



HIRSCHMANN

A **BELDEN** BRAND

User Manual

Basic Configuration

Embedded Ethernet Switch (HiOS-2E EES)

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.

© 2014 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).

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

Contents

	Safety instructions	9
	About this Manual	11
	Key	13
	Introduction	15
1	User interfaces	17
1.1	Graphical user interface (GUI)	18
1.2	Command Line Interface	20
1.2.1	Preparing the data connection	21
1.2.2	CLI access via telnet	22
1.2.3	CLI via SSH (Secure Shell)	27
1.2.4	CLI via the V.24 port	32
1.3	System Monitor	35
1.3.1	Functional scope	36
1.3.2	Starting the System Monitor	37
2	Entering IP Parameters	39
2.1	IP Parameter Basics	40
2.1.1	IP Address (Version 4)	41
2.1.2	Netmask	43
2.1.3	Classless Inter-Domain Routing	47
2.2	Entering IP parameters using the CLI	48
2.3	Entering the IP Parameters via HiDiscovery	51
2.4	Enter the IP Parameter using the graphical user interface	53
2.5	Entering IP Parameters per BOOTP	55
2.6	Entering IP Parameters per DHCP	56
2.7	Management Address Conflict Detection	59
2.7.1	Active and Passive detection	60
3	Access to the device	61
3.1	Authentication lists	62

3.1.1	Applications	63
3.1.2	Methods	64
3.1.3	Default setting	65
3.1.4	Managing authentication lists	66
3.1.5	Adjusting the settings	67
3.2	User Management	73
3.2.1	Access Roles	74
3.2.2	Managing user accounts	77
3.2.3	Default setting	78
3.2.4	Changing standard passwords	79
3.2.5	Setting up a new user account	82
3.2.6	Deactivating the user account	85
3.2.7	Adjusting policies for passwords	87
3.3	SNMP Access	89
3.3.1	SNMPv1/v2 Community	90
3.3.2	SNMPv3 access	94
4	Managing configuration profiles	97
4.1	Detecting changed settings	98
4.2	Saving settings	99
4.2.1	Saving the configuration profile in the device	100
4.2.2	Exporting a configuration profile	105
4.3	Loading settings	107
4.3.1	Activating a configuration profile	108
4.3.2	Importing a configuration profile	110
4.4	Resetting the device to the factory defaults	113
4.4.1	With the graphical user interface or CLI	114
4.4.2	In the System Monitor	115
4.5	Service Shell	116
5	Synchronizing the System Time in the Network	117
5.1	Basic settings	119
5.1.1	Setting the time	120
5.1.2	Automatic daylight saving time changeover	122
5.2	SNTP	123
5.2.1	Preparation	125
5.2.2	Defining settings of the SNTP client	127
5.2.3	Specifying SNTP server settings	129
5.3	PTP	131
5.3.1	Types of clocks	132
5.3.2	Best Master Clock algorithm	134

5.3.3	Delay measurement	135
5.3.4	PTP domains	136
5.3.5	Using PTP	137
5.4	IRIG-B/PPS	138
5.4.1	Preparation	139
5.4.2	Turning on IRIG-B	140
5.4.3	Turning on PPS	141
6	Network Load Control	143
6.1	Direct Packet Distribution	144
6.1.1	Learning MAC addresses	145
6.1.2	Aging of learned MAC addresses	146
6.1.3	Static address entries	147
6.2	Multicasts	152
6.2.1	Example of a Multicast Application	153
6.2.2	IGMP snooping	154
6.3	Rate limiter	162
6.4	QoS/Priority	164
6.4.1	Description of Prioritization	165
6.4.2	Handling of Received Priority Information	167
6.4.3	VLAN tagging	168
6.4.4	IP ToS	170
6.4.5	Handling of traffic classes	171
6.4.6	Queue Management	173
6.4.7	Management prioritization	175
6.4.8	Setting prioritization	176
6.5	Flow Control	181
6.5.1	Halfduplex or fullduplex link.	183
6.5.2	Setting the Flow Control	184
7	VLANs	185
7.1	Examples of VLANs	186
7.1.1	Example 1	187
7.1.2	Example 2	193
7.2	Guest / Unauthenticated VLAN	200
7.3	RADIUS VLAN assignment	202
7.4	VLAN unaware mode	203
8	Operation Diagnosis	205
8.1	Sending Traps	206

8.1.1	List of SNMP traps	207
8.1.2	Traps for configuration activity	208
8.1.3	Configuring Traps	209
8.1.4	ICMP Messaging	211
8.2	Monitoring the Device Status	212
8.2.1	Events which can be monitored	213
8.2.2	Configuring the Device Status	214
8.2.3	Displaying the Device Status	216
8.3	Security Status (DEVMON)	217
8.3.1	Events which can be monitored	218
8.3.2	Configuring the Security Status	219
8.3.3	Displaying the Security Status	221
8.4	Port Event Counter	222
8.4.1	Detecting Non-matching Duplex Modes	223
8.5	Displaying the SFP Status	225
8.6	Topology Discovery	226
8.6.1	Displaying the Topology Discovery Results	228
8.7	Detecting Loops	229
8.8	Reports	230
8.8.1	Global Settings	231
8.8.2	Syslog	233
8.8.3	System Log	235
8.8.4	Audit Trail	236
8.9	Network Analysis with TCPDump	237
8.10	Monitoring Data Traffic on the Ports (Port Mirroring)	238
8.11	Cause and Action management during Selftest	241
8.12	Copper Cable Test	243
9	Advanced functions of the device	245
9.1	Auto Disable	246
9.2	MRP-IEEE	248
9.2.1	MRP Operation	249
9.2.2	MMRP	251
9.2.3	MVRP	254
9.3	CLI Client	257
9.4	IEC 61850/MMS	258
9.4.1	Switch model for IEC 61850	259
9.4.2	Integration into a Control System	261
9.4.3	Offline configuration	262

9.4.4	Monitoring the device	263
A	Setting up the Configuration Environment	265
A.1	Setting up a DHCP/BOOTP Server	266
A.2	Changing the MAC Address	272
A.3	Define the Management port	273
B	General Information	275
B.1	Management Information Base (MIB)	276
B.2	Abbreviations used	279
B.3	Technical Data	281
B.4	Maintenance	282
B.5	Readers' Comments	283
C	Index	285
D	Further Support	287

Safety instructions



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





The document “HiView User Manual” contains information about the GUI application HiView. 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).

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






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

Key

The designations used in this manual have the following meanings:

	List
<input type="checkbox"/>	Work step
	Subheading
Link	Cross-reference with link
Note:	A note emphasizes an important fact or draws your attention to a dependency.
<i>Courier</i>	ASCII representation in the graphical user interface
	Execution in the Graphical User Interface
	Execution in the Command Line Interface

Symbols used:

	WLAN access point
	Router with firewall
	Switch with firewall
	Router
	Switch

Key



Bridge



Hub



A random computer



Configuration Computer



Server



PLC -
Programmable logic
controller



I/O -
Robot

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 User interfaces

The device allows you to specify the settings of the device using the following user interfaces.

User interface	Can be reached through ...	Prerequisite
Graphical user interface (GUI)	Ethernet (in-band)	HiView or Web browser and Java
Command Line Interface (CLI)	Ethernet (in-band) V.24 (out-of-band)	Terminal emulation software
System Monitor	V.24 (out-of-band)	Terminal emulation software

Table 1: User interfaces for accessing the management of the device

1.1 Graphical user interface (GUI)

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.

Start the graphical user interface in HiView:

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

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

Start the graphical user interface in the Web browser:

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

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

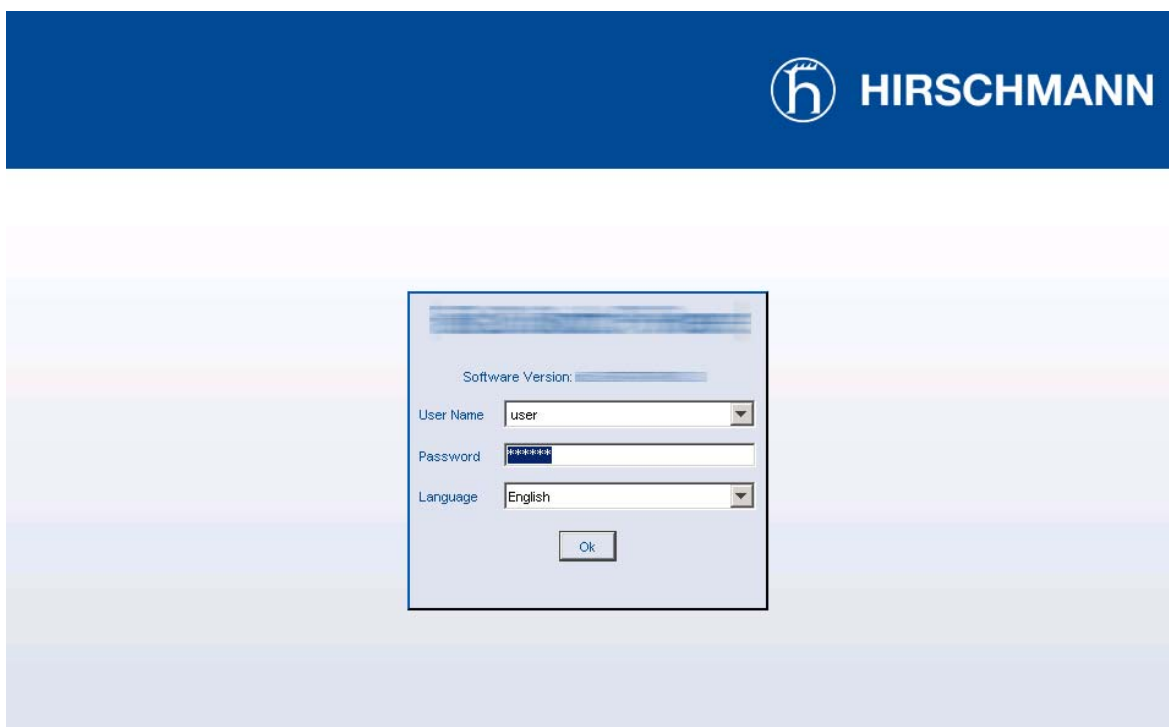


Figure 1: Login window

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

The window with the graphical user interface will appear on the screen.

