U				

Table 22: Egress table for device on right

VLAN ID	Port					
2	T	U		U		
3	T		U		U	

Table 22: Egress table for device on right

The communication relationships here are as follows: terminal devices at ports 1 and 4 of the left device and terminal devices at ports 2 and 4 of the right device are members of VLAN 2 and can thus communicate with each other. The behavior is the same for the terminal devices at ports 2 and 3 of the left device and the terminal devices at ports 3 and 5 of the right device. These belong to VLAN 3.

The terminal devices “see” their respective part of the network. Participants outside this VLAN cannot be reached. The device also sends broadcast, multicast, and unicast packets with unknown (unlearned) destination addresses exclusively inside a VLAN.

Here, VLAN tagging (IEEE 801.1Q) is used within the VLAN with the ID 1 (Uplink). You can see this from the letter `T` in the egress table of the ports.

The configuration of the example is the same for the device on the right. Proceed in the same way, using the ingress and egress tables created above to adapt the previously configured left device to the new environment.

Proceed as follows to perform the example configuration:

☐ Configure VLAN

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

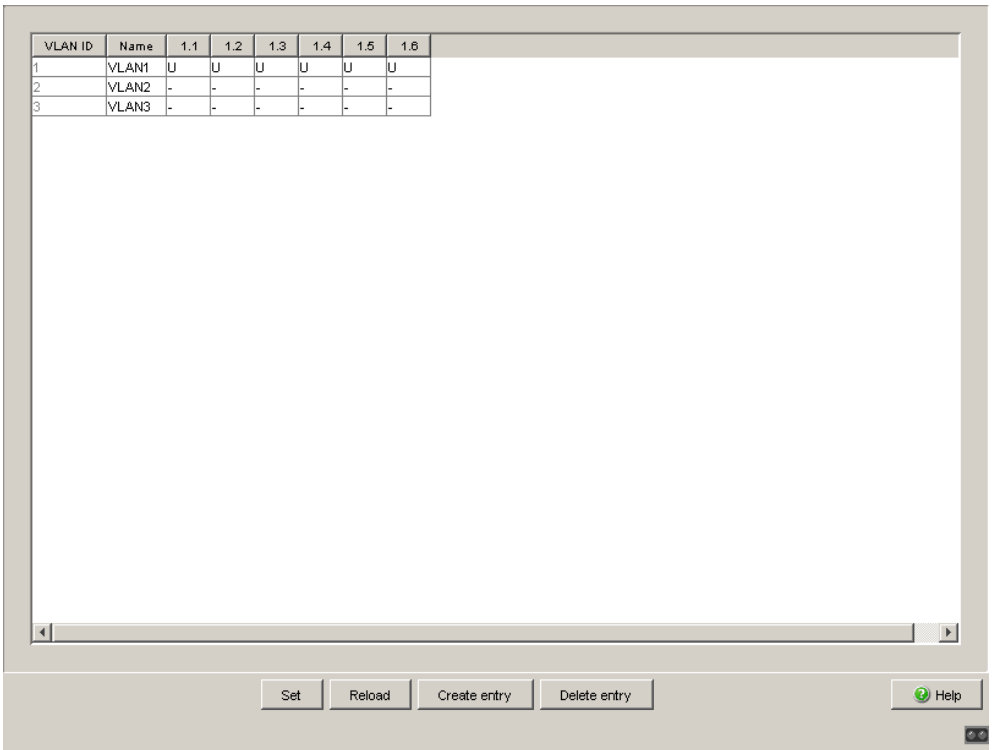


Figure 43: Creating and naming new VLANs

- ☐ Click on "Create" to open the window for entering the VLAN ID.
- ☐ Assign VLAN ID `2` to the VLAN.
- ☐ You give this VLAN the name VLAN2 by clicking on the field and entering the name. Also change the name for VLAN 1 from `Default` to `VLAN1`.
- ☐ Repeat the previous steps and create another VLAN with the VLAN ID 3 and the name `VLAN3`.

`enable`	Switch to the privileged EXEC mode.
`vlan database`	Switch to the VLAN configuration mode.
`vlan 2`	Create a new VLAN with the VLAN ID 2.
`vlan name 2 VLAN2`	Give the VLAN with the VLAN ID 2 the name VLAN2.
`vlan 3`	Create a new VLAN with the VLAN ID 3.
`vlan name 3 VLAN3`	Give the VLAN with the VLAN ID 3 the name VLAN3.
`vlan name 1 VLAN1`	Give the VLAN with the VLAN ID 1 the name VLAN1.
`exit`	Switch to the privileged EXEC mode.

```
show vlan brief                    Display the current VLAN configuration.
Max. VLAN ID..................................... 4042
Max. supported VLANs.............................  255
Number of currently configured VLANs...........    3
VLAN 0 Transparent Mode (Prio. Tagged Frames).. Disabled
VLAN ID VLAN Name                       VLAN Type VLAN Creation Time
---- -------------------------------- --------- -------------------
1       VLAN1                            Default    0 days, 00:00:05
2       VLAN2                            Static     0 days, 02:44:29
3       VLAN3                            Static     0 days, 02:52:26
```

☐ Configuring the ports

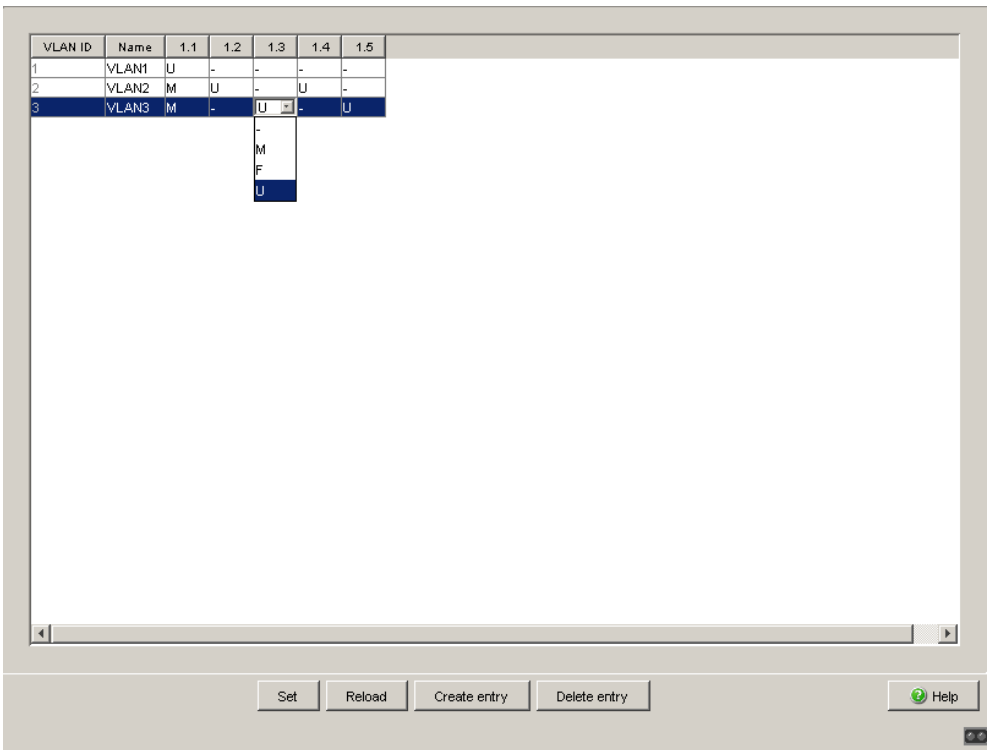


Figure 44: Defining the VLAN membership of the ports.

☐ Assign the ports of the device to the corresponding VLANs by clicking on the related table cell to open the selection menu and define the status. The selection options are:

- `-` = currently not a member of this VLAN (GVRP allowed)
- `T` = member of VLAN; send data packets with tag
- `U` = Member of the VLAN; send data packets without tag
- `F` = not a member of the VLAN (also disabled for GVRP)

Because terminal devices usually interpret untagged data packets, you select the `U` setting. You select the `T`setting on the uplink port on which the VLANs communicate with each other.

☐ Click "Set" to save the changes temporarily.

☐ Open the `Switching:VLAN:Port` dialog.

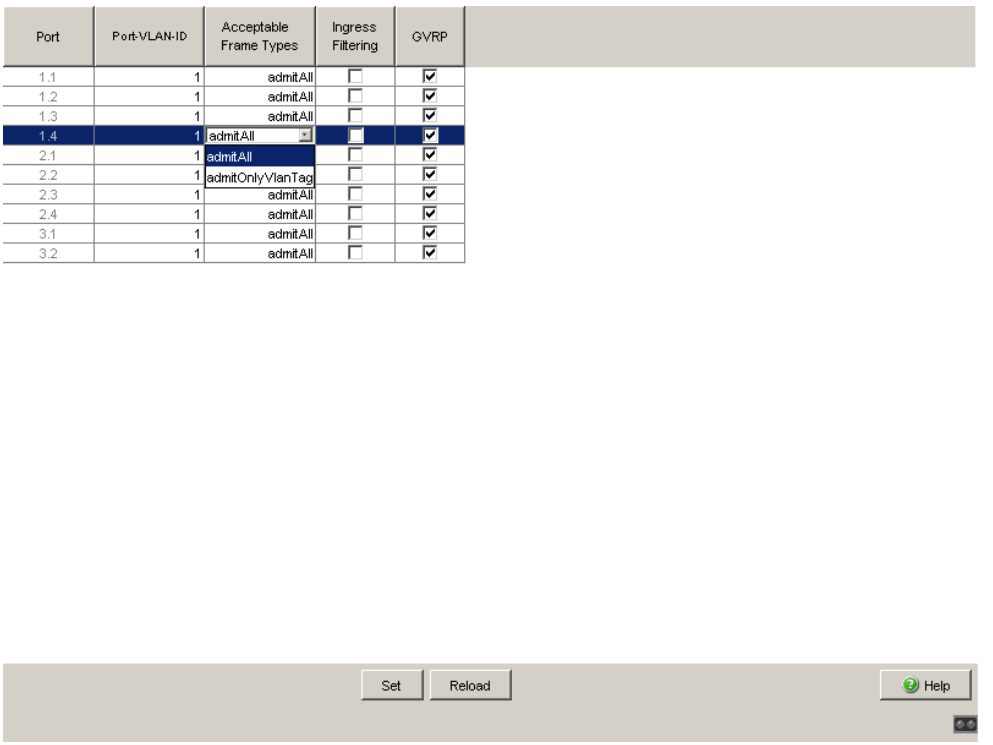


Figure 45: Assigning and saving "Port VLAN ID", "Acceptable Frame Types" and "Ingress Filtering"

☐ Assign the ID of the related VLANs (1 to 3) to the individual ports.

☐ Because terminal devices usually send data packets as untagged, you select the `admitAll` setting for the terminal device ports. Configure the uplink port with `admit only VLAN tags`.

☐ To evaluate the VLAN tag on this port, activate "Ingress Filtering" on the uplink port.

☐ Click "Set" to save the changes temporarily.

☐ Select the `Basics: Load/Save` dialog.

☐ In the “Save” frame, select “To Device” for the location and click “Save” to permanently save the configuration in the active configuration.

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`interface 1/1`	Switch to the Interface Configuration mode of interface 1/1.
`vlan participation include 1`	Port 1/1 becomes member untagged in VLAN 1.
`vlan participation include 2`	Port 1/1 becomes member untagged in VLAN 2.
`vlan tagging 2`	Port 1/1 becomes member tagged in VLAN 2.

`vlan participation include 3`	Port 1/1 becomes member untagged in VLAN 3.
`vlan tagging 3`	Port 1/1 becomes member tagged in VLAN 3.
`vlan pvid 1`	Port 1/1 is assigned the port VLAN ID 1.
`vlan ingressfilter`	Port 1/1 ingress filtering is activated.
`vlan acceptframe vlanonly`	Port 1/1 only forwards frames with a VLAN tag.
`exit`	Switch to the Configuration mode.
`interface 1/2`	Switch to the interface configuration mode for port 1.2.
`vlan participation include 2`	Port 1/2 becomes member untagged in VLAN 2.
`vlan pvid 2`	Port 1/2 is assigned the port VLAN ID 2.
`exit`	Switch to the Configuration mode.
`interface 1/3`	Switch to the Interface Configuration mode of Interface 1/3.
`vlan participation include 3`	Port 1/3 becomes member untagged in VLAN 3.
`vlan pvid 3`	Port 1/3 is assigned the port VLAN ID 3.
`exit`	Switch to the Configuration mode.
`interface 1/4`	Switch to the interface configuration mode of interface 1/4.
`vlan participation include 2`	Port 1/4 becomes member untagged in VLAN 2.
`vlan pvid 2`	Port 1/4 is assigned the port VLAN ID 2.
`exit`	Switch to the Configuration mode.
`interface 1/5`	Switch to the interface configuration mode for port 1.5.
`vlan participation include 3`	Port 1/5 becomes member untagged in VLAN 3.
`vlan pvid 3`	Port 1/5 is assigned the port VLAN ID 3.
`exit`	Switch to the Configuration mode.
`exit`	Switch to the privileged EXEC mode.
`show vlan 3`	Show details for VLAN 3.

```
VLAN ID           : 3
VLAN Name         : VLAN3
VLAN Type         : Static
VLAN Creation Time: 0 days, 00:07:47 (System Uptime)
Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1         Include   Include      Tagged
1/2         Exclude   Autodetect   Untagged
1/3         Include   Include      Untagged
1/4         Exclude   Autodetect   Untagged
1/5         Include   Include      Untagged
```

For further information on VLANs, see the reference manual and the integrated help function in the program.

8.6.3 Double VLAN Tagging

For the devices MACH 1040 and MACH 4002-24G/48G.

Double VLAN tagging (VLAN tunneling) enables you to transmit from traffic to layer 2. Double VLAN tagging allows you to avoid conflicts between the VLAN IDs of the incoming traffic and the VLANs already set up your network. You leave existing VLANs in your network unchanged and thus minimize your configuration work. This applies to:

- frames without VLAN tags,
- frames with priority tags, and
- frames with VLAN tags with any VLAN ID, including those which you are already employing for other purposes in your network.