1.2 Command Line Interface

The Command Line Interface enables you to use the functions of the device through a local or remote connection.

The Command Line Interface provides IT specialists with a familiar environment for configuring IT devices. As an experienced user or administrator, you have knowledge about the basics and about using Embedded Ethernet Switch devices.

The “Command Line Interface” reference manual gives you step-by-step information on using the Command Line Interface (CLI) and its commands.

1.2.1 Preparing the data connection

Information for assembling and starting up your HiOS-2E EES device can be found in the “Installation” user manual.

You will find information for configuring your HiOS-2E EES device in the “Configuration” user manual.

- Connect the device with the network. The network parameters must be set correctly for the data connection to be successful.

You can access the user interface of the Command Line Interface with the freeware program PuTTY.

This program is located on the product CD.

- Install PuTTY on your computer.

1.2.2 CLI access via telnet

■ Telnet connection via Windows

Note: Telnet is only installed as standard in Windows versions before Windows Vista.

► Start screen

- Open the Windows start screen on your computer with Start>Run... .
- Enter the command `telnet <IP address of the device>` into the "Open:" field.

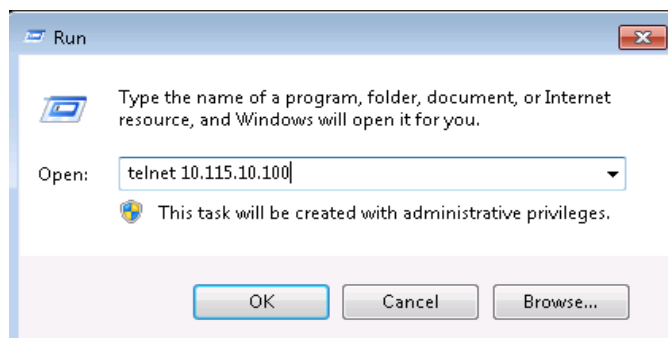


Figure 2: Setting up the telnet connection to the HiOS-2E EES via the Windows entry screen

► Command prompt

- With Start>Programs>Accessories>Command Prompt you start the DOS command line interpreter on your computer.
- Enter the command `telnet <IP address of the device>`.

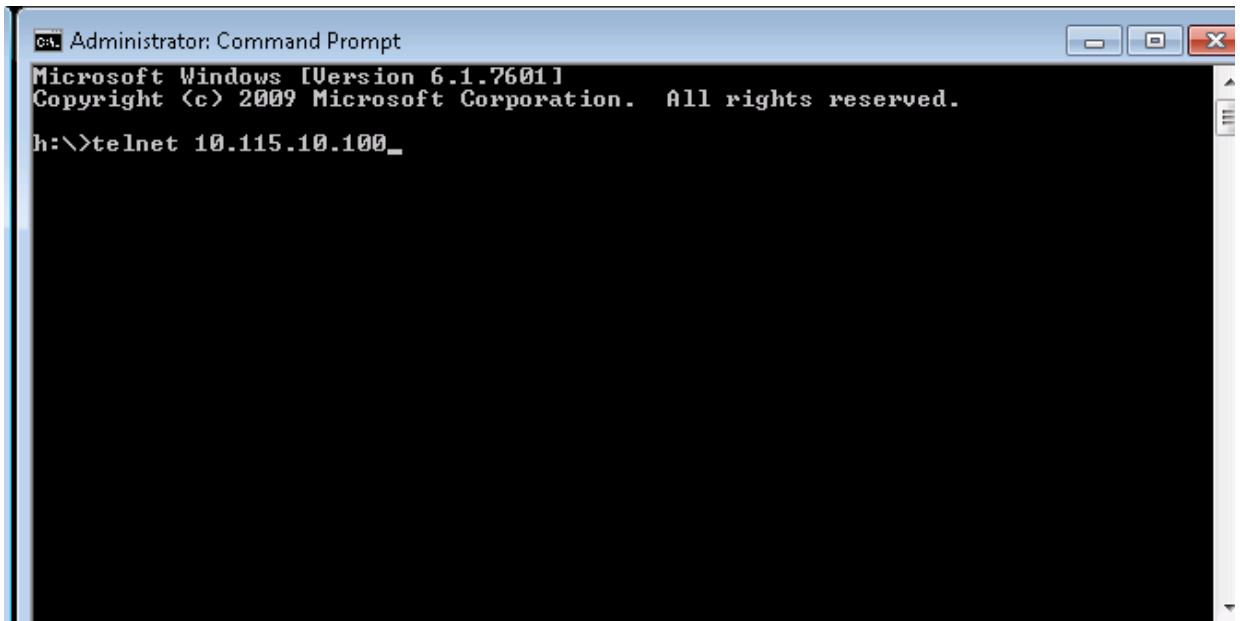


Figure 3: Setting up the telnet connection to the HiOS-2E EES via the DOS command line

■ **Telnet connection via PuTTY**

- Start the PuTTY program on your computer.

PuTTY appears with the login screen.

Set up the serial configuration parameters of the terminal emulation program as follows:

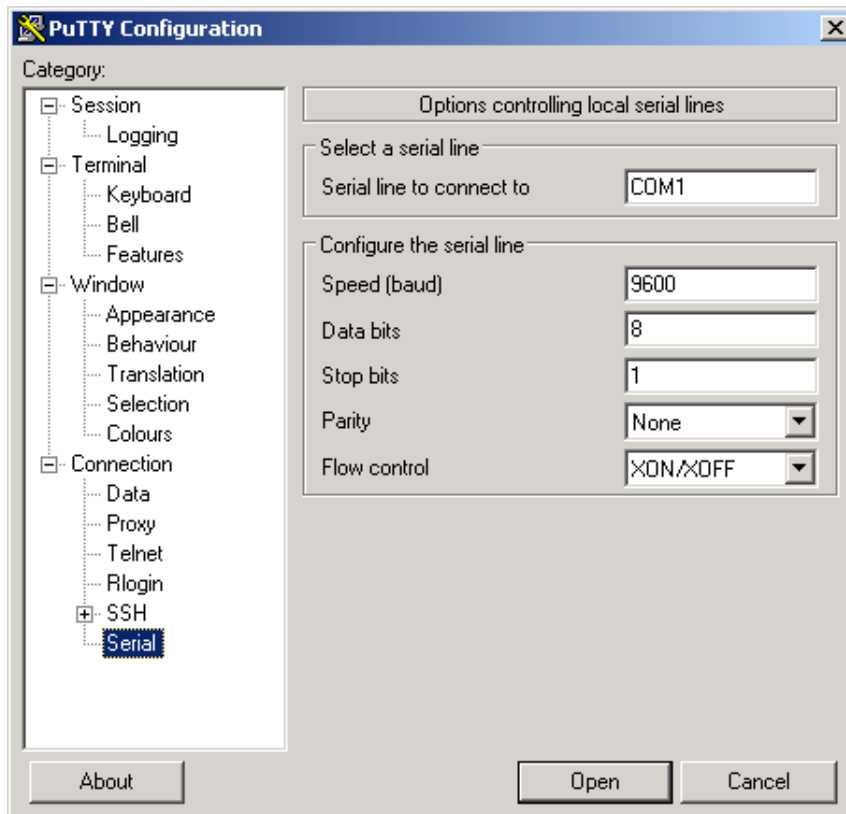


Figure 4: Configuring the serial data connection via PuTTY

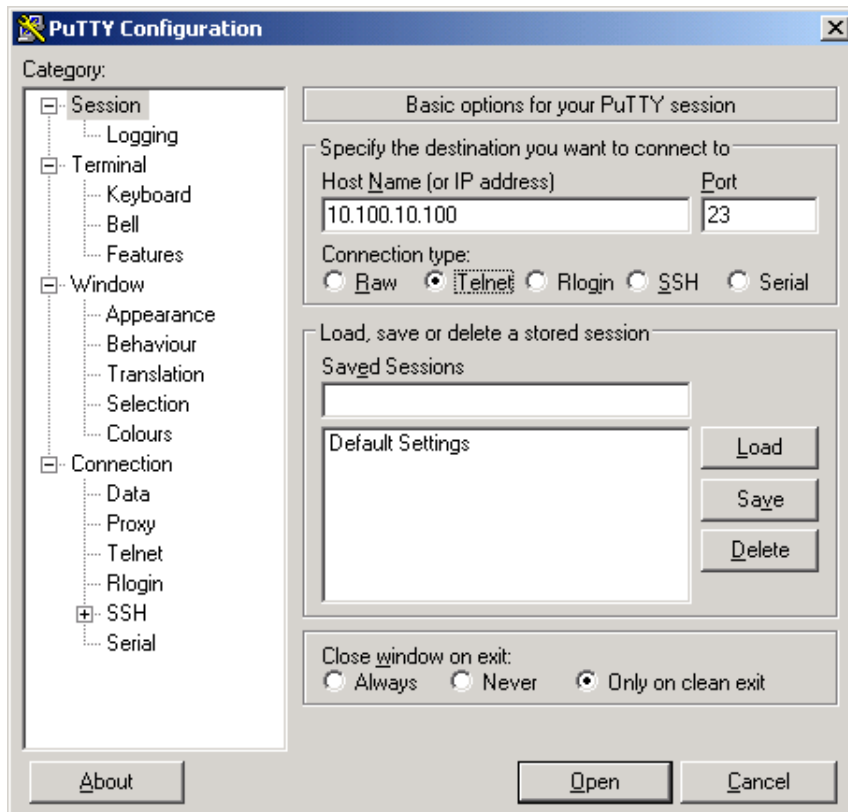


Figure 5: PuTTY input screen

- In the Host Name (or IP address) input field you enter the IP address of your device.
The IP address (a.b.c.d) consists of 4 decimal numbers with values from 0 to 255. The 4 decimal numbers are separated by points.
- To select the connection type, click Telnet under Connection type.
- Click "Open" to set up the data connection to your device.

CLI appears on the screen with a window for entering the user name. The device enables up to 5 users to have access to the Command Line Interface at the same time.

```
User: admin
Password:*****
```

Figure 6: Login window in CLI

Note: Change the password during the first startup procedure.

- 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.
The device offers the possibility to change the user name and the password later in the Command Line Interface.
These entries are case-sensitive.

The device displays the CLI start screen.

```
Copyright (c) 2011-2012 Hirschmann Automation and Control GmbH
All rights reserved

HiOS-2E Release 3.0.0-CL1.00
(Build date Aug 29 2013)

System Name   : HiOS-2E-000000000000
Management IP : 10.115.46.205
Subnet Mask   : 255.255.224.0
Base MAC      : 00:00:00:00:00:00
System Time   : 2013-07-26 09:57:14

NOTE: Enter '?' for Command Help. Command help displays all options
that are valid for the particular mode.
For the syntax of a particular command form, please
consult the documentation.

* (EES) >
```

Figure 7: Start screen of CLI.

Your HiOS-2E EES appears with the command prompt
EES >

1.2.3 CLI via SSH (Secure Shell)

- Start the PuTTY program on your computer.

PuTTY appears with the login screen.

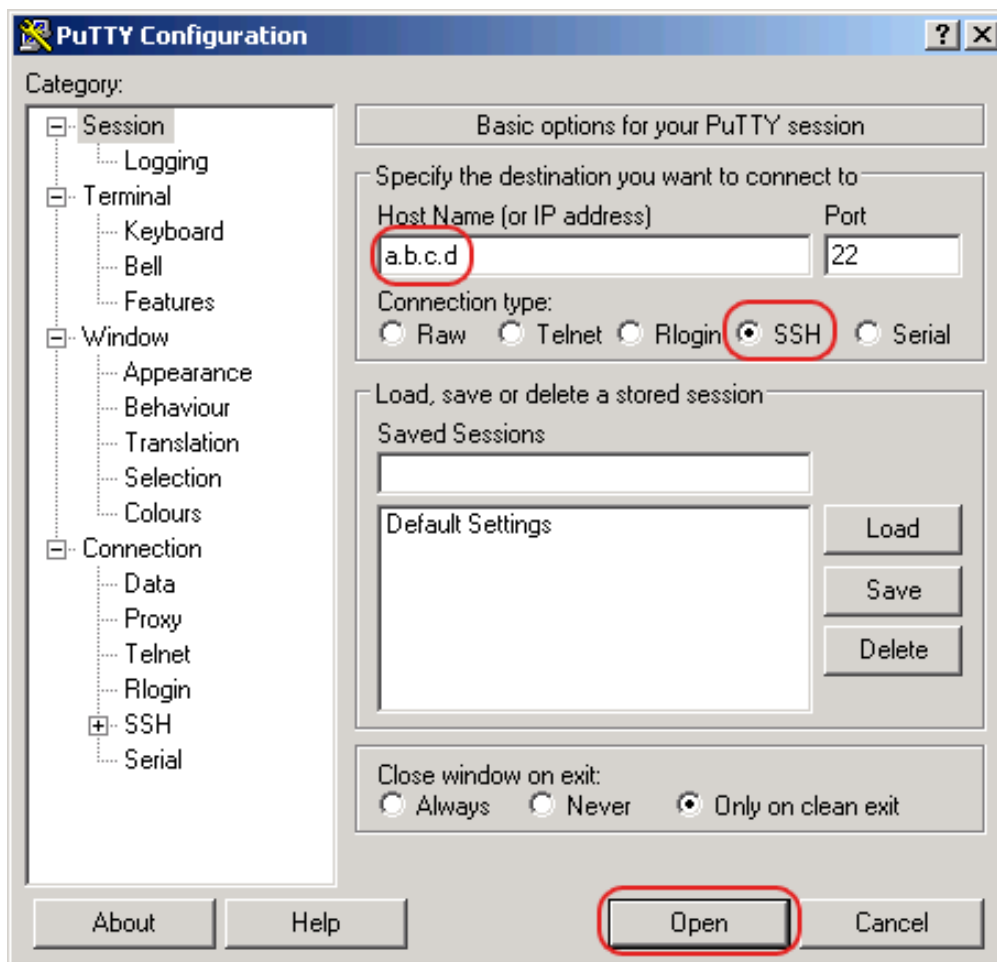


Figure 8: PuTTY input screen

- In the `Host Name (or IP address)` input field you enter the IP address of your device.
The IP address (a.b.c.d) consists of 4 decimal numbers with values from 0 to 255. The 4 decimal numbers are separated by points.
- To select a connection type, click on `SSH` under `Connection type`.
- After selecting and setting the required parameters, the device enables you to set up the data connection via SSH.
Click “Open” to set up the data connection to your device. Depending on the device and the time at which SSH was configured, setting up the connection takes up to a minute.

When you first login to your device, towards the end of the connection setup, PuTTY displays a security alert message and gives you the option of checking the fingerprint of the key.



Figure 9: Security alert prompt for the fingerprint

- Check the fingerprint to help protect yourself from unwelcome guests.
- If the fingerprint matches that of the device key, click “Yes”.

The device offers the possibility to read the fingerprints of the device key with the CLI command `show ssh` or in the graphical user interface, in the `Device Security > Management Access > Server` dialog, "SSH" tab.

Note:

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

```
ssh admin@10.149.112.53
```

`admin` represents the user name.

`10.149.112.53` is the IP address of your device.

CLI appears on the screen with a window for entering the user name. The device enables up to 5 users to have access to the Command Line Interface at the same time.

```
login as: admin
admin@a.b.c.d's password:
```

Figure 10: Login window in CLI

`a.b.c.d` is the IP address of your device.

- 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.
The device offers the possibility to change the user name and the password later in the Command Line Interface.
These entries are case-sensitive.

The device displays the CLI start screen.

Note: This device is a security-relevant product. Change the password during the first startup procedure.

```
login as: admin
admin@10.115.46.205's password:

Copyright (c) 2011-2012 Hirschmann Automation and Control GmbH
All rights reserved

UMS Release 3.0.0-01-1.00
(Build date Jun 25 2012)

System Name      : UMS-40010012000
Management IP    : 10.115.46.205
Subnet Mask      : 255.255.224.0
Base MAC         : 8C-85-10-01-20-00
System Time      : 2012-07-26 10:23:47

NOTE: Enter '?' for Command Help.  Command help displays all options
      that are valid for the particular mode.
      For the syntax of a particular command form, please
      consult the documentation.

*(UMS) >
```

Figure 11: Start screen of CLI.

1.2.4 CLI via the V.24 port

The V.24 interface is a serial interface for the local connection of an external management station (VT100 terminal or PC with terminal emulation). The interface allows you to set up a data connection to the Command Line Interface (CLI) and to the system monitor.

VT 100 terminal settings	
Speed	9,600 Baud
Data	8 bit
Stopbit	1 bit
Handshake	off
Parity	none

The socket housing is electrically connected to the housing of the device.

- Connect the device to a terminal via V.24. Alternatively connect the device to a “COM” port of your PC using terminal emulation based on VT100 and press any key.
- Alternatively you set up the serial data connection to the device via V.24 with PuTTY (see figure 12). Press the Enter key.

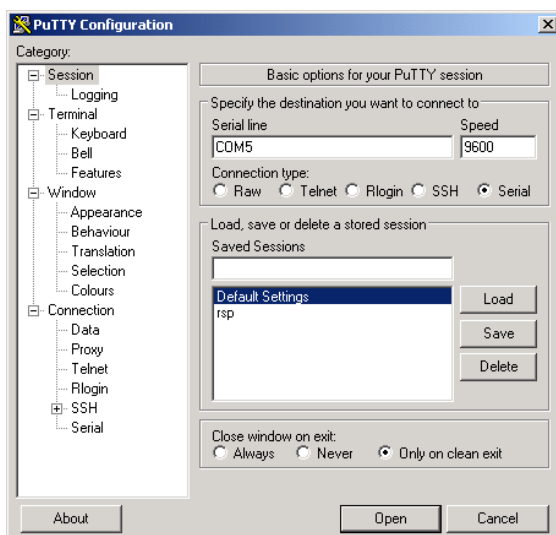


Figure 12: Serial data connection via V.24 with PuTTY

After the data connection has been set up successfully, the device displays a window for entering the user name.

```
Copyright (c) 2011-2012 Hirschmann Automation and Control GmbH
All rights reserved

HMP Release 3.00-26-02.0.00-002
(Build date 2012-04-25 13:34)

System Name   : HMP-000000000000
Management IP : 10.0.1.32
Subnet Mask   : 255.255.255.0
Base MAC      : 88:00:00:00:00:00
System Time   : 2012-07-26 09:10:34

User:admin
Password:*****
```

Figure 13: 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.
The device offers the possibility to change the user name and the password later in the Command Line Interface.
These entries are case-sensitive.

The device displays the CLI start screen.

```
NOTE: Enter '?' for Command Help.  Command help displays all opt
      that are valid for the particular mode.
      For the syntax of a particular command form, please
      consult the documentation.

! ( ) >
```

Figure 14: CLI screen after login

Note: You can configure the V.24 interface as a terminal/CLI interface. Press any key on your terminal keyboard a number of times until the login screen indicates the CLI mode.

1.3 System Monitor

The System Monitor allows you to set basic operating parameters before starting the operating system.

1.3.1 Functional scope

In the System Monitor, you carry out the following tasks, for example:

- ▶ Updating the operating system
- ▶ Starting the operating system
- ▶ Deleting configuration profiles, resetting the device to the factory defaults
- ▶ Checking boot code information

1.3.2 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 interface of the device with the “COM” port of the PC.
- Start the VT100 terminal emulation on the PC.
- Specify the following transmission parameters:
 - Speed: 9,600 baud
 - Stopbit: 8 bit
 - Parity: none
 - Stopbit: 1 bit
 - Flow control: none
- Set up a connection to the device.
- Switch on the device. If the device is already on, reboot it.
The screen displays the following message after rebooting:
`Press <1> to enter System Monitor 1.`
- Press 1 within 3 seconds.
The device starts the System Monitor. The screen displays the following view:

```
System Monitor 1
(Selected OS: HiOS-2E-EES (2013-04-29 13:30))

1 Manage operating systems
2 Update operating System
3 Start selected operating system
4 Manage configurations
5 Show boot code information
q End (reset and reboot)

sysMon1>
```

Figure 15: Screen display of system monitor 1

- 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.

2 Entering 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 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
- ▶ 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 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. Write these 4 bytes in decimal notation, separated by a decimal point.

RFC 1340 written in 1992, defines 5 IP Address classes.

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 first byte of an IP address is the network 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 (ISP). Your ISP contacts their local higher-level organization to reserve an IP address block:

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

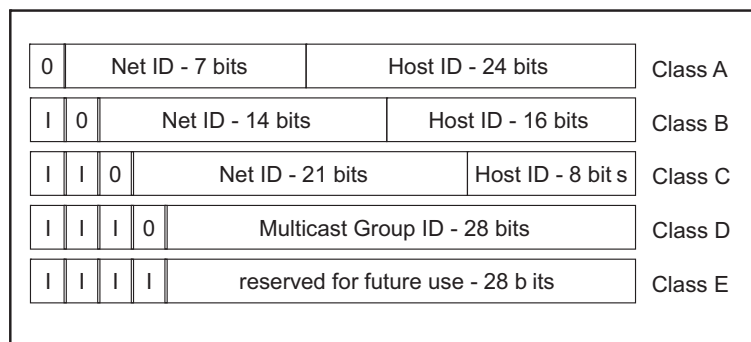


Figure 16: Bit representation of the IP address

The IP addresses belong to class A when their first bit is a zero, for example, the first octet 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, for example, the first octet is between 128 and 191.

The IP address belongs to class C when the first 2 bits are a one, for example, the first octet is higher than 191.

Assigning the host address (host ID) is the responsibility of the network operator. The network operator alone is responsible for the uniqueness of the assigned IP addresses.

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.

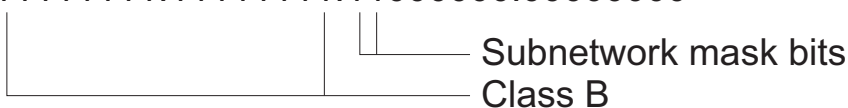
You perform subnetwork division using the netmask in much the same way as the division of the network addresses (net id) into classes A to C.

Set the bits of the host address (host id) that represent the mask to one. Set the remaining host address bits to zero (see the following examples).

Example of a subnet mask:

Decimal notation
255.255.192.0

Binary notation
11111111.11111111.11000000.00000000



Example of IP addresses with subnetwork assignment when applying the subnet mask:

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?

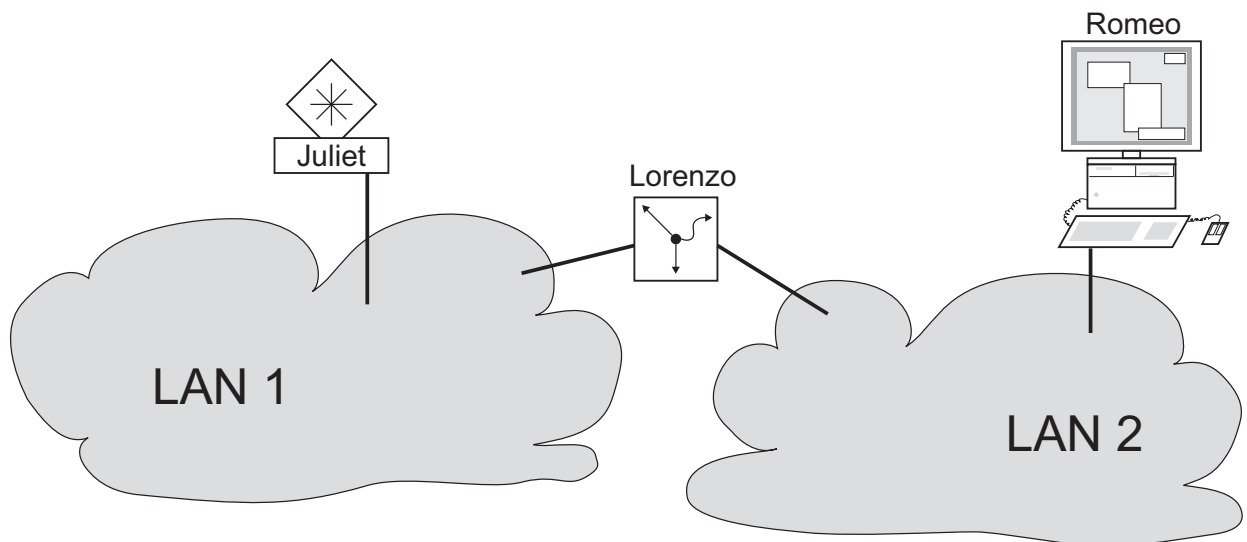


Figure 17: Management agent that is separated from its management station by a router

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. Resulting in an ineffective usage of the available class B addresses.

Class D contains reserved multicast addresses. Class E is for experimental purposes. A non-participating gateway ignores experimental 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 mask bits equal the number of bits used for the subnet in a given IP address range. Example:

IP address, decimal	Network mask, decimal	IP address, binary
149.218.112.1	255.255.255.128	10010101 11011010 01110000 00000001
149.218.112.127		10010101 11011010 01110000 01111111
		
CIDR notation: 149.218.112.0/25		
		

The term “supernetting” refers to combing a number of class C address ranges. Supernetting enables you to subdivide class B address ranges to a fine degree.

2.2 Entering IP parameters using the CLI

There are several methods you enter the system configuration, either via BOOTP/DHCP or the HiDiscovery protocol. You also have the possibility to perform the configuration via the V.24 interface using the CLI.