Applications include:

- tunneling from any client traffic to layer 2,
- bypassing restrictions to the number of VLAN IDs,
- summarizing VLANs per port.

You can set up several tunnels with different VLAN IDs and thereby freely select the Ethertype of the inserted tunnel tags for your network.

The ports participating in this VLAN tunnel are either:

- Access ports on which your network receives and sends external traffic, or
- Core ports which are all located inside your network and are connected with another core port.

To construct a VLAN tunnel, set up a selectable VLAN on your devices and put the access and core ports in this tunnel VLAN. Access ports are untagged members in your tunnel VLAN and have the tunnel VLAN ID as their port VLAN ID. Core ports are tagged members in all tunnel VLANs and do not need a port VLAN ID. Also, increase the maximum size for frames on all switches with core ports to 1,552 bytes.

How the VLAN tunnel works

- The device assigns the port VLAN ID to the frame when a frame is received at an access port. This is the tunnel VLAN ID. This also applies to frames which have already been tagged.
- Core ports are tagged members in all tunnel VLANs and send out the frame with the tunnel tag.
- The core ports transmit traffic with the tunnel VLAN ID.
- Access ports are untagged members only in their tunnel VLAN. The device removes the tunnel tag at the sending access port and sends out the original frame.

Default setting: Double VLAN tagging is deactivated at all ports. The presetting for the Ethertype of the tunnel tag is 8100Hex.

Example of Double VLAN Tagging

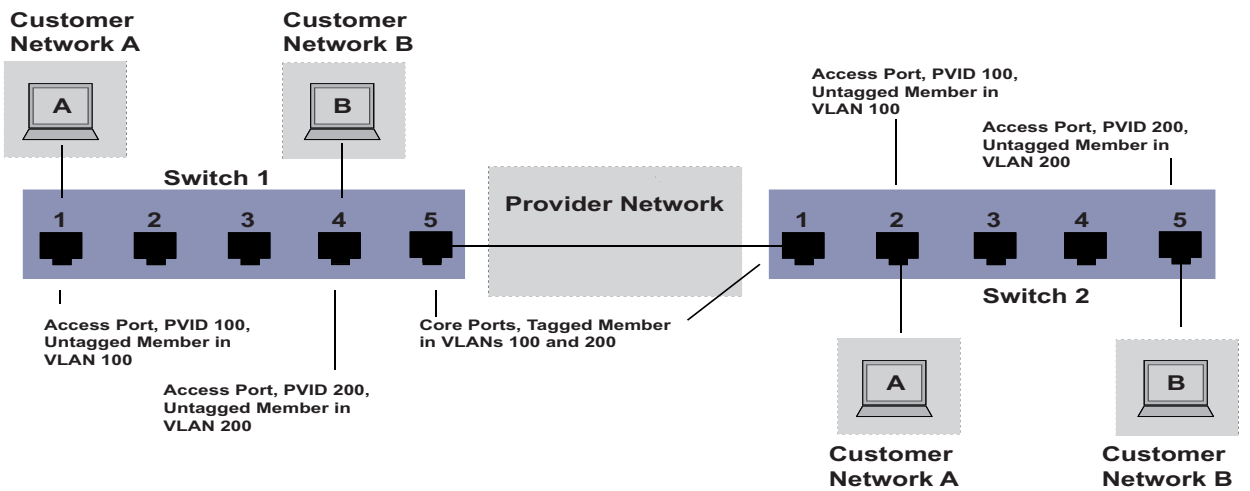


Figure 46: Example of a VLAN tunnel through use of double VLAN tagging

This example shows a provider network, the data from two client networks, A and B, transported to layer 2 through 2 VLAN tunnels. The traffic received from the client network is not subject to any restrictions with regard to VLAN IDs. The frames received can be without VLAN tags, or provided with VLAN tags or only priority tags.

VLAN-IDs 100 and 200 are not yet used on the provider network. You decide to assign the new VLAN 100 service to Client A, and the VLAN 200 service to Client B. The VLANs for the device are defined as follows:

Client	Service VLAN ID
A	100
B	200

Table 23: Assignment of client networks to service VLANs (VLAN tunnels)

On Switch 1, ports 1 and 4 are access ports, and port 5 is a core port (port within the provider network). On switch 2, ports 2 and 5 are access ports and port 1 is a core port. All ports are located on module 1 of the related Switch. The port settings are defined as follows:

Switch	Port	Port role	Participant in VLAN (Tagging)	PVID
1	1/1	Access	100 (U)	100
	1/4	Access	200 (U)	200
	1/5	Core	100 (T), 200 (T)	-
2	1/1	Core	100 (T), 200 (T)	-
	1/2	Access	100 (U)	100
	1/5	Access	200 (U)	200

Table 24: Port settings for VLAN tunnel

Set the sample configuration with the CLI:

Switch 1:

`enable`	Switch to the privileged EXEC mode.
`vlan database`	Switch to the VLAN configuration mode.
`vlan 100`	Create a new VLAN with the VLAN ID 100.
`vlan name 100 KUNDE_A`	Give the VLAN with the VLAN ID 100 the name CLIENT_A.
`vlan 200`	Create a new VLAN with the VLAN ID 200.
`vlan name 200 KUNDE_B`	Give the VLAN with the VLAN ID 200 the name CLIENT_B.
`exit`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`bridge framesize 1552`	Set the permissible frame size to 1,522 bytes.
`interface 1/1`	Switch to the Interface Configuration mode of interface 1/1.
`vlan pvid 100`	Port 1.1 is given the port VLAN ID 100.
`vlan participation include 100`	Port 1.1 becomes a member of VLAN 100.

`no vlan tagging`	Port 1.1 becomes an untagged member (`no vlan tagging` is default)
`mode dvlan-tunnel access`	Port 1.1 becomes an access port
`exit`	Switch to the Configuration mode.
`interface 1/4`	Switch to the interface configuration mode of interface 1/4.
`vlan pvid 200`	Port 1.4 is given the port VLAN ID 200.
`vlan participation include 200`	Port 1.4 becomes a member of VLAN 200.
`no vlan tagging`	Port 1.4 becomes an untagged member (`no vlan tagging` is default)
`mode dvlan-tunnel access`	Port 1.4 becomes an access port
`exit`	Switch to the Configuration mode.
`interface 1/5`	Switch to the interface configuration mode for port 1.5.
`vlan participation include 100`	Port 1.5 becomes a member of VLAN 100.
`vlan participation include 200`	Port 1.5 becomes a member of VLAN 200.
`vlan tagging`	Port 1.5 becomes a tagged member
`mode dvlan-tunnel core`	Port 1.5 becomes a core port
`exit`	Switch to the Configuration mode.

Switch 2:

`enable`	Switch to the privileged EXEC mode.
`vlan database`	Switch to the VLAN configuration mode.
`vlan 100`	Create a new VLAN with the VLAN ID 100.
`vlan name 100 KUNDE_A`	Give the VLAN with the VLAN ID 100 the name CLIENT_A.
`vlan 200`	Create a new VLAN with the VLAN ID 200.
`vlan name 200 KUNDE_B`	Give the VLAN with the VLAN ID 200 the name CLIENT_B.
`exit`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`bridge framesize 1552`	Set the permissible frame size to 1,522 bytes.
`interface 1/1`	Switch to the Interface Configuration mode of interface 1/1.
`vlan participation include 100`	Port 1.1 becomes a member of VLAN 100.
`vlan participation include 200`	Port 1.1 becomes a member of VLAN 200.
`vlan tagging`	Port 1.1 becomes a tagged member
`mode dvlan-tunnel core`	Port 1.1 becomes a core port

`exit`	Switch to the Configuration mode.
`interface 1/2`	Switch to the interface configuration mode for port 1.2.
`vlan pvid 100`	Port 1.2 is given the port VLAN ID 100.
`vlan participation include 100`	Port 1.2 becomes a member of VLAN 100.
`no vlan tagging`	Port 1.2 becomes an untagged member (`no vlan tagging` is default)
`mode dvlan-tunnel access`	Port 1.2 becomes an access port
`exit`	Switch to the Configuration mode.
`interface 1/5`	Switch to the interface configuration mode for port 1.5.
`vlan participation include 200`	Port 1.5 becomes a member of VLAN 200.
`no vlan tagging`	Port 1.5 becomes an untagged member (`no vlan tagging` is default)
`mode dvlan-tunnel access`	Port 1.5 becomes an access port
`exit`	Switch to the Configuration mode.

9 Operation Diagnosis

The device provides you with the following diagnostic tools:

- Sending traps
- Monitoring the device status
- Out-of-band signaling via signal contact
- Port status indication
- Event counter at port level
- Detecting non-matching duplex modes
- SFP status display
- TP cable diagnosis
- Topology Discovery
- Detecting IP address conflicts
- Detecting loops
- Reports
- Monitoring data traffic at a port (port mirroring)
- Syslog
- Event log

9.1 Sending Traps

The device reports unusual events which occur during normal operation immediately to the management station. This is done by messages called traps that bypass the polling procedure ("Polling" means querying the data stations at regular intervals). Traps allow you to react quickly to unusual events.

Examples of such events are:

- Hardware reset
- Changes to the configuration
- Segmentation of a port

The device sends traps to various hosts to increase the transmission reliability for the messages. The unacknowledged trap message consists of a packet containing information about an unusual event.

The device sends traps to those hosts entered in the trap destination table. The device allows you to configure the trap destination table with the management station via SNMP.

9.1.1 List of SNMP traps

The following table shows a list of the traps that can be sent by the device.

Trap name	Meaning
authenticationFailure	this is sent if a station attempts to access an agent without authorisation.
coldStart	this is sent during the boot phase for both cold starts and warm starts, after successful initialisation of the network management.
hmAutoconfigAdapterTrap	this is sent when the AutoConfiguration AdapterACA is disconnected or connected.
linkDown	this is sent if the connection to a port is interrupted.
linkUp	this is sent when connection is established to a port.
hmTemperature	this is sent if the temperature exceeds the set threshold limits.
hmPowerSupply	this is sent if the power supply status changes.
hmSigConRelayChange	this is sent if the status of the signal contact changes in the function monitoring.
newRoot	this is sent if the sending agent becomes the new root of the spanning tree.
topologyChange	this is sent if the switching mode of a port changes.
risingAlarm	this is sent if an RMON alarm input exceeds its upper threshold.
fallingAlarm	this is sent if an RMON alarm input goes below its lower threshold.
hmPortSecurityTrap	this is sent if an MAC/IP address detected on this port does not correspond to the current settings for – hmPortSecPermission and – hmPorSecAction is set to either trapOnly (2) or portDisable (3).
hmModuleMapChange	this is sent if the hardware configuration changes.
hmBPDUGuardTrap	this is sent if a BPDU is received on a port while the BPDU Guard function is active.
hmMrpReconfig	this is sent if the configuration of the MRP Ring changes.
hmRingRedReconfig	this is sent if the configuration of the HIPER Ring changes.
hmRingRedCplReconfig	this is sent if the configuration of the redundant ring/network coupling changes.
hmSNTPTrap	this is sent if an error occurs in relation to the SNTP (e.g. server not available).
hmRelayDuplicateTrap	this is sent if a duplicate IP address is detected in relation to DHCP Option 82.
lldpRemTablesChangeTrap	this is sent if an entry in the Remote Table topology changes.
vrrpTrapNewMaster	this is sent if another router becomes the master router for an interface or a virtual address.
vrrpTrapAuthFailure	this is sent if the router receives a packet with an invalid authentication from another VRRP router.
hmConfigurationSavedTrap	this is sent after the device has successfully saved its configuration locally.

Table 25: Possible traps

Trap name	Meaning
hmConfigurationChangedTrap	this is sent if you change the configuration of the device after saving locally for the first time.
hmAddressRelearnDetectTrap	this is sent if Address Relearn Detection is active and the relearn threshold for MAC addresses on different ports is exceeded. This process indicates high probability of a loop situation on the network.
hmDuplexMismatchTrap	this is sent if the device detects a possible problem with duplex mode on a port.
hmTrapRebootOnError	this is sent if the device detects an error which is to be corrected by a cold start.

Table 25: Possible traps

9.1.2 SNMP Traps when Booting

The device sends the ColdStart trap during every booting.

9.1.3 Configuring Traps

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

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

☐ Click "Create".

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

☐ In the "Enabled“ column, you mark the entries that the device should take into account when it sends traps. Default setting: inactive.

☐ In the column "Password", enter the community name that the device uses to identify itself as the trap's source.

☐ In the “Configuration” frame, select the trap categories from which you want to send traps. Default setting: all trap categories are active.