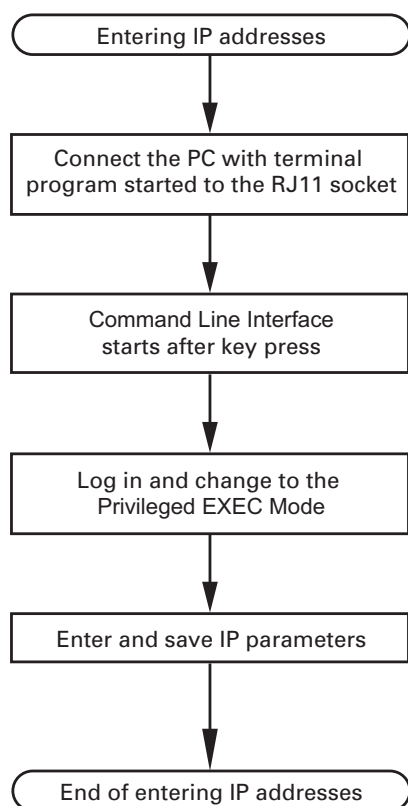


Figure 18: Flow chart for entering IP addresses

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.

The start screen appears.

```
NOTE: Enter '?' for Command Help. Command help displays all opt
      that are valid for the particular mode.
      For the syntax of a particular command form, please
      consult the documentation.

!( )>
```

- 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 45 “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 config running-config nvm`.

```
enable
network protocol none
network parms 10.0.1.23
                255.255.255.0

copy config running-config
nvm
```

Switch to the privileged EXEC mode.

Deactivate DHCP.

Assign the device the IP address 10.0.1.23 and the netmask 255.255.255.0. You have the option of also assigning a gateway address.

Save the current configuration to the non-volatile memory.

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

2.3 Entering the IP Parameters via HiDiscovery

The HiDiscovery protocol enables you to assign IP parameters to the device via the Ethernet.

You easily configure other parameters via the graphical user interface (see the “GUI” 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.

The screenshot shows the HiDiscovery software interface with a menu bar (File, Edit, Options, ?) and a toolbar (Signal, Properties, WWW, Telnet, Ping, Rescan, Preferences). Below the toolbar is a table with the following columns: Id, MAC Address, Writable, IP Address, Net Mask, Default Gateway, Product, and Name. The table contains 24 rows of data, with the 5th row highlighted in red.

Id	MAC Address	Writable	IP Address	Net Mask	Default Gateway	Product	Name
1	00:80:63:A4:CC:00	<input type="checkbox"/>	10.115.0.76	255.255.224.0	10.115.0.3		
2	00:80:63:C0:50:00	<input type="checkbox"/>	10.115.0.33	255.255.224.0	10.115.0.3		
3	00:80:63:A3:40:00	<input type="checkbox"/>	10.115.0.70	255.255.224.0	10.115.0.3		
4	00:80:63:9B:14:00	<input type="checkbox"/>	10.115.0.17	255.255.224.0	10.115.0.3		
5	00:80:63:96:E4:00	<input type="checkbox"/>	0.0.0.0	0.0.0.0	0.0.0.0		
6	00:80:63:46:00:06	<input checked="" type="checkbox"/>	192.168.2.181	255.255.255.0	192.168.2.1		
7	00:80:63:A3:40:40	<input type="checkbox"/>	10.115.0.59	255.255.224.0	10.115.0.3		
8	00:80:63:A4:CC:40	<input type="checkbox"/>	10.115.0.81	255.255.224.0	10.115.0.3		
9	00:80:63:6E:38:4E	<input checked="" type="checkbox"/>	192.168.2.174	255.255.255.0	192.168.2.1		
10	00:80:63:1B:2A:61	<input checked="" type="checkbox"/>	192.168.2.170	255.255.255.0	192.168.2.1		
11	00:80:63:A3:40:80	<input type="checkbox"/>	10.115.0.66	255.255.224.0	10.115.0.3		
12	00:80:63:A4:CC:80	<input type="checkbox"/>	10.115.0.80	255.255.224.0	10.115.0.3		
13	00:80:63:61:AC:81	<input checked="" type="checkbox"/>	192.168.2.176	255.255.255.0	192.168.2.1		
14	00:80:63:9B:10:95	<input type="checkbox"/>	10.115.0.22	255.255.224.0	10.115.0.3		
15	00:80:63:61:AC:AB	<input checked="" type="checkbox"/>	192.168.2.40	255.255.255.0	192.168.2.1		
16	00:80:63:3B:5C:BD	<input checked="" type="checkbox"/>	192.168.2.178	255.255.255.0	192.168.2.1		
17	00:80:63:A3:40:C0	<input type="checkbox"/>	10.115.0.72	255.255.224.0	10.115.0.3		
18	00:80:63:8F:2C:BE	<input type="checkbox"/>	10.115.0.40	255.255.224.0	10.115.0.3		
19	00:80:63:88:38:EC	<input checked="" type="checkbox"/>	192.168.110.92	255.255.255.0	0.0.0.0		
20	00:80:63:9B:11:00	<input type="checkbox"/>	10.115.0.35	255.255.224.0	10.115.0.3		
21	00:80:63:A4:CD:00	<input type="checkbox"/>	10.115.0.77	255.255.224.0	10.115.0.3		
22	00:80:63:99:41:08	<input type="checkbox"/>	10.115.0.13	255.255.224.0	10.115.0.3		
23	00:80:63:17:35:0B	<input checked="" type="checkbox"/>	192.168.2.164	255.255.255.0	192.168.2.1		
24	00:80:63:44:19:2E	<input checked="" type="checkbox"/>	10.115.5.130	255.255.224.0	10.115.0.3		

Figure 19: HiDiscovery

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.

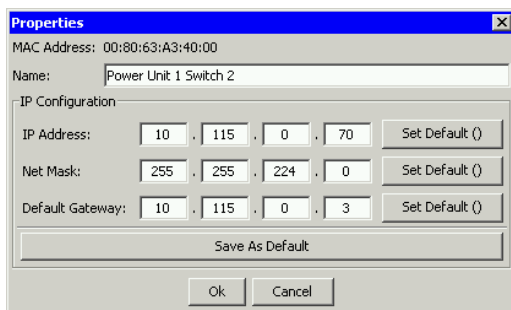


Figure 20: HiDiscovery – assigning IP parameters

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.

Note: Save the settings so that you will still have the entries after a restart.

2.4 Enter the IP Parameter using the graphical user interface

To configure the global parameters use the following steps:

- Open the `Basic Settings > Network` dialog.

In this dialog you first define the source from which the device gets its IP parameters after starting. You also define the VLAN in which the device management can be accessed, configure the HiDiscovery access and allocate manual IP parameters.

The screenshot shows a graphical user interface for configuring network parameters. The main window is titled "Management Interface" and contains several sections:

- IP Address Assignment:** Three radio buttons are present: "BOOTP", "DHCP" (which is selected), and "Local".
- VLAN ID:** A text input field containing the value "1".
- MAC Address:** A text input field containing the value "EC:E5:55:F5:C2:00".
- HiDiscovery Protocol:** Includes an "Operation" section with "On" and "Off" radio buttons, where "On" is selected. Below it is an "Access" dropdown menu set to "read/Write".
- BOOTP/ DHCP:** A "Client ID" text input field containing "MSP-ECE555F5C200".
- IP Parameter:** Three text input fields: "IP Address" (10.115.45.104), "Netmask" (255.255.224.0), and "Gateway address" (10.115.32.3).

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

Figure 21: Basic Settings > Network dialog

- In the "Management Interface" frame you first define where the device gets its IP parameters from:

- ▶ In the "BOOTP" mode, the configuration is via a BOOTP or DHCP server on the basis of the MAC address of the device.
- ▶ In the "DHCP" mode, the configuration is via a DHCP server on the basis of the MAC address or the name of the device.
- ▶ In the "Local" mode, the device uses the network parameters from the internal device memory.

Note: When you change the allocation mode of the IP address, the device activates the new mode immediately after the "Set" button is pressed.

- In the "VLAN ID" field you enter the ID of the VLAN in which the device management can be accessed via the network.
- Note here that you can only access the management via device ports that are members of the relevant VLAN.

The "MAC address" field shows the MAC address of the device with which you access the device via the network.

- In the "HiDiscovery Protocol" frame you define the settings for accessing the device via the HiDiscovery software.
- The HiDiscovery protocol allows you to allocate an IP address to the device on the basis of its MAC address . Activate the HiDiscovery protocol if you want to allocate an IP address to the device from your PC with the supplied HiDiscovery software (default setting: "Operation" On, "Access" read-write).
- If required, you can manually enter the IP address, the netmask and the gateway in the "IP Parameter" frame.
- To temporarily save the changes, click "Set".

Note: To make the configuration available even after a restart, save the settings permanently in the `Basic Settings > Load/Save` dialog.

2.5 Entering IP Parameters per BOOTP

With the BOOTP function activated the device sends a boot request message to the BOOTP server. The boot request message contains the Client ID configured in the `Basic Settings > Network` dialog. The BOOTP server enters the Client ID into a database and assigns an IP address. The server answers with a boot reply message. The boot reply message contains the assigned IP address.

2.6 Entering IP Parameters per 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 `Basic Settings > System` dialog), or the Command Line Interface.

The device sends its system name to the DHCP server. The DHCP server then uses 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 applies the configuration data to the appropriate parameters. When the DHCP Server assigns the IP address, the device permanently saves the configuration data in non-volatile memory..

Option	Meaning
1	Subnet Mask
2	Time Offset
3	Router
4	Time server
12	Host Name
42	NTP server
61	Client Identifier

Table 3: DHCP options which the device requests

Option	Meaning
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. The `Basic Settings > Network` dialog offers you the opportunity to activate or to deactivate DHCP.

[See “Enter the IP Parameter using the graphical user interface” on page 53.](#)

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.

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 Management Address Conflict Detection

You assign an IP address to the device using several different methods. This function helps the device detect IP address conflicts on a network after boot up and the device also checks periodically during operation. This function is described in RFC 5227.

When enabled, the device sends an SNMP trap informing you that it detected an IP address conflict.

The follow list contains the default settings for this function:

- ▶ Operation setting:
 - Operation: Enabled
- ▶ Configuration settings:
 - Detection Mode: Active and Passive
 - Send Periodic ARP Probes: Enabled
 - Detection Delay [ms]: 200
 - Release Delay [s]: 15
 - Number of Address Protections: 3
 - Protection Interval [ms]: 200
 - Send Trap: Enabled

2.7.1 Active and Passive detection

Actively checking the network helps prevent the device from connecting to the network with a duplicate IP address. After connecting the device to a network or after configuring the IP address, the device immediately checks whether its IP address exists within the network. To check the network for address conflicts, the device sends 4 ARP probes with the detection delay of 200 ms into the network. If the IP address exists, the device returns to the previous configuration, if possible, and makes another check after the configured release delay time.

When you disable active detection, the device sends 2 gratuitous APR announcements in 2 s intervals. Using the ARP announcements with passive detection enabled, the device polls the network to determine whether there is an address conflict. After resolving an address conflict or after expired release delay time, the device reconnects to the network. Following 10 detected conflicts, if the configured release delay interval is less than 60 s, then the device sets the release delay interval to 60 s.

After the device performs active detection or you disable the active detection function, with passive detection enabled the device listens on the network for other devices using the same IP address. If the device detects a duplicate IP address, it initially defends its address by employing the ACD mechanism in the passive detection mode and sends out gratuitous ARPs. The number of protections that the device sends and the protection interval are configurable. To resolve conflicts, if the remote device remains connected to the network, the network interface of the local device disconnects from the network.

When a DHCP server assigns an IP address to the device, the device returns a DHCP decline message when an address conflict occurs.

The device uses the ARP probe method which has the following advantages:

- ▶ ARP caches on other devices remain unchanged
- ▶ the method is robust through multiple ARP probe transmissions

3 Access to the device

3.1 Authentication lists

The device allows you to use authentication lists to specify which method it uses for the authentication. For every application with which someone accesses the device, a separate policy is possible.

3.1.1 Applications

The device supports the following applications, with which the device management can be accessed:

- ▶ Access using CLI via a serial connection
- ▶ Access using CLI via SSH
- ▶ Access using CLI via Telnet
- ▶ Access using the graphical user interface (GUI)

The device also controls the access to the network from connected terminal devices using port-based access control (IEEE802.1x).

3.1.2 Methods

When users login, the device uses one of the following methods for the authentication:

- ▶ `local`
The device authenticates the users by using the local user management, see the `Device Security > User Management` dialog.
- ▶ `radius`
The device forwards authentication requests to a RADIUS server in the network.

When terminal devices login to access the network using IEEE802.1X, the device uses one of the following methods for the authentication:

- ▶ `radius`
The device forwards authentication requests to a RADIUS server in the network.
- ▶ `ias`
The device authenticates the terminal devices with the integrated authentication server (IAS) implemented in the device. The IAS manages the login data in a separate database, see the `Network Security > 802.1X Port Authentication > Integrated Authentication Server` dialog.

3.1.3 Default setting

In the default settings of the device, the following lists are already set up and active:

- ▶ `defaultDot1x8021AuthList`
This list specifies the methods for the authentication of connected terminal devices using IEEE 802.1X. The `8021x` application is allocated to the list.
- ▶ `defaultLoginAuthList`
This list specifies the methods for the authentication for users that log in using the graphical user interface (GUI) or using the CLI via SSH or Telnet. The `SSH`, `Telnet` and `Web Interface` applications are allocated to the list
- ▶ `defaultV24AuthList`
This list specifies the methods for the authentication for users that log in using the CLI via a serial connection. The `Console (V.24)` application is allocated to the list.

3.1.4 Managing authentication lists

You manage the authentication lists in the graphical user interface (GUI) or in the CLI.

Prerequisite: User account with authorization profile `administrator`.

- Open the `Device Security > Authentication List` dialog. The dialog shows the lists that are set up.

Name	Policy 1	Policy 2	Policy 3	Policy 4	Policy 5	Dedicated Applications	Active
defaultDot1x8021AuthList	radius	reject	reject	reject	reject	8021x	<input checked="" type="checkbox"/>
defaultLoginAuthList	local	reject	reject	reject	reject	SSH, Telnet, WebInterface	<input checked="" type="checkbox"/>
defaultV24AuthList	local	reject	reject	reject	reject	Console(V.24)	<input checked="" type="checkbox"/>

Set Reload Create Remove Allocate Applications ? Help

Figure 22: `Device Security > Authentication List` dialog

`show authlists`

Shows the lists that are set up.

3.1.5 Adjusting the settings

The device allows you to allocate a separate policy for the authentication to every application with which someone accesses the device.

In the following example, we will set up a separate list for each of the applications included in the default list `defaultLoginAuthList`.

Prerequisite: User account with authorization profile `administrator`.

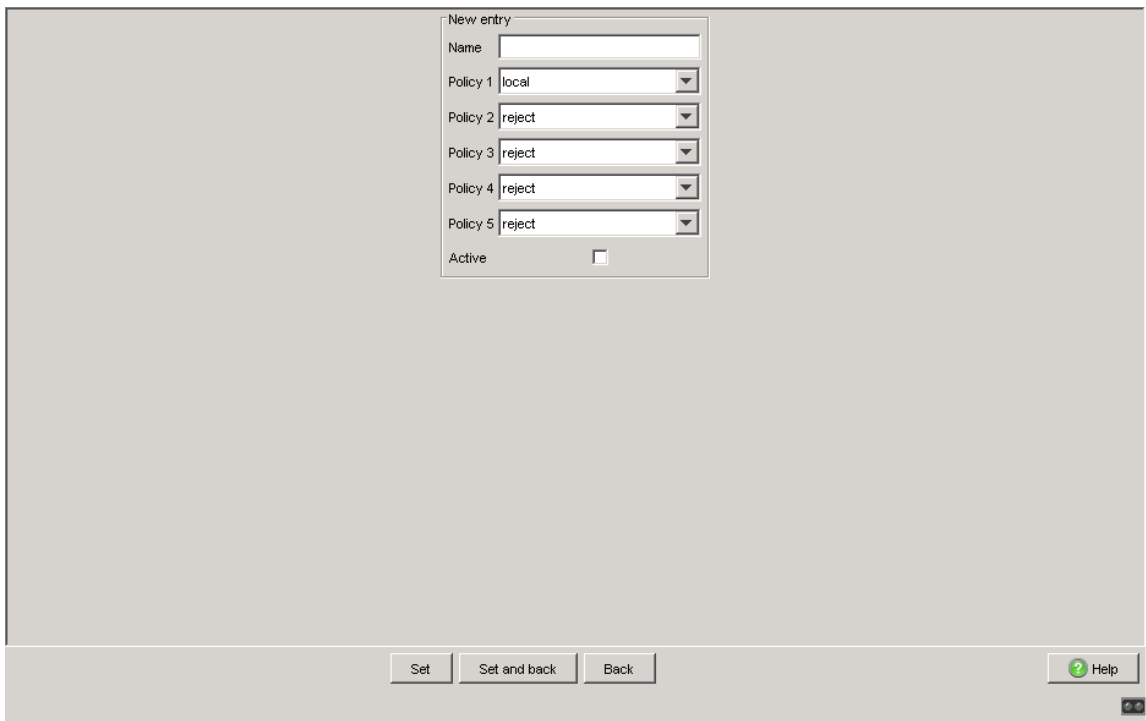
Perform the following work steps:

Create new lists.

Open the `Device Security > Authentication List` dialog.

Click "Create".

The dialog shows the "New Entry" frame.



The screenshot shows a "New entry" dialog box with the following fields:

- Name:
- Policy 1:
- Policy 2:
- Policy 3:
- Policy 4:
- Policy 5:
- Active:

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

Figure 23: New entry frame in the `Device Security > Authentication List` dialog

- Enter a meaningful name in the "Name" field.
In this example, we give the list the following names:
 - ▶ loginGUI ... for access using the graphical user interface (GUI)
 - ▶ loginSSH ... for access using the CLI via SSH
 - ▶ loginTelnet ... for access using the CLI via Telnet
- Select the desired method in the fields "Policy 1" to "Policy 5".
 - Select `radius` for the device to forward authentication requests to a RADIUS server in the network.
 - Select `local` for the device to authenticate users using the local user management.
 - Select `reject` for the device to reject authentication requests. This prevents the user from being granted access to the device.