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

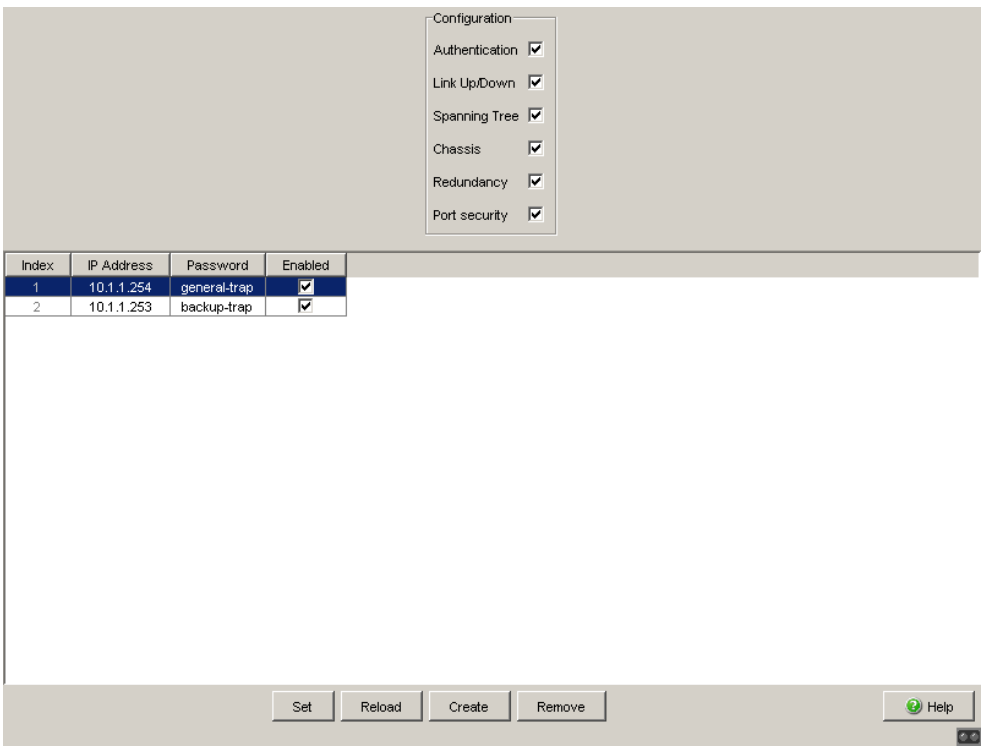


Figure 47: Alarms dialog

The events which can be selected are:

Name	Meaning
Authentication	The device has rejected an unauthorized access attempt (see the `Access for IP Addresses and Port Security` dialog).
Link Up/Down	At one port of the device, the link to another device has been established/interrupted.
Spanning Tree	The topology of the Rapid Spanning Tree has changed.
Chassis	Summarizes the following events: – The status of a supply voltage has changed (see the `System` dialog). – The status of the signal contact has changed. To take this event into account, you activate “Create trap when status changes” in the `Diagnostics:Signal Contact 1/2` dialog. - The AutoConfiguration Adapter (ACA), has been added or removed. - The configuration on the AutoConfiguration Adapter(ACA) does not match that in the device. – The temperature thresholds have been exceeded/not reached. – A media module has been added or removed (only for modular devices). – The receiver power status of a port with an SFP module has changed (see dialog `Diagnostics:Ports:SFP Modules`).
	The redundancy status of the ring redundancy (redundant line active/inactive) or (for devices that support redundant ring/network coupling) the redundant ring/network coupling (redundancy exists) has changed.
Port security	On one port a data packet has been received from an unauthorized terminal device (see the `Port Security` dialog).

Table 26: Trap categories

9.2 Monitoring the Device Status

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

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

- signal the device status out-of-band via a signal contact (see on page 224 “Monitoring the Device Status via the Signal Contact”)
- signal the device status by sending a trap when the device status changes
- detect the device status in the graphical user interface on the system side.
- query the device status in the Command Line Interface.

The `Diagnostics:Device Status` dialog of the device includes:

- Incorrect supply voltage
  - at least one of the 2 supply voltages is not operating,
  - the internal supply voltage is not operating.
- The temperature threshold has been exceeded or has not been reached.
- The removal of a module (for modular devices).
- The removal of the ACA.
- The configuration on the external memory does not match that in the device.
- The interruption of the connection at at least one port. In the `Basic Settings:Port Configuration` menu, you define which ports the device signals if the connection is down (see on page 88 “Displaying detected loss of connection”). On delivery, there is no link monitoring.
- Events for ring redundancy:
  Loss of the redundancy (in ring manager mode). On delivery, ring redundancy monitoring is inactive.
  The device is a normal ring participant and detects an error in the local configuration.

- Event in the ring/network coupling:
  Loss of the redundancy. On delivery, there is no ring redundancy monitoring.
  The following conditions are also reported by the device in standby mode:
  – Defective link status of the control line
  – Partner device is in standby mode
- Failure of a fan (MACH 4000).

Select the corresponding entries to decide which events the device status includes.

Note: With a non-redundant voltage supply, the device reports the absence of a supply voltage. If you do not want this message to be displayed, feed the supply voltage over both inputs or switch off the monitoring (see on page 224 “Monitoring the Device Status via the Signal Contact”).

9.2.1 Configuring the Device Status

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

`enable`	Change to the privileged EXEC mode.
`configure`	Change to the Configuration mode.
`device-status monitor all error`	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.

Note: The above CLI commands activate the monitoring and the trapping respectively for all the supported components. If you want to activate or deactivate monitoring only for individual components, you will find the corresponding syntax in the CLI manual or in the help of the CLI console (enter a question mark “?“ at the CLI prompt).

9.2.2 Displaying the Device Status

☐ Select the `Basics:System` dialog.

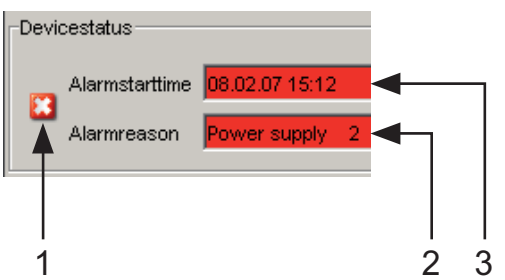


Figure 48: Device status and alarm display
1 - The symbol displays the device status
2 - Cause of the oldest existing alarm
3 - Start of the oldest existing alarm

`exit`	Change to the privileged 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 device. Function monitoring enables you to perform remote diagnostics.
The device reports the operating status via a break in the potential-free signal contact (relay contact, closed circuit):

- Incorrect supply voltage
  - at least one of the 2 supply voltages is not operating,
  - the internal supply voltage is not operating.
- The temperature threshold has been exceeded or has not been reached.
- The removal of a module (for modular devices).
- The removal of the ACA.
- The configuration on the external memory does not match that in the device.
- The interruption of the connection at at least one port. In the `Basic Settings:Port Configuration` menu, you define which ports the device signals if the connection is down (see on page 88 “Displaying detected loss of connection”). On delivery, there is no link monitoring.
- Events for ring redundancy:
  Loss of the redundancy (in ring manager mode). On delivery, ring redundancy monitoring is inactive.
  The device is a normal ring participant and detects an error in the local configuration.
- Event in the ring/network coupling:
  Loss of the redundancy. On delivery, there is no ring redundancy monitoring.
  The following conditions are also reported by the device in standby mode:
  – Defective link status of the control line
  – Partner device is in standby mode
- Failure of a fan (MACH 4000).

Select the corresponding entries to decide which events the device status includes.

Note: With a non-redundant voltage supply, the device reports the absence of a supply voltage. If you do not want this message to be displayed, feed the supply voltage over both inputs or switch off the monitoring (see on page 224 “Monitoring the Device Status via the Signal Contact”).

9.3.1 Controlling the Signal Contact

With this mode you control this signal contact remotely.

Application options:

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

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

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

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

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

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

9.3.2 Monitoring the Device Status via the Signal Contact

The "Device Status" option enables you, like in the operation monitoring, to monitor the device state (see on page 224 “Monitoring the Device Status via the Signal Contact”) via the signal contact.

9.3.3 Monitoring the Device Functions via the Signal Contact

Configuring the operation monitoring

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

`enable`	Switch to the privileged 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’s status

The device gives you 3 additional options for displaying the status of the signal contact:

- LED display on device,
- display in the graphical user interface,
- query in the Command Line Interface.

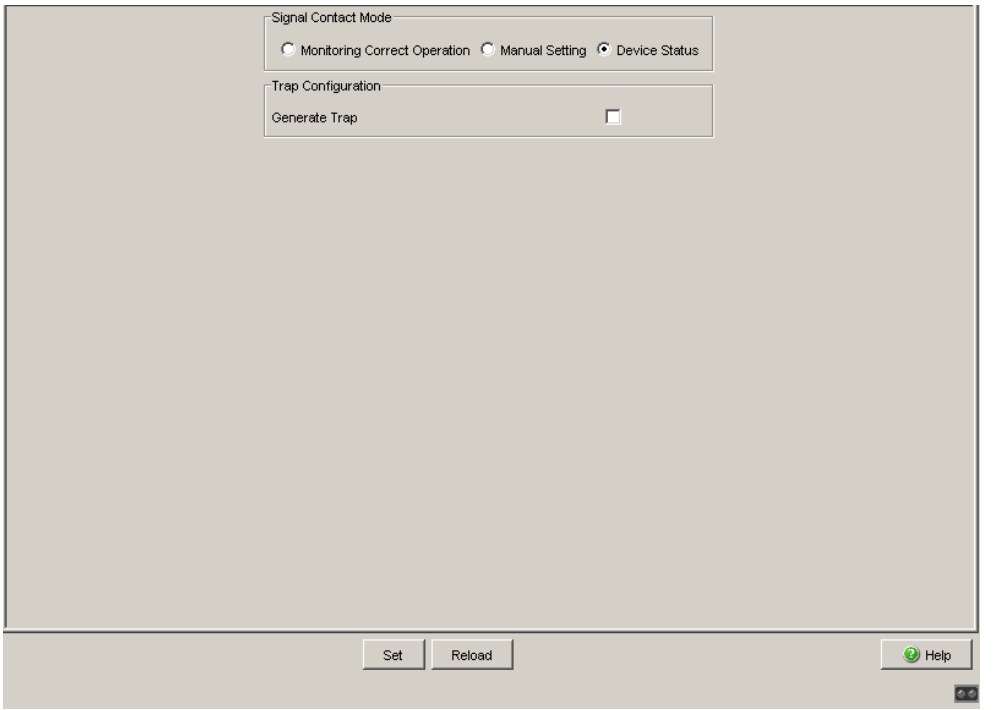


Figure 49: Signal Contact dialog

```
exit
show signal-contact 1
```

Change to the privileged EXEC mode.
Displays the status of the operation monitoring and the setting for the status determination.

9.3.4 Monitoring the Fan

Devices in the Mach 4000 family have a replaceable plug-in fan unit. This plug-in fan helps considerably in reducing the internal temperature of the device.
Fans are subject to natural wear. The failure of one or more fans in the plug-in fan can have a negative effect on the operation and life span of the device, or can lead to a total failure of the device.

The device enables you

- to signal changes to the status of the plug-in fan out-of-band (outside the data flow) via a signal contact (see on page 224 “Monitoring the Device Status via the Signal Contact”)
- to signal changes to the status of the plug-in fan by sending a trap when the device status changes
- to detect status changes to the plug-in fan in the Web-based interface on the system side and
- to query changes to the status of the plug-in fan in the Command Line Interface.

Proceed as follows to signal changes to the fan status via a signal contact and with an alarm message:

- ☐ Select the `Diagnostics:Signal Contact` dialog.
- ☐ Select the signal contact you want to use (in the example, signal contact 1) in the corresponding tab page “Signal contact 1” or “Signal contact 2”.
- ☐ In the “Signal contact mode” frame, select “Function monitoring”.
- ☐ In the “Function monitoring” frame, select the fan monitoring.
- ☐ Click "Set" to save the changes temporarily.
- ☐ Select the `Basics: Load/Save` dialog.
- ☐ In the “Save” frame, select “To Device” for the location and click “Save” to permanently save the configuration in the active configuration.

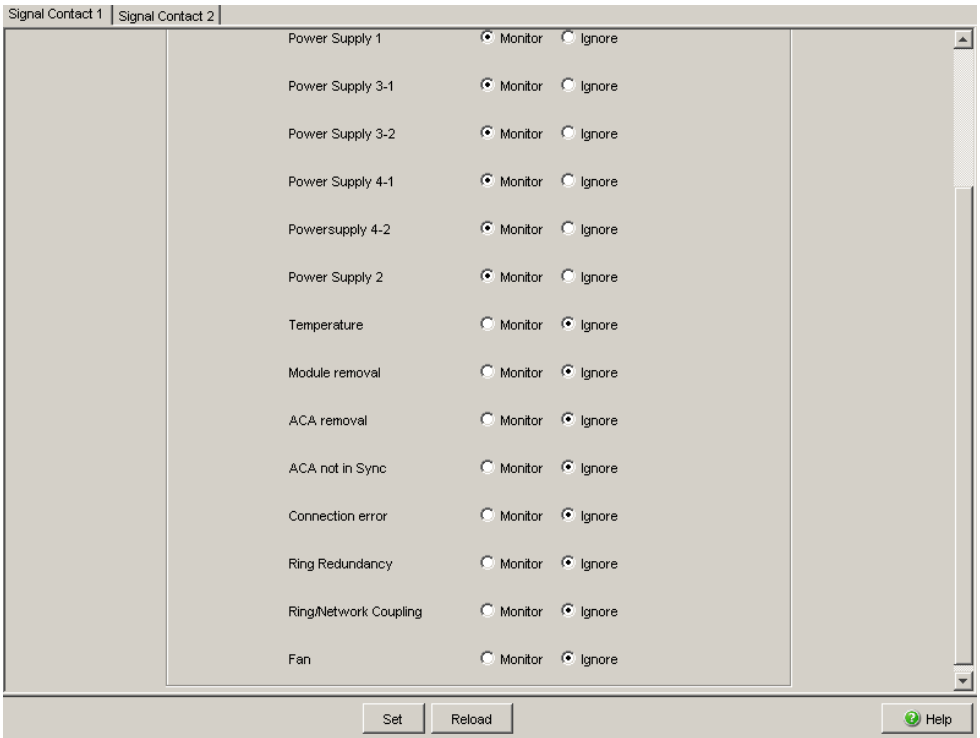


Figure 50: Monitoring the fan with the signal contact and trap

9.4 Port Status Indication

☐ Select the `Basics:System` dialog.

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

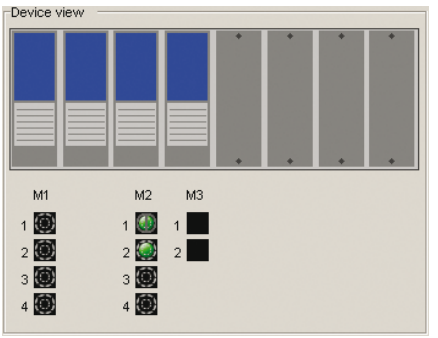


Figure 51: Device View

Meaning of the symbols:

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

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

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

The port is in autonegotiation mode.

The port is in HDX mode.