The device gives you the option of a fall-back solution. For this, you specify one other method in each of the "Policy 2" to "Policy 5" fields. If the authentication with the specified method is not successful, the device uses the next policy.

In this example, we select the following methods:

- ▶ `radius` in the "Policy 1" field
- ▶ `local` in the "Policy 2" field
- ▶ `reject` in the fields "Policy 3" to "Policy 5"

The screenshot shows a 'New entry' dialog box with the following fields and values:

Field	Value
Name	loginGUI
Policy 1	radius
Policy 2	local
Policy 3	reject
Policy 4	reject
Policy 5	reject
Active	<input type="checkbox"/>

Buttons at the bottom: Set, Set and back, Back, Help.

Figure 24: New entry frame in the Device Security > Authentication List dialog

- To activate the list, select the "Active" checkbox.
- Click "Set and back".

- Repeat these work steps to create another list.
The dialog shows the lists that are set up.

Name	Policy 1	Policy 2	Policy 3	Policy 4	Policy 5	Dedicated Applications	Active
defaultDot1x8021AuthList	radius	reject	reject	reject	reject	8021x	<input checked="" type="checkbox"/>
defaultLoginAuthList	local	reject	reject	reject	reject	SSH, Telnet, WebInterface	<input checked="" type="checkbox"/>
defaultV24AuthList	local	reject	reject	reject	reject	Console(V.24)	<input checked="" type="checkbox"/>
loginGUI	radius	local	reject	reject	reject		<input checked="" type="checkbox"/>
loginSSH	radius	local	reject	reject	reject		<input checked="" type="checkbox"/>
loginTelnet	radius	local	reject	reject	reject		<input checked="" type="checkbox"/>

Buttons: Set, Reload, Create, Remove, Allocate Applications, Help

Figure 25: Device Security > Authentication List dialog

```
enable
configure
authlists add loginGUI
authlists enable loginGUI
authlists set-policy
  loginGUI radius local reject
  reject reject
show authlists
```

Switch to the privileged EXEC mode.

Switch to the Configuration mode.

Creates the loginGUI list.

Activates the loginGUI list.

Allocates the methods to the loginGUI list according to the example.

Shows the lists that are set up.

Connect the list with an application.

Mark in the `Device Security > Authentication List` dialog the desired list by clicking the "Name" field.

Click "Allocate Applications".

The dialog shows the "Allocate Applications" window.

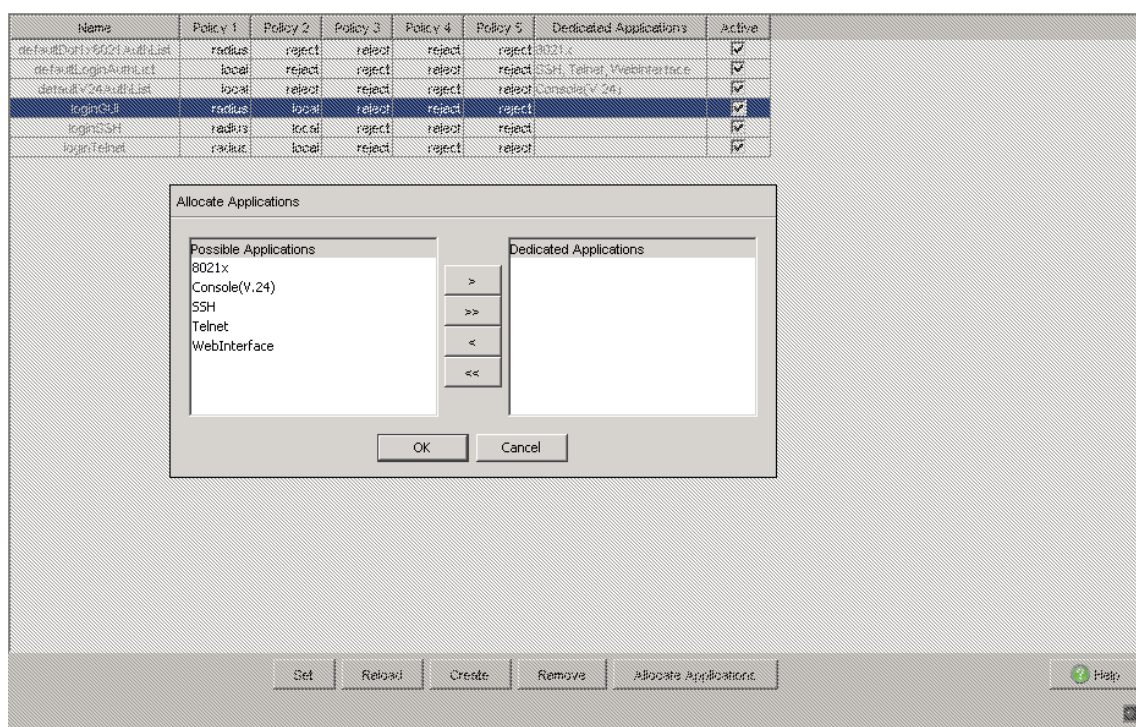


Figure 26: Allocate Applications window in the `Device Security > Authentication List` dialog

In the "Possible Applications" column, select the application that you are allocating to the list.

- ▶ For access using the graphical user interface (GUI), select `Web Interface`.
- ▶ For access using the CLI via SSH, select `SSH`.
- ▶ For access using the CLI via Telnet, select `Telnet`.

Click " > ".

The "Dedicated Applications" column now shows the application.

Click "OK".

The dialog shows the updated settings.

Name	Policy 1	Policy 2	Policy 3	Policy 4	Policy 5	Dedicated Applications	Active
defaultDot1x8021AuthList	radius	reject	reject	reject	reject	8021x	<input checked="" type="checkbox"/>
defaultLoginAuthList	local	reject	reject	reject	reject		<input checked="" type="checkbox"/>
defaultV24AuthList	local	reject	reject	reject	reject	Console(V.24)	<input checked="" type="checkbox"/>
loginGUI	radius	local	reject	reject	reject	WebInterface	<input checked="" type="checkbox"/>
loginSSH	radius	local	reject	reject	reject	SSH	<input checked="" type="checkbox"/>
loginTelnet	radius	local	reject	reject	reject	Telnet	<input checked="" type="checkbox"/>

Buttons: Set, Reload, Create, Remove, Allocate Applications, Help

Figure 27: Device Security > Authentication List dialog

- Repeat these work steps to allocate an application to the other lists.
- To temporarily save the changes, click "Set".

```
show applist
applist set-authlist
WebInterface loginGUI
```

Shows the applications and the allocated lists.
Allocates the loginGUI list to the Web Interface application.

- Deactivate the list for those applications by means of which no access to the device is performed.

In this example we assume that no access using the CLI via Telnet is performed. Therefore we remove the selection from the "Active" checkbox for the `loginTelnet` list.

- To deactivate a list, you remove the selection from the "Active" checkbox.

Name	Policy 1	Policy 2	Policy 3	Policy 4	Policy 5	Dedicated Applications	Active
defaultDot1x8021AuthList	radius	reject	reject	reject	reject	8021x	<input checked="" type="checkbox"/>
defaultLoginAuthList	local	reject	reject	reject	reject		<input checked="" type="checkbox"/>
defaultV24AuthList	local	reject	reject	reject	reject	Console(V.24)	<input checked="" type="checkbox"/>
loginGUI	radius	local	reject	reject	reject	WebInterface	<input checked="" type="checkbox"/>
loginSSH	radius	local	reject	reject	reject	SSH	<input checked="" type="checkbox"/>
loginTelnet	radius	local	reject	reject	reject	Telnet	<input type="checkbox"/>

Buttons: Set, Reload, Create, Remove, Allocate Applications, Help

Figure 28: *Device Security > Authentication List dialog*

- To temporarily save the changes, click "Set".
- To permanently save the changes, you open the `Basic Settings > Load/Save` dialog and click "Save".

```
authlists disable
loginTelnet
save
```

Deactivates the `loginTelnet` list.

Saves the settings in the non-volatile memory of the device (NVM) in the "selected" configuration profile.

3.2 User Management

The device allows users to access its management functions when they log in with valid login data. The device authenticates the users either using the local user management or with a RADIUS server in the network. To get the device to use the user management, assign the `local` method to an authentication list, see the `Device Security > Authentication List` dialog.

In the local user management, you manage the user accounts. One user account is usually allocated to each user.

3.2.1 Access Roles

The device allows you to use a role-based authorization model to specifically control the access to the management functions. Users to whom a specific authorization profile is allocated are allowed to use commands and functions from the same authorization profile or a lower one.

The device uses the authorization profiles on all applications with which the management functions can be accessed.

Every user account is linked to an access role that regulates the access to the individual functions of the device. Depending on the planned activity for the respective user, you assign a predefined access role to the user. The device differentiates between the following access roles.