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

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

9.5 Event Counter at Port Level

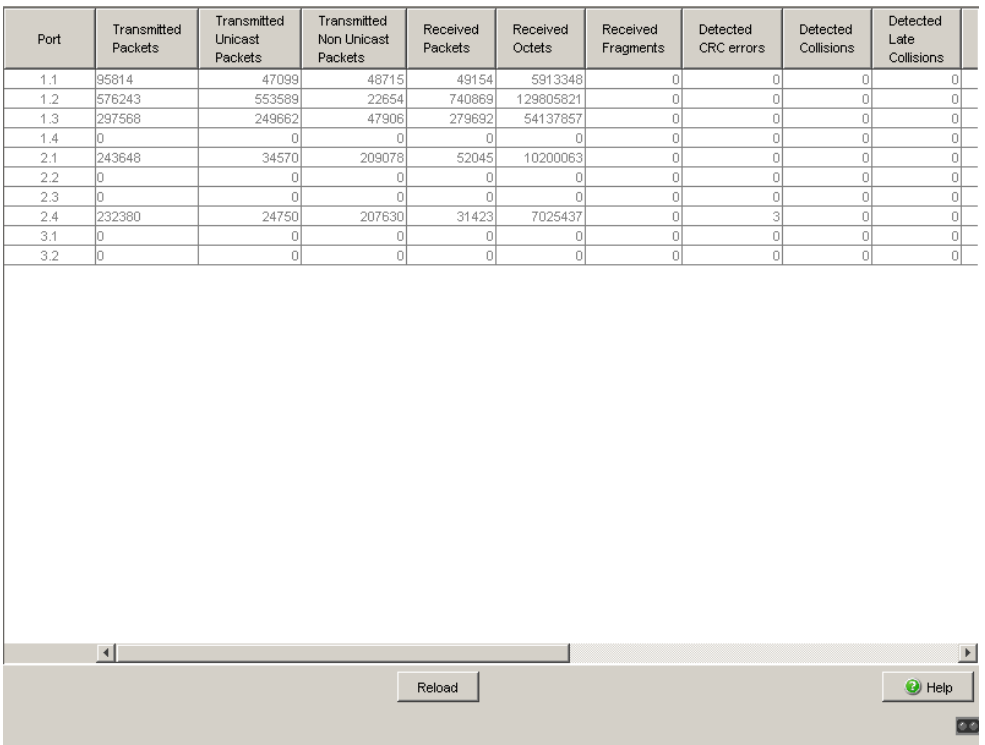
The port statistics table enables experienced network administrators to identify possible detected problems in the network.
This table shows you the contents of various event counters. In the Restart menu item, you can reset the event counters to zero using "Warm start", "Cold start" or "Reset port counter".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

Counter	Indication of known possible weakness
Received fragments	– Non-functioning controller of the connected device – Electromagnetic interference in the transmission medium
CRC error	– Non-functioning controller of the connected device – Electromagnetic interference in the transmission medium – Inoperable component in the network
Collisions	– Non-functioning controller of the connected device – Network over extended/lines too long – Collision or a detected fault with a data packet

Table 27: Examples indicating known weaknesses

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

☐ To reset the counters, click on “Reset port counters” in the Basic Settings:Restart dialog.



Port	Transmitted Packets	Transmitted Unicast Packets	Transmitted Non Unicast Packets	Received Packets	Received Octets	Received Fragments	Detected CRC errors	Detected Collisions	Detected Late Collisions
1.1	95814	47099	48715	49154	5913348	0	0	0	0
1.2	576243	553589	22654	740869	129805821	0	0	0	0
1.3	297568	249662	47906	279692	54137857	0	0	0	0
1.4	0	0	0	0	0	0	0	0	0
2.1	243648	34570	209078	52045	10200063	0	0	0	0
2.2	0	0	0	0	0	0	0	0	0
2.3	0	0	0	0	0	0	0	0	0
2.4	232380	24750	207630	31423	7025437	0	3	0	0
3.1	0	0	0	0	0	0	0	0	0
3.2	0	0	0	0	0	0	0	0	0

Figure 52: Port Statistics dialog

9.5.1 Detecting Non-matching Duplex Modes

If the duplex modes of 2 ports directly connected to each other do not match, this can cause problems that are difficult to track down. The automatic detection and reporting of this situation has the benefit of recognizing it before problems occur.

This situation can arise from an incorrect configuration, e.g. if you deactivate the automatic configuration at the remote port.

A typical effect of this non-matching is that at a low data rate, the connection seems to be functioning, but at a higher bi-directional traffic level the local device records a lot of CRC errors, and the connection falls significantly below its nominal capacity.

The device allows you to detect this situation and report it to the network management station. In the process, the device evaluates the error counters of the port in the context of the port settings.

Possible causes of port error events

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

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

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

Table 28: Evaluation of non-matching of the duplex mode

No.	Automatic configuration	Current duplex mode	Detected error events (≥ 10 after link up)	Duplex modes	Possible causes
15	Off	Full duplex	Late collisions	OK	EMI
16	Off	Full duplex	CRC error	Duplex problem detected	Duplex problem, EMI

Table 28: Evaluation of non-matching of the duplex mode (cont.)

Activating the detection

☐ Select the Switching:Switching Global dialog.

☐ Select “Activate Duplex Mismatch Detection”. The device then checks whether the duplex mode of a port might not match that of the remote port.
If the device detects a potential mismatch, it creates an entry in the event log and sends an alarm (trap).

`enable`	Change to the privileged EXEC mode.
`configure`	Change to the Configuration mode.
`bridge duplex-mismatch-detect operation enable`	Activates the detection and reporting of non-matching duplex modes.
`bridge duplex-mismatch-detect operation disable`	Deactivates the detection and reporting of non-matching duplex modes.

9.5.2 TP Cable Diagnosis

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

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

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

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

Table 29: Meaning of the possible results

Prerequisites for correct TP cable diagnosis:

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

9.5.3 Port Monitor

When you enable this feature the device monitors the port states. The device offers you the ability to disable individual ports or send a trap when user-defined conditions occur.

Definable port conditions are:
- Link Flap
- CRC/Fragments
- Overload Detection
- Speed and duplex combination

In the Global dialog, you activate the configurations defined in the "Link Flap", "CRC/Fragments" and "Overload Detection" tabs. The device detects these conditions when you activate the functions. If the device detects the user defined condition on a port, it produces the response defined for that port.

Link Flapping occurs when a link alternately advertises its link state as up and down. You configure the device to detect this condition and then define whether to send a trap or shut the port off.

Using the Cyclical Redundancy Check (CRC) the device detects data packets modified during the transmission based on the checksum. The device detects the total number of packets received that were less than 64 octets in length, excluding framing bits, but including FCS octets, and had either a FCS error or an Alignment Error.
- A FCS error is a bad Frame Check Sequence (FCS) with an integral number of octets.
- An Alignment Error is a bad FCS with a non-integral number of octets.

The device monitors both criteria if you enable the function in the "Global" tab. If the number of occurred CRC/fragment errors exceeds the specified threshold, the device executes the user-specified action.

Overload Detection prevents a broadcast, multicast, or unicast storm from disrupting traffic on a port. The Overload Detection function monitors packets passing from a port to the switching bus to determine if the packet is unicast, multicast, or broadcast. The switch counts the number of user-defined packets received within the "Sampling Interval "and compares the measurement with a user-defined threshold. The port blocks traffic after reaching the "Upper Threshold". When you activate the recovery function for Overload Detection, the port remains blocked until the traffic rate drops below the "Lower Threshold" and then forwards traffic as normal.

The device allows you to define which duplex mode is allowed for which speed for a specific port. The monitoring of the combination of speed and duplex mode prevents any undesired connections.

- ☐ Open the `Diagnositics:Ports:Port Monitor` dialog.

- ☐ Open the "Link Flap" tab.
- ☐ Define the number of times that a port cycles between link up and link down before the function disables the port, in the "Link Flap Count" text box, in the "Parameter" frame.
- ☐ Define the elapse time in the "Sample Interval [s]" text box in the "Parameter" frame.

- ☐ Open the "CRC/Fragments" tab.
- ☐ Define the number of packets received containing changes in raw data or fragment packets received before the function disables the port, in the "CRC/Fragments count [ppm]" text box, in the "Parameter" frame.
- ☐ Define the elapse time in the "Sample Interval [s]" text box in the "Parameter" frame.

- ☐ Open the "Overload Detection" tab.
- ☐ Define the elapse time in the "Sample Interval [s]" text box in the "Parameter" frame.
- ☐ For each port, define the type of traffic to monitor in the "Traffic Type" column.
- ☐ For each port, define the type of threshold to use in the "Threshold Type" column.
- ☐ For each port, define the threshold at which the device enables the port in the "Lower Threshold" column.
- ☐ For each port, define the threshold at which the device disables the port in the "Upper Threshold" column.

- ☐ Open the "Speed Duplex" tab.

☐ You define for each port which duplex mode is allowed for which speed.
- "hdx" = half duplex
- "fdx" = full duplex
- "10" = 10 Mbit/s
- "100" = 100 Mbit/s

etc.

☐ Open the "Global" tab.
☐ In the "Port Monitor on" column of the "Global" tab, select the ports to monitor.
☐ To activate the Port Monitor function, click `On` in the "Operation" frame.

9.5.4 Auto Disable

If the configuration shows a port as enabled, but the device detects an error, the software shuts down that port. In other words, the device software disables the port because of a detected error condition.

When a port is auto-disabled, the device effectively shuts down the port and the port blocks traffic. The port LED blinks green 3 times per period and identifies the reason for the shutdown. In addition, the device generates a log entry listing the reason for the auto-disable. When you enable the port after a timeout by auto-disable, the device generates a log entry.

This feature provides a recovery function which automatically enables an auto-disabled port after a user-defined time. When this function enables a port, the device sends a trap with the port number and an empty "Reason" entry.

The auto-disable function serves the following purposes:
- It assists the network administrator in port analysis.
- It eliminates the possibility that this port causes other ports on the module (or the entire module) to shut down.

Note: The "Reset" button allows you to enable the port before the "Reset Timer [s]" counts down.

So that the device enables the ports again that were disabled because of a detected error state, complete the following steps:

- ☐ Open the `Diagnositics:Ports:Auto Disable` dialog.
- ☐ To enable ports again that the device has disabled due to link flaps, in the "Configuration" frame mark the "Link Flap" checkbox.
  You define the parameters that cause the ports to be disabled due to link flaps in the `Diagnostics:Ports:Port Monitor` dialog, on the "Link Flap" tab.

- ☐ To enable ports again that the device has disabled due to CRC or fragment errors, on the "Configuration" frame mark the "CRC Error" checkbox.
  You define the parameters that cause the ports to be disabled due to CRC or fragment errors in the `Diagnostics:Ports:Port Monitor` dialog, on the "CRC/Fragments" tab.
- ☐ To enable ports again that the device has disabled due to an overload, in the "Configuration" frame mark the "Overload Detection" checkbox.
  You define the parameters that cause the ports to be disabled due to an overload in the `Diagnostics:Ports:Port Monitor` dialog, on the "Overload Detection" tab.
- ☐ To enable ports again that the device disabled due to an incorrect speed and duplex combination, in the "Configuration" frame mark the "Speed Duplex" checkbox.
  You define the parameters that cause the ports to be disabled due to an incorrect speed and duplex combination in the `Diagnostics:Ports:Port Monitor` dialog, on the "Speed Duplex" tab.
- ☐ To enable ports again that the device disabled due to an unauthorized access to the port, in the "Configuration" frame you mark the "Port Security" checkbox.
  You define the parameters that cause the ports to be disabled due to unauthorized access in the `Security:Port Security` dialog.
- ☐ You define the time until each port is automatically enabled again in the "Reset Timer [s]" column in the table.

9.6 Displaying the SFP Status

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

- module type
- support provided in media module
- temperature in ° C
- transmission power in mW
- receive power in mW

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

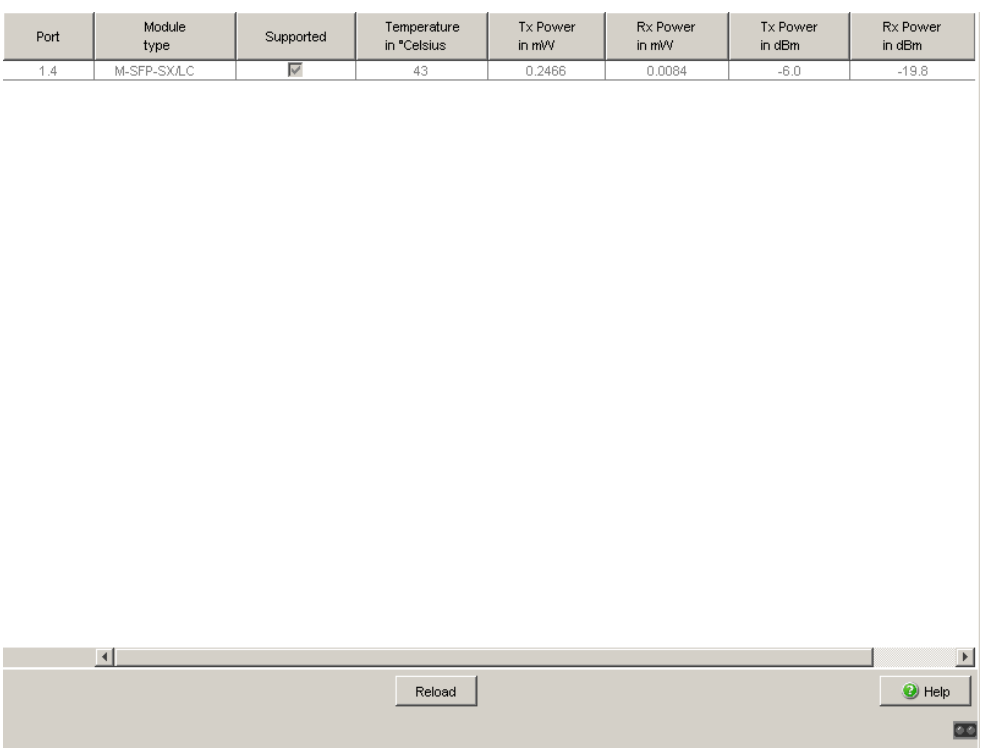


Figure 53: SFP Modules dialog

9.7 Topology Discovery

9.7.1 Description of Topology-Detection

IEEE 802.1AB defines the Link Layer Discovery Protocol (LLDP). LLDP allows the user to automatically detect the LAN network topology.

Devices with LLDP active

- broadcast their connection and management information to adjacent devices on the shared LAN. These devices can then be evaluated provided they also have LLDP active.
- receive connection and management information from adjacent devices on the shared LAN, provided these devices also have LLDP active.
- builds a management-information table and object definitions for storing information about adjacent devices with LLDP active.

As the main element, the connection information contains an exact, unique identifier for the connection end point: MSAP (MAC Service Access Point). This is made up of a device identifier which is unique on the entire network and a unique port identifier for this device.
Content of the connection and management-information:

- Chassis identifier (its MAC address)
- Port identifier (its port-MAC address)
- Description of port
- System name
- System description
- Supported system capabilities
- System capabilities currently active
- Interface ID of the management address
- VLAN-ID of the port
- Auto-negotiation status at the port
- Medium, half/full duplex setting and port speed setting

- Indication whether a redundancy protocol is enabled at the port, and which one (e.g. RSTP, HIPER-Ring, FastHIPER Ring, MRP, ring coupling).
- Information about the VLANs installed in the device (VLAN-ID and VLAN name, irrespective of whether the port is a VLAN participant).

A network management station can query this information from devices that have LLDP active. This information allows the network management station to form a description of the network topology.

For information exchanges, the LLDP uses an IEEE MAC address, which devices do not normally communicate. Devices without LLDP therefore do not allow support for LLDP packets. If a device without LLDP capability is located between two devices with LLDP capability, then LLDP information exchanges are prevented between these two devices. To work around this, Hirschmann devices send and receive additional LLDP packets with the Hirschmann Multicast-MAC address 01:80:63:2F:FF:0B. Hirschmann-Devices with the LLDP function are therefore able to exchange LLDP information with each other even across devices that do not have LLDP capability.

The Management Information Base (MIB) for a Hirschmann device with LLDP capability holds the LLDP information in the lldp MIB and in the private hmLLDP.

9.7.2 Displaying the Topology Discovery Results

☐ Select the `Diagnostics:Topology Discovery` dialog.
The table on the “LLDP” tab page shows you the collected LLDP information for neighboring devices. This information enables the network management station to map the structure of your network.

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

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

If
- devices with active topology discovery function and
- devices without active topology discovery function are connected to a port

then
- the topology table hides the devices without active topology discovery.

If
- only devices without active topology discovery are connected to a port

then
- the table will contain one line for this port to represent all devices. This line contains the number of connected devices.
  MAC addresses of devices that the topology table hides for the sake of clarity, are located in the address table (FDB), (see on page 158 “Entering Static Addresses”).

9.8 Detecting IP Address Conflicts

9.8.1 Description of IP Address Conflicts

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

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

Table 30: Possible address conflict operation modes

9.8.2 Configuring ACD

☐ Select the Diagnostics:IP Address Conflict Detection dialog.
☐ With "Status" you enable/disable the IP address conflict detection or select the operating mode (see table 30).

9.8.3 Displaying ACD

☐ Select the `Diagnostics:IP Address Conflict Detection` dialog.
▶ In the table, the device logs IP address conflicts with its IP address. The device logs the following data for each conflict:
  ▶ the time („Timestamp“ column)
  ▶ the conflicting IP address („IP Address“ column)
  ▶ the MAC address of the device with which the IP address conflicted („MAC Address“ column).

  For each IP address, the device logs a line with the last conflict that occurred.
☐ During a restart, the device deletes the table.

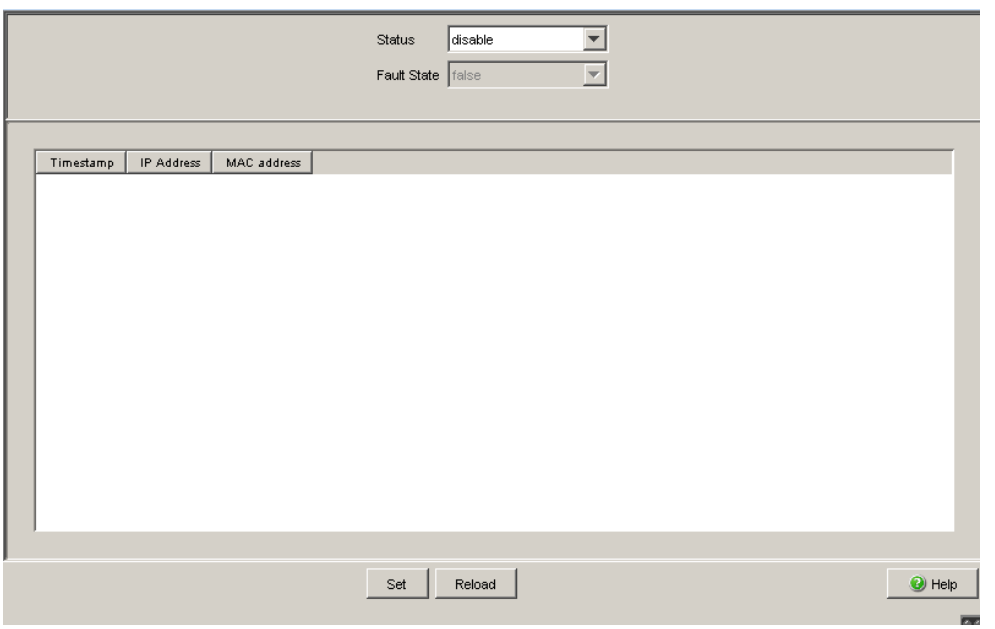


Figure 54: IP Address Conflict Detection dialog

9.9 Detecting Loops

Loops in the network, even temporary loops, can cause connection interruptions or data losses that may cause unintended equipment operation. The automatic detection and reporting of this situation allows you to detect it faster and diagnose it more easily.

An incorrect configuration can cause a loop, for example, if you deactivate Spanning Tree.

The device allows you to detect the effects typically caused by loops and report this situation automatically to the network management station. You have the option here to specify the magnitude of the loop effects that triggers the device to send a report.

A typical effect of a loop is that frames from multiple different MAC source addresses can be received at different ports of the device within a short time. The device evaluates how many of the same MAC source addresses it has learned at different ports within a time period. This process detects loops when the same MAC address is received at different ports.
Conversely, the same MAC address being received at different ports can also have other causes than a loop.

☐ Select the `Switching:Switching Global` dialog.
☐ Select “Enable address relearn detection”. Enter the desired threshold value in the “Address relearn threshold” field.

If the address relearn detection is enabled, the device checks whether it has repeatedly learned the same MAC source addresses at different ports. This process very probably indicates a loop situation.
If the device detects that the threshold value set for the MAC addresses has been exceeded at its ports during the evaluation period (a few seconds), the device creates an entry in the log file and sends an alarm (trap). The preset threshold value is 1.

9.10 Reports

The following reports and buttons are available for the diagnostics:

- Log file.
  The log file is an HTML file in which the device writes all the important device-internal events.
- System information.
  The system information is an HTML file containing the system-relevant data.
- Download Support Information.
  This button allows you to download system information as files in a ZIP archive.

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

The following button is available as an alternative for operating the Web-based interface:

- Download JAR file.
  This button allows you to download the applet of the Web-based interface as a JAR file. Then you have the option to start the applet outside of a browser.
  This facilitates the device administration even when you have disabled its web server for security reasons.

☐ To display the HTML file with system-relevant data, select the dialog `Diagnosis:Report:System Information`.
☐ To view the log file with important device-internal events, select the dialog `Diagnosis:Report:Event Log`.

☐ Select the `Diagnosis:Report` dialog.

☐ Click “Download Switch Dump”.

☐ Select the directory in which you want to save the switch dump.

☐ Click “Save”.

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

☐ Click “Download JAR-File”.

☐ Select the directory in which you want to save the applet.

☐ Click “Save”.

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

9.11 Monitoring Data Traffic on the Ports (Port Mirroring)

The MACH4002 24/48 + 4G and the Power MICE support up to 8 ports.

The port mirroring function enables you to review the data traffic from a group of ports on the device for diagnostic purposes (N:1). The device forwards (mirrors) the data for these ports to another port. This process is port mirroring.
The ports from which the device copies the traffic are source ports. The port on which you review the data is the destination port. You use physical ports as source or destination ports.

In port mirroring, the device copies valid data packets of the source port to the destination port. The device does not affect the data traffic on the source ports during port mirroring.
A management tool connected at the destination port, e.g. an RMON probe, can thus monitor the data traffic of the source ports in the sending and receiving directions.

When selecting "RX" as the monitoring direction on a source port, only frames received on the source port will be copied/mirrored to the destination port (monitoring ingress).
When selecting "TX" as the monitoring direction on a source port, only frames transmitted on the source port will be copied/mirrored to the destination port (monitoring egress).

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

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

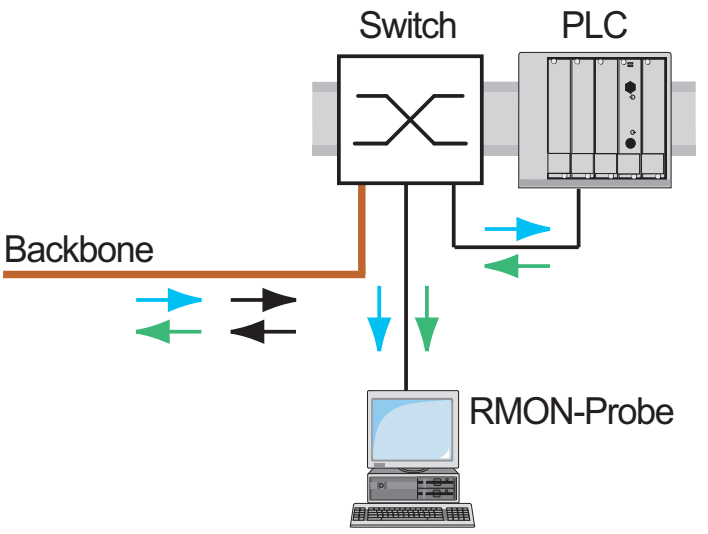


Figure 55: Port mirroring

☐ Select the `Diagnostics:Port Mirroring` dialog.

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

- ☐ Select the source ports whose data traffic you want to review from the physical ports list by checkmarking the relevant boxes.
  The device displays the "Source Port" currently used as the "Destination Port" as grayed out in the table. Default setting: no source ports.
- ☐ Select the destination port to which you have connected your management tool from the drop-down menu in the "Destination Port" frame.
  Selecting a destination port is mandatory for a valid port mirroring configuration. The drop-down menu displays available ports exclusively, for example, the list excludes the ports currently in use as source ports. Default setting: port - (no destination port).
- ☐ To select the monitoring traffic direction, checkmark the relevant "RX" and "TX" boxes for ingress and egress monitoring directions.
- ☐ To switch on the function, select `On` in the "Operation" frame. Default setting: `Off`.

The “Reset configuration” button in the dialog allows you to reset all the port mirroring settings of the device to the state on delivery.

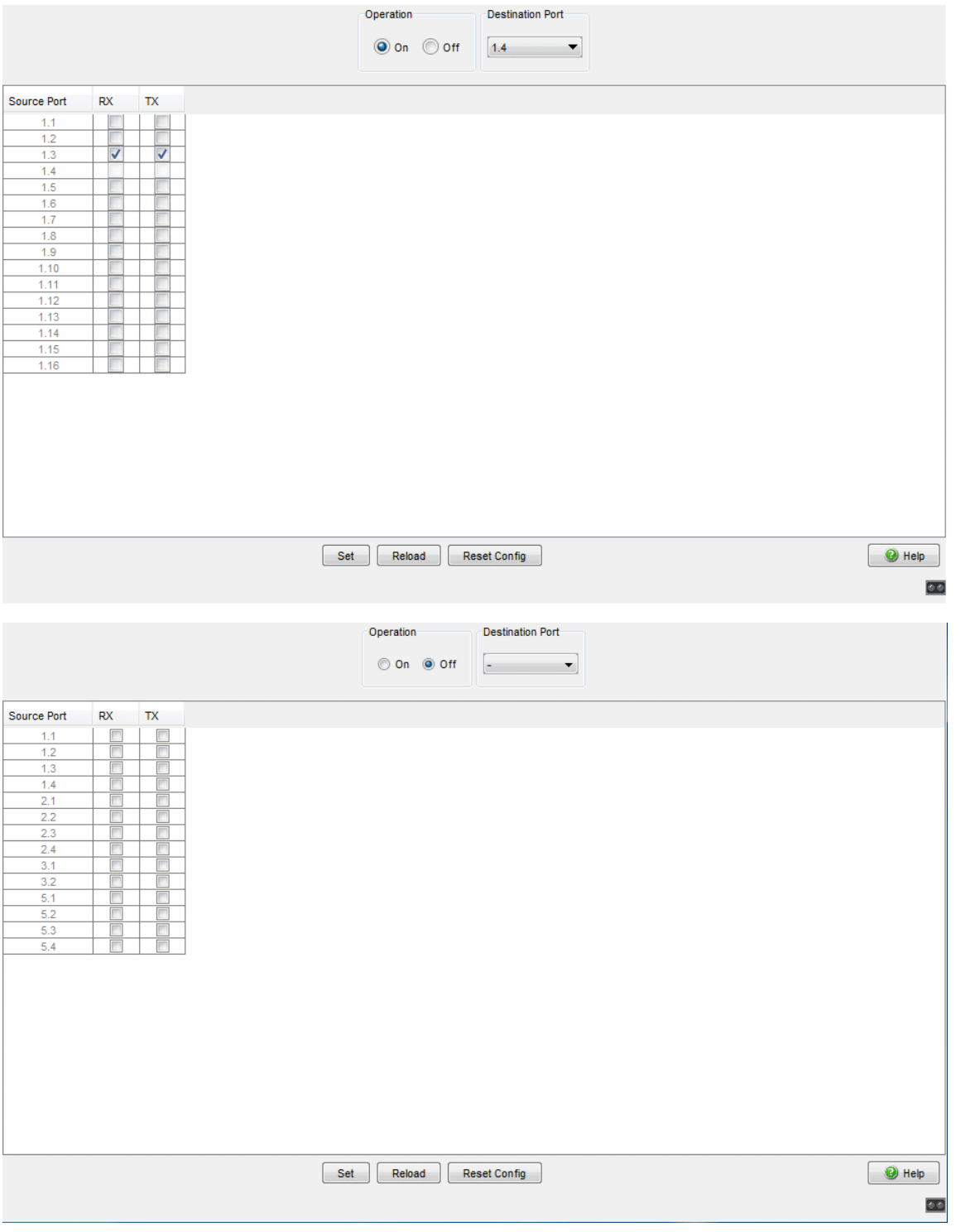


Figure 56: Port Mirroring dialog

9.12 Syslog

The device enables you to send messages about important device-internal events to one or more syslog servers (up to 8). Additionally, you can also include SNMP requests to the device as events in the syslog.

Note: You will find the actual events that the device has logged in the “Event Log” (see on page 256 “Trap log”) and in the log file (see on page 247 “Reports”), a HTML page with the title “Event Log”.

☐ Select the `Diagnostics:Syslog` dialog.

☐ Activate the syslog function in the “Operation” frame.
☐ Click on “Create”
☐ In the “IP Address” column, enter the IP address of the syslog server to which the log entries should be sent.
☐ In the “Port” column, enter the UDP port of the syslog server at which the syslog receives log entries. The default setting is 514.
☐ In the “Minimum level to report” column, you enter the minimum level of seriousness an event must attain for the device to send a log entry to this syslog server.
☐ In the “Active” column, you select the syslog servers that the device takes into account when it is sending logs.

"SNMP Logging" frame:

- ☐ Activate "Log SNMP Get Request" if you want to send reading SNMP requests to the device as events to the syslog server.
- ☐ Select the level to report at which the device creates the events from reading SNMP requests.
- ☐ Activate "Log SNMP Set Request" if you want to send writing SNMP requests to the device as events to the syslog server.
- ☐ Activate "Log SNMP Set Request" if you want to send writing SNMP requests to the device as events to the syslog server.

Note: For more details on setting the SNMP logging, see the "Syslog" chapter in the "GUI" (Graphical User Interface / Web-based Interface) reference manual.

`enable`	Switch to the privileged 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 seriousness of the message sent by the device. "3" means "error".
`logging syslog`	Enable the Syslog function.
`exit`	Switch to the privileged EXEC mode.
`show logging hosts`	Display the syslog host settings.

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

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`logging snmp-requests get operation enable`	Create log events from reading SNMP requests.
`logging snmp-requests get severity 5`	The "5" indicates the seriousness of the message that the device allocates to messages from reading SNMP requests. "5" means "note".
`logging snmp-requests set operation enable`	Create log events from writing SNMP requests.
`logging snmp-requests set severity 5`	The "5" indicates the seriousness of the message that the device allocates to messages from writing SNMP requests. "5" means "note".
`exit`	Switch to the privileged EXEC mode.
`show logging snmp-requests`	Display the SNMP logging settings.

```
Log SNMP SET requests                : enabled
Log SNMP SET severity                : notice
Log SNMP GET requests                : enabled
Log SNMP GET severity                : notice
```

9.13 Trap log

The device allows you to call up a log of the system events. The table of the “Trap Log” dialog lists the logged events with a time stamp.

- ☐ Click “Reload” to update the content of the trap log.
- ☐ Click “Clear” to delete the content of the trap log.

Note: You have the option to also send the logged events to one or more syslog servers (see on page 253 “Syslog”).

9.14 MAC Notification

MAC notification, also known as MAC address change notification, tracks users on a network by storing the MAC address change activity. When the switch learns or removes a MAC address, the device sends an SNMP trap to a configured trap destination. The device generates MAC address change notifications for dynamic unicast MAC addresses.

The device buffer contains up to 20 addresses. If the buffer is full before the user -defined interval expires, then the device sends a trap to the management station.

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

- ☐ Open the `Diagnositics:MAC Notification` dialog.
- ☐ Select the activity for which the device sends a trap in the "Mode"column.
- ☐ To select the ports for which the device sends a trap, activate the checkbox in the "Enabled" column.
- ☐ Define the number of seconds between trap transmissions in the "Interval [s]" textbox.
- ☐ To enable the function, click `On` in the "Operation" frame.

`enable`	Change to the privileged EXEC mode.
`configure`	Change to the Configuration mode.
`mac notification interval 20`	Set MAC notification interval to 20 seconds.
`interface 1/1`	Change to the Interface Configuration mode of port 1/1.
`mac notification mode`	Set the mode for which the device sends a MAC notification.
`mac notification operation`	Enable sending of MAC notification traps for this port.
`exit`	Change to the Configuration mode.
`mac notification operation`	Enable the MAC notification function globally.

A Setting up the Configuration Environment

A.1 Setting up a DHCP/BOOTP Server

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

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

☐ Start the `DHCP Server` program.

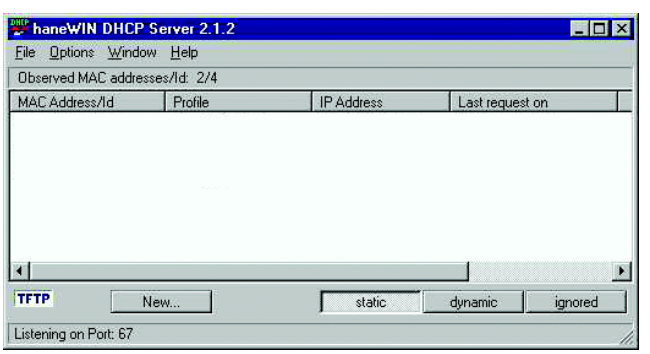


Figure 57: Start window of the DHCP server

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

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

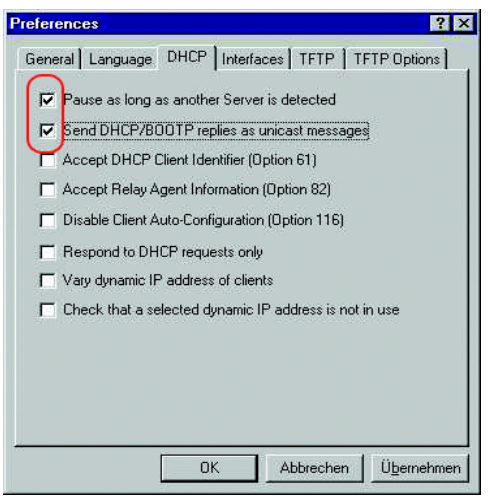


Figure 58: DHCP setting

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

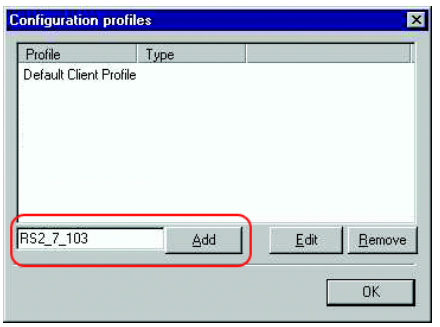


Figure 59: Adding configuration profiles

☐ Enter the netmask and click `Apply`.

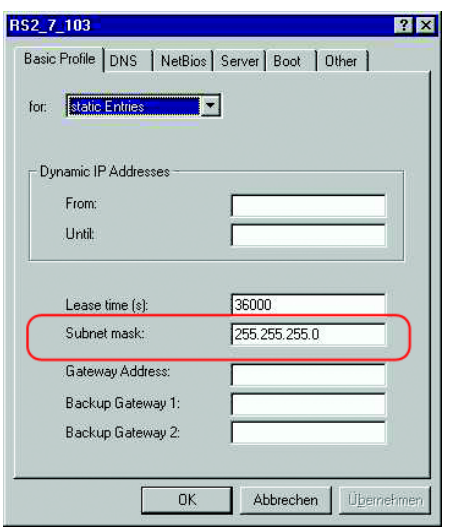


Figure 60: Netmask in the configuration profile

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

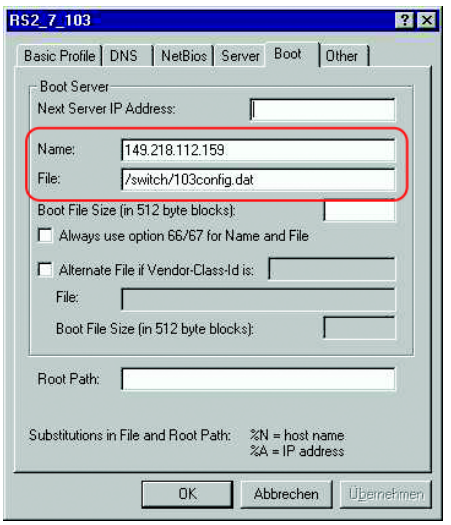


Figure 61: Configuration file on the tftp server

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

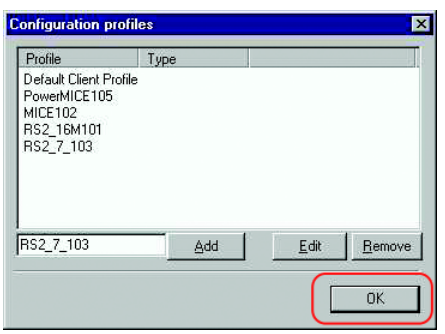


Figure 62: Managing configuration profiles

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

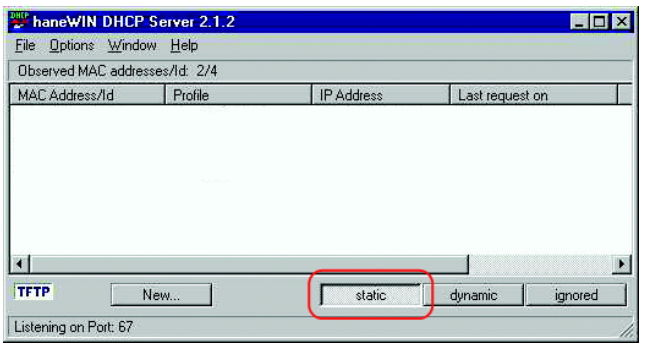


Figure 63: Static address input

☐ Click `New`.

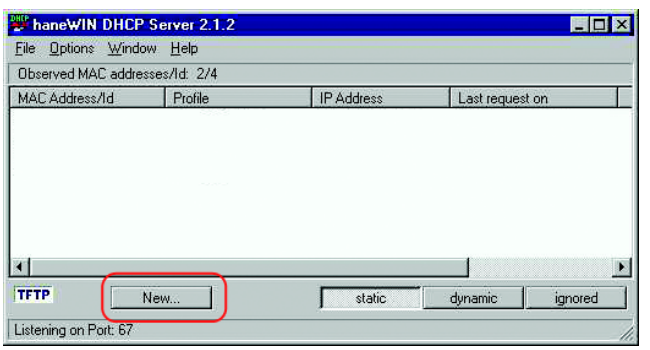


Figure 64: Adding static addresses

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

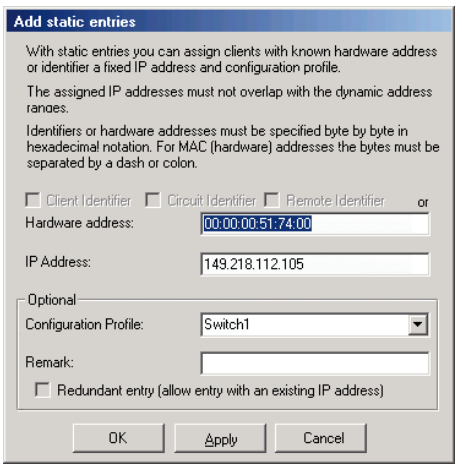


Figure 65: Entries for static addresses

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

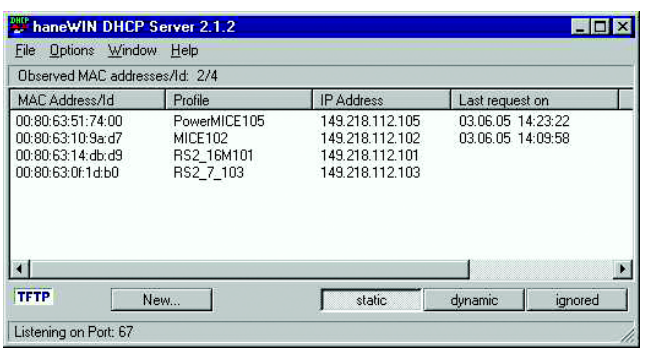


Figure 66: DHCP server with entries

A.2 Setting up a DHCP Server with Option 82

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

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

☐ Start the `DHCP Server` program.

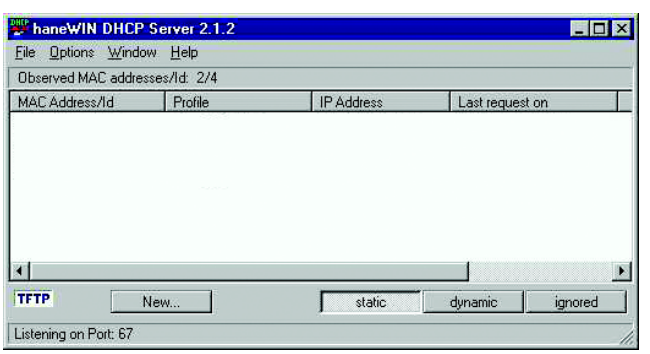


Figure 67: Start window of the DHCP server

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

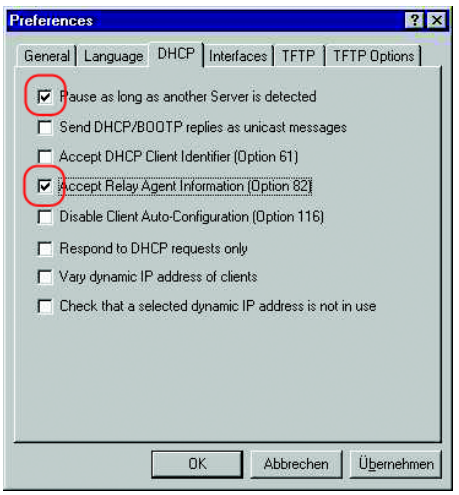


Figure 68: DHCP setting

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

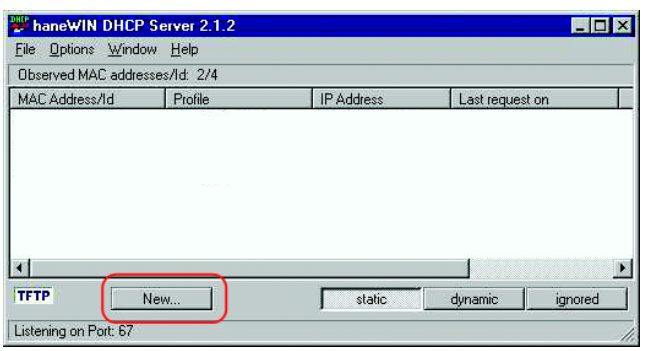


Figure 69: Adding static addresses

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

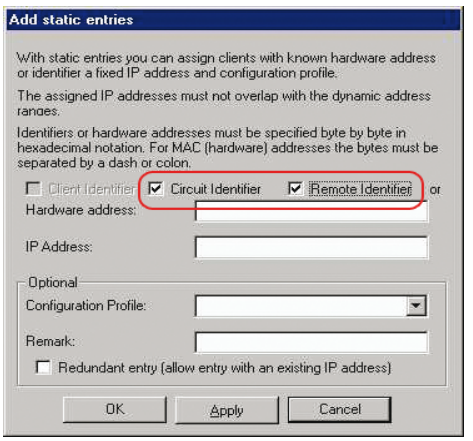


Figure 70: Default setting for the fixed address assignment

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

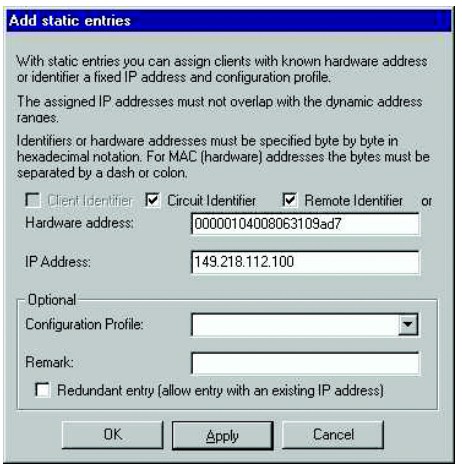


Figure 71: Entering the addresses

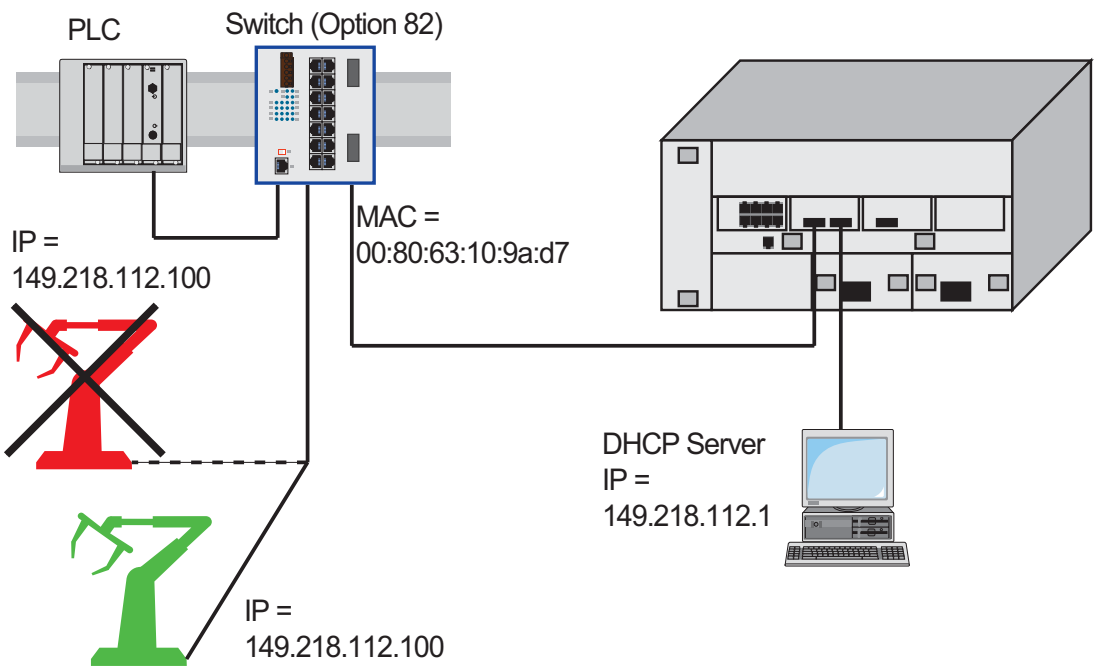


Figure 72: Application example of using Option 82

A.3 TFTP Server for Software Updates

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

Note: An alternative to the TFTP update is the HTTP update. The HTTP update saves you having to configure the TFTP server.

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

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

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

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

A.3.1 Setting up the TFTP Process

General prerequisites:

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

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

SunOS and HP

☐ First check whether the tftp daemon (background process) is running, i.e. whether the file /etc/inetd.conf contains the following line (see figure 73) and whether the status of this process is "IW":

SunOS

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

HP

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

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

SunOS

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

HP

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

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

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

Special steps for HP workstations:

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

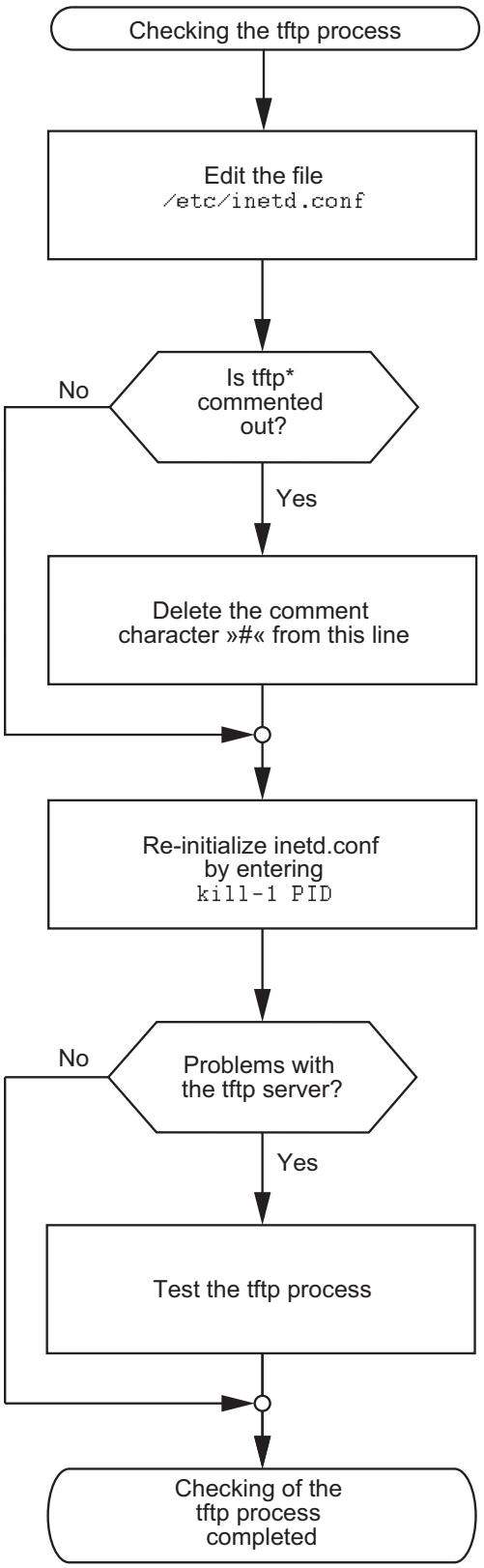
For example:

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

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

☐ Test the tftp process with, for example:`cd /tftpboot/device`

```
tftp <tftp-Servername>
get device/device.bin
rm device.bin
```



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

Response if the process is running: `Received ...`

`rm device.bin`

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

Figure 73: Flow chart for setting up TFTP server with SunOS and HP

A.3.2 Software Access Rights

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

Example of a UNIX tftp Server

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

File name	Access
device.bin	-rw-r--r--

Table 31: Directory structure of the software

l = link; d = directory; r = read; w = write; x = execute
1st position denotes the file type (- = normal file),
2nd to 4th positions designate user access rights,
5th to 7th positions designate access rights for users from other groups,
8th to 10th positions designate access rights of every other user.

A.4 Preparing access via SSH

To be able to access the device via SSH, perform the following steps:

- Generate a key (SSH host key).
- Install the key on the device.
- Enable access via SSH on the device.
- Install a program for executing the SSH protocol (SSH client) on your computer.

A.4.1 Generating a key

The device gives you the option to use your own self-generated keys for the SSH server. If there is no SSH key on the device, the device generates the required keys automatically when the SSH server is switched on for the first time.

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

☐ Start the program by double-clicking on it.
☐ In the “Parameters” frame you select the type of key to be generated.
  ☐ To generate a key for SSH version 2, you select "SSH-2 (RSA)" or "SSH-2 (DSA)".
  ☐ To generate a key for SSH version 1, you select "SSH-1 (RSA)".
☐ Make sure that the field "Number of bits in a generated key" in the "Parameters" frame is showing the value `1024`.
☐ In the "Actions" box, click on "Generate". Move the mouse pointer over the PuTTYgen-window, so that PuTTYgen can create the key using random numbers.
☐ Leave the "Key passphrase" and "Confirm passphrase" input boxes empty.

- ☐ Save the key:
  - ☐ To save a key for SSH version 2, click the `Conversions:Export OpenSSH key` menu.
  - ☐ To save a key for SSH version 1, click the "Save private key" button in the "Actions" frame.
- ☐ Answer the question about saving the key without a passphrase with "Yes".
- ☐ Select the Save location and enter a file name for the key file.
- ☐ Note down the key fingerprint, so that you can check it when establishing a connection.
- ☐ You should also store the key in a location separate from the device so that, if the device is being replaced, the key can be transferred to the new device.

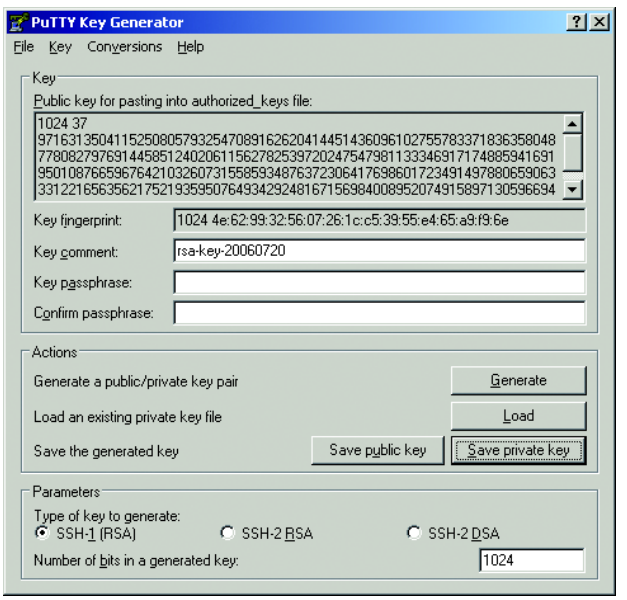


Figure 74: PuTTY key generator

For experienced network administrators, another way of creating the key is with the OpenSSH Suite. To generate the key, enter the following command:

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

A.4.2 Loading a key onto the device

You load the SSH key onto the device with the Command Line Interface via TFTP.

SSH version 1 works with an RSA key. However, SSH version 2 works with an RSA key and a DSA key. For SSH version 2, you always load both keys to the device.

☐ Store the keys on your tftp server.

☐ Load the keys from the tftp server onto the device.

`enable`	Switch to the privileged EXEC mode.
`no ip ssh`	Deactivates the SSH server.
`copy tftp://ip/filepath/key nvram:sshkey-rsa2`	Loads the key to the non-volatile memory of the device. ▶ `nvram:sshkey-rsa2` is the storage location of the RSA key for SSH version 2. ▶ `nvram:sshkey-dsa` is the storage location of the DSA key for SSH version 2. ▶ `nvram:sshkey-rsa1` is the storage location of the RSA key for SSH version 1.
`copy tftp://ip/filepath/key nvram:sshkey-dsa`	
`copy tftp://ip/filepath/key nvram:sshkey-rsa1`	
`ip ssh`	Activates the SSH server.

A.4.3 Access through an SSH

One way of accessing your device through an SSH is by using the PuTTY program. This program is provided on the product-CD.

☐ Start the program by double-clicking on it.
☐ Enter the IP address of your device.
☐ Select "SSH".

☐ Click on "Open" to set up the connection to your device.

Depending on the device and the time at which SSH was configured, it can take up to a minute to set up the connection.

Just before the connection is established, the PuTTY program displays a security alarm message and gives you the option of checking the key fingerprint.

Figure 75: Security alert prompt for the fingerprint

☐ Check the fingerprint of the key to ensure that you have actually connected to the desired device. You will find the fingerprint of your key in the "Key fingerprint" field of the PuTTY key generator.
☐ If the fingerprint matches your key, click on "Yes".

PuTTY also displays another security alarm message at the defined warning threshold.

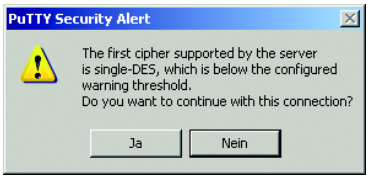


Figure 76: Security query at the defined warning threshold

☐ Click on "Yes" in the security alarm message.

To suppress this message when establishing subsequent connections, select "SSH" in the "Category" box in the PuTTY program before opening the connection. In the "Encryption options" box, select "DES" and click on "Up" until "DES" comes above the line "-- warn below here --". In the "Category" box, switch back to "Session" and establish the connection as usual.

For experienced network administrators, another way of accessing your device through an SSH is by using the OpenSSH Suite. To open the connection, enter the following command:

```
ssh admin@10.0.112.53 -cdes
```

- `admin` for the user name.
- `10.0.112.53` is the IP address of your device.
- `-cdes` sets the encryption type for SSHv1.

A.5 HTTPS Certificate

The encryption of HTTPS connections requires an X.509 certificate. The device allows you to use your own X.509 certificate. If there is no X.509 certificate on the device, the device generates this automatically when the HTTPS server is switched on for the first time.

You load your own X.509 certificate onto the device with the Command Line Interface via TFTP.

☐ Store the certificate on your tftp server.

☐ Load the certificate from the tftp server onto the device.

`enable`	Change to the privileged EXEC mode.
`no ip https`	Deactivates the HTTPS function before transferring the certificate to the device.
`copy tftp://ip/filepath/cert nvram:httpscert`	Loads the certificate to the non-volatile memory of the device. `nvram:httpscert` is the storage location of the X.509 certificate.
`ip https`	Activates the HTTPS function after transferring the certificate to the device.

A.6 Service Shell

When you need assistance with your device, then the service personnel use the Service Shell function to monitor internal conditions, for example switch or CPU registers.

The CLI Reference Manual contains a description of deactivating the Service Shell.

Note: When you deactivate the Service Shell, then you are still able to configure the device, but you limit the service personnel to system diagnostics. In order to reactivate the Service Shell function, the device requires disassembly by the manufacturer.

B General Information

B.1 Management Information Base (MIB)

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

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

The following abbreviations are used in the MIB:	
Comm	Group access rights
con	Configuration
Descr	Description
Fan	Fan
ID	Identifier
Lwr	Lower (e.g. threshold value)
PS	Power supply
Pwr	Power supply
sys	System

The following abbreviations are used in the MIB:	
UI	User interface
Upr	Upper (e.g. threshold value)
ven	Vendor = manufacturer (Hirschmann)

Definition of the syntax terms used:	
Integer	An integer in the range -2^{31} - 2^{31}-1
IP Address	xxx.xxx.xxx.xxx (xxx = integer in the range 0-255)
MAC Address	12-digit hexadecimal number in accordance with ISO/IEC 8802-3
Object identifier	x.x.x.x… (e.g. 1.3.6.1.1.4.1.248...)
Octet string	ASCII character string
PSID	Power supply identifier (number of the power supply unit)
TimeTicks	Stopwatch, Elapsed time (in seconds) = numerical value / 100 Numerical value = integer in range 0-2^{32}-1
Timeout	Time value in hundredths of a second Time value = integer in range 0-2^{32}-1
Type field	4-digit hexadecimal number in accordance with ISO/IEC 8802-3
Counter	Integer (0-2^{32-1}), whose value is increased by 1 when certain events occur.

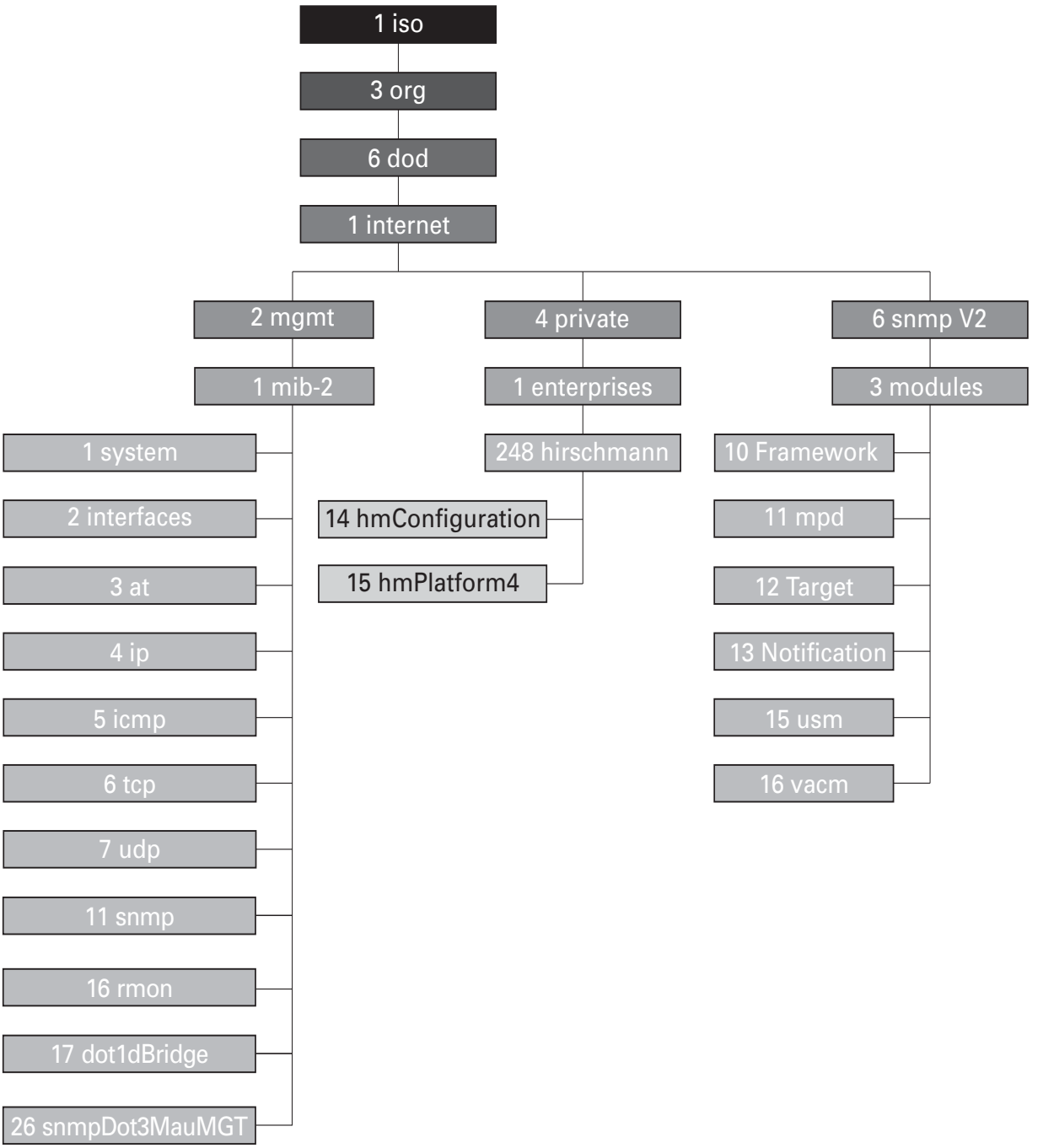


Figure 77: Tree structure of the Hirschmann MIB

A complete description of the MIB can be found on the product CD provided with the device.

B.2 Abbreviations used

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

B.3 Technical Data

You will find the technical data in the document “GUI Reference Manual”.

B.4 Readers' Comments

What is your opinion of this manual? We are constantly striving to provide as comprehensive a description of our product as possible, as well as important information to assist you in the operation of this product. Your comments and suggestions help us to further improve the quality of our documentation.

Your assessment of this manual:

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

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

Suggestions for improvement and additional information:

General comments:

Sender:

Company / Department:

Name / Telephone number:

Street:

Zip code / City:

E-mail:

Date / Signature:

Dear User,

Please fill out and return this page

- as a fax to the number +49 (0)7127/14-1600 or
- per mail to

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

C Index

A

ACA 58, 75, 77, 218
ACA31 41
ACD 244
ACL 175
Access 218
Access Control List 175
Access rights 69, 95
Access security 87
Address Conflict Detection 244
Address table 157
AF 179
Aging Time 157, 163, 163
Alarm 217
Alarm messages 214
APNIC 29
ARIN 29
ARP 34
ASF Finder 58
Assured Forwarding 179
Authentication 218
AutoConfiguration Adapter 41, 218
Automatic Configuration 87

B

Bandwidth 161, 191
Bandwidth restriction 183
BOOTP 27
Booting 19
Boundary clock 142
Broadcast 156, 158, 161

C

CD-ROM 260, 266
CIDR 34
CLI Banner 129
Classless Inter-Domain Routing 34
Class Selector 179
Clock 139
Clock synchronization 141
Closed circuit 222
Cold start 78
Command Line Interface 21
Configuration 62
Configuration changes 214
Configuration data 43, 51, 60, 67
Configuration file 48, 63, 64
Connection error 88

D

Data transfer parameters 18
Destination address 156, 158, 159, 169
Device Status 219
DHCP 27, 48, 51
DHCP Client 48
DHCP Option 82 51
DHCP server 132, 260, 266
Differentiated management access 106
Differentiated Services 179
DiffServ 175
DiffServ codepoint 179
Double VLAN tagging 208
DSCP 176, 179, 181, 186, 186
DVLAN tagging 208
Dynamic 158

E

E2E 142
EF 179
End-to-End 142
Event Log 256
Expedited Forwarding 179

F

FAQ 295
Fan 225
Faulty device replacement 55
FDB 158
Filter 158
Filter table 158, 169
First installation 27
Flash memory 62, 77
Flow control 191
Forwarding database 158

G

Gateway 30, 38
Generic object classes 284
GMRP 161, 169
GMRP per port 172
Grandmaster 139

H

HaneWin 260, 266
Hardware address 44
Hardware clock (buffered) 132
Hardware reset 214
HIPER-Ring (source for alarms) 218

HiDiscovery 39, 109
HiView 24
Host address 30

I
IANA 29
IEEE 1588 time 133
IEEE 802.1 Q 176
IEEE MAC Address 242
IGMP 163
IGMP Querier 164
IGMP Snooping 161, 163
Industrial HiVision 12, 49
Industry Protocols 11
Instantiation 284
Internet Assigned Numbers Authority 29
Internet service provider 29
In-band 21
IP Address 29, 37, 44, 48, 244
IP header 175, 178, 179
IP Parameter 27
ISO/OSI layer model 34

J
Java Runtime Environment 65
JRE 65

L
LACNIC 29
Leave 163
Link monitoring 219, 222
Loading a script file from the ACA 63
Local clock 140
Login banner 128
Login window 25

M
MAC 141
MAC destination address 34
Maximum bandwidth 183
Media module for modular devices (source for alarms) 218
Message 214
Mode 87
Multicast 136, 158, 161, 163
Multicast address 169

N
Netmask 30, 38
Network address 29
Network Management 49
Network management station 242
Network topology 51

O
Object classes 284
Object description 284
Object ID 284
Offline configuration 64
Operation monitoring 222
Option 82 28, 51, 266
Ordinary clock 142
Out-of-band 21
Overload protection 191

P
P2P 142
Password 22, 69, 96, 97
Peer-to-Peer 142
PHB 179
Phy 141
Polling 214
Port authentication 113
Port Configuration 87
Port Mirroring 249
Port Priority 181, 185
PROFINET IO 11
Precedence 179
Precision Time Protocol 139
Priority 176, 181
Priority Queues 175
Priority tagged frames 176
Protocol stack 141
PTP 131, 133, 139
PTP Subdomains 143

Q
QoS 176
Query 163
Query function 164
Queue 182

R
Rate Limiter Settings 174
Real time 131, 175
Reboot 78
Receiver power status (source for alarms) 218
Receiving port 159
Redundancy 11
Reference clock 132, 135, 139, 146
Relay contact 222
Release 73
Remote diagnostics 222
Report 163, 247
Request interval (SNTP) 136
Reset 78
Restart 78

RIPE NCC 29
Ring manager 158
Ring/Network coupling (source for alarms) 218
RMON probe 249
Router 12, 30

S

Segmentation 214
Service 247
Service provider 29
Service shell reactivation 281
SFP Module (source for alarms) 218
SFP module 240
SFP status display 240
Signal contact 88, 222
Signal contact (source for alarm) 218
Signal runtime 135
SNMP 24, 95, 214
SNTP 131, 136
SNTP client 136
SNTP server 152
Software 274
Software release 73
Source address 156
SSH 21
Starting the graphical user interface 24
State on delivery 62, 62, 95
Static 158
Strict Priority 182
Subdomains 143
Subidentifier 284
Subnet 38, 157
Summer time 132
Supply voltage 218
Symbol 13
System Monitor 18
System Name 48
System requirements (GUI) 24
System time 135, 136

T

TAI 133
Target table 214
TCP/IP stack 271
Technical Questions 295
Telnet 21
TFTP 270
TFTP Update 81
Time difference 133
Time Management 139
Time Stamp Unit 141, 145
Time zone 132
Topology 51
ToS 175, 176, 178, 179
TP cable diagnosis 233
Traffic Classes 175, 182, 185
Traffic Shaping 183, 187, 187
Training Courses 295
Transmission reliability 214
Transparent Clock 142
Trap 214, 217
Trap target table 214
Trivial File Transfer Protocol 270
Trust dot1p 181
Trust ip-dscp 181
Type Field 176
Type of Service 178

U

UDP 124
Unicast 161
Untrusted 181
Update 18
USB stick 75
User name 22
UTC 133

V

Video 182
VLAN 176, 181, 194
VLAN 0 53
VLAN ID (network parameter) 52
VLAN priority 184
VLAN tag 176, 194
VLAN tunnel 208
VoIP 182
V.24 21

W

Web-based Interface 24
Weighted Fair Queuing 182, 183, 187
Weighted Round Robin 182
Winter time 132

X

XML (Offline Configurator Format) 65

D Further Support

Technical Questions

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

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

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

You can contact us

in the EMEA region at
- Tel.: +49 (0)1805 14-1538
- E-mail: hac.support@belden.com

in the America region at
- Tel.: +1 (717) 217-2270
- E-mail: inet-support.us@belden.com

in the Asia-Pacific region at
- Tel.: +65 6854 9860
- E-mail: inet-ap@belden.com

Hirschmann Competence Center

The Hirschmann Competence Center is ahead of its competitors:

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- Training offers you an introduction to the basics, product briefing and user training with certification.
  The current technology and product training courses can be found at http://www.hicomcenter.com
- Support ranges from the first installation through the standby service to maintenance concepts.

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

HIRSCHMANN

A BELDEN BRAND