Access Role	Description	Authorized for the following activities
Administrator	The user is authorized to monitor and administer the device.	All activities with read/write access, including the following activities reserved for an administrator: <ul style="list-style-type: none"> ▶ Add, modify or delete user accounts ▶ Activate, deactivate or unlock user accounts ▶ Change all passwords ▶ Configure password management ▶ Set or change system time ▶ Load files to the device, e.g. device configurations, certificates or software images ▶ Reset settings and security-related settings to the state on delivery ▶ Configure RADIUS server and authentication lists ▶ Apply CLI scripts ▶ Switch CLI logging and SNMP logging on and off ▶ System monitor activation and deactivation ▶ Switch the services for the management access (e. g. SNMP) on and off. ▶ Configure access restrictions to the user interfaces or the CLI based on the IP addresses
Operator	The user is authorized to monitor and configure the device - with the exception of security-related settings.	All activities with read/write access, with the exception of the above-named activities, which are reserved for an administrator:
Auditor	The user is authorized to monitor the device and to save the log file in the Diagnostics > Report > Audit Trail dialog.	Monitoring activities with read access.

Table 4: Access roles for user accounts

Access Role	Description	Authorized for the following activities
Guest	The user is authorized to monitor the device - with the exception of security-related settings.	Monitoring activities with read access.
Unauthorized	No access to the device possible. <ul style="list-style-type: none">▶ As an administrator you assign this access role to temporarily lock a user account.▶ The device assigns this access role to a user account if an error occurs when assigning a different access role.	No activities allowed.

Table 4: Access roles for user accounts (cont.)

3.2.2 Managing user accounts

You manage the user accounts in the graphical user interface (GUI) or in the CLI.

Prerequisite: User account with authorization profile `administrator`.

- Open the `Device Security > User Management` dialog. The dialog shows the user accounts that are set up.

User Name	Active	Password	Access Role	User Locked	Policy Check	SNMP Auth Type	SNMP Encryption Type
admin	<input checked="" type="checkbox"/>	*****	administrator	<input type="checkbox"/>	<input type="checkbox"/>	hmacmd5	des
user	<input checked="" type="checkbox"/>	*****	guest	<input type="checkbox"/>	<input type="checkbox"/>	hmacmd5	des

Figure 29: Device Security > User Management dialog

`show users`

Shows the user accounts that are set up.

3.2.3 Default setting

In the state on delivery, the user accounts `admin` and `user` are set up on the device.

Parameters	Value in the state on delivery	
User Name	<code>admin</code>	<code>user</code>
Password	<code>private</code>	<code>public</code>
Authorization	<code>administrator</code>	<code>guest</code>
User locked	<code>off</code>	<code>off</code>
Policy Check	<code>off</code>	<code>off</code>
SNMP Auth Type	<code>hmacmd5</code>	<code>hmacmd5</code>
SNMP Encryption Type	<code>des</code>	<code>des</code>

Table 5: Default settings for the factory setting user accounts

Note: Change the password for the `admin` user account before making the device available in the network.


3.2.4 Changing standard passwords

To prevent undesired access, change the password in the default settings of the user accounts.

Prerequisite: User account with authorization profile `administrator`.

Perform the following work steps:

Change the passwords for the `admin` and `user` user accounts.

 Open the `Device Security > User Management` dialog.

The dialog shows the user accounts that are set up.

The dialog is divided into two main sections: Configuration and Password Policy. Below these is a table of user accounts and a set of control buttons.

Configuration		Password Policy	
Number of Login Attempts	0	Minimum Upper Cases	1
Minimum Password Length	6	Minimum Lower Cases	1
		Minimum Numbers	1
		Minimum Special Characters	1

User Name	Active	Password	Access Role	User locked	Policy Check	SNMP Auth Type	SNMP Encryption Type
admin	<input checked="" type="checkbox"/>	*****	administrator	<input type="checkbox"/>	<input type="checkbox"/>	hmacmd5	des
user	<input checked="" type="checkbox"/>	*****	guest	<input type="checkbox"/>	<input type="checkbox"/>	hmacmd5	des

Buttons: Set, Reload, Create, Remove, Help

Figure 30: Device Security > User Management dialog

- To obtain a higher level of complexity for the password, mark the "Policy Check" checkbox.

Before saving it, the device checks the password according to the policy specified in the "Password Policy" frame.

Note: The password check may lead to a message in the `Basic Settings > System` dialog, in the "Security Status" frame. You specify the settings that cause this message in the `Basic Settings > System` dialog.

- Click the row of the relevant user account in the "Password" field. Enter a password of at least 6 characters. Up to 64 alphanumeric characters are allowed.
 - ▶ The device differentiates between upper and lower case.
 - ▶ The minimum length of the password is defined in the "Configuration" frame. The device always checks the minimum length of the password.
- To temporarily save the changes, click "Set".
- To permanently save the changes, you open the `Basic Settings > Load/Save` dialog and click "Save".

<code>enable</code>	Switch to the privileged EXEC mode.
<code>configure</code>	Switch to the Configuration mode.
<code>users password-policy-check <user> enable</code>	Activates the checking of the password for the <user> user account based on the specified policy. In this way, you obtain a higher level of complexity for the password.
Note: The password check may lead to a message when you display the security status (<code>show security-status all</code>). You specify the settings that cause this message with the command <code>security-status monitor pwd-policy-inactive</code> .	
<code>users password <user> SECRET</code>	Specifies the password "SECRET" for the <user> user account. Enter at least 6 characters.
<code>save</code>	Saves the settings in the non-volatile memory of the device (NVM) in the "selected" configuration profile.

3.2.5 Setting up a new user account

Allocate a separate user account to each user that accesses the device management. In this way you can specifically control the authorizations for the access.

In the following example, we will set up the user account for an `<operator>` user. The `<operator>` user is authorized to monitor and configure the device - with the exception of security-related settings.

Prerequisite: User account with authorization profile `administrator`.

Perform the following work steps:

Create a new user account.

Open the `Device Security > User Management` dialog.

Click "Create".

The dialog shows the "New Entry" frame.

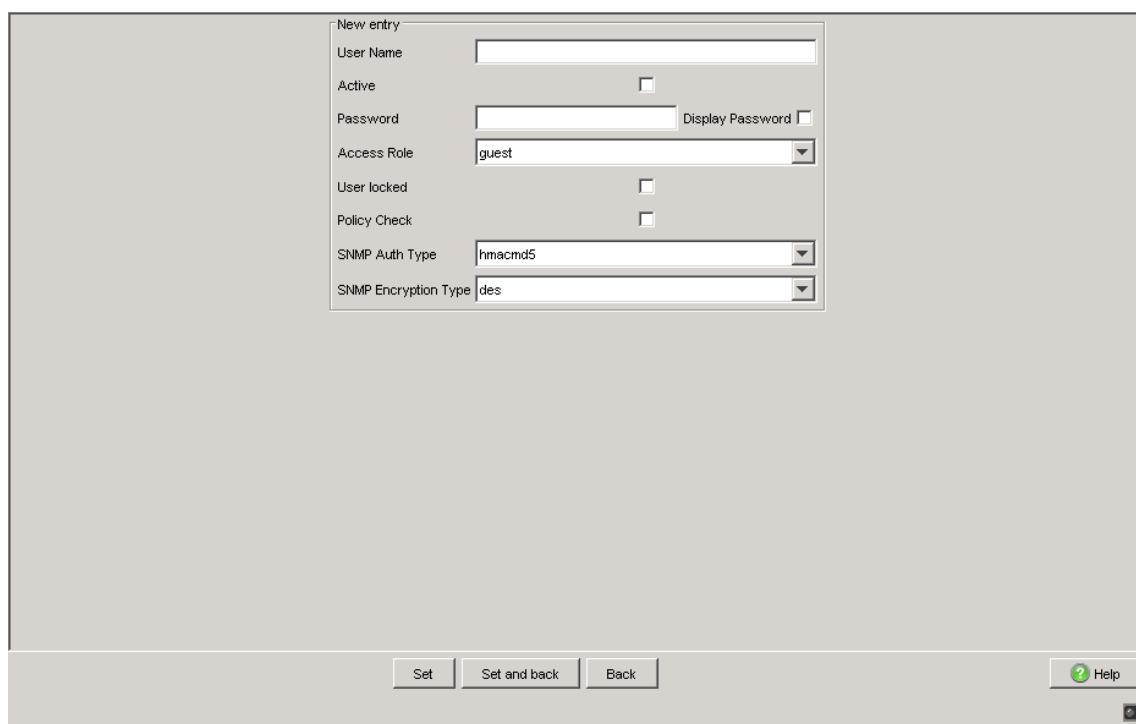


Figure 31: New entry frame in the `Device Security > User Management` dialog

Enter the name in the "User Name" field.

In this example, we give the user account the name `<operator>`.

- To obtain a higher level of complexity for the password, select the "Policy Check" checkbox.
Before saving it, the device checks the password according to the policy defined in the "Password Policy" frame.
- In the "Password" field, enter a password of at least 6 characters. Up to 64 alphanumeric characters are allowed.
 - To make the password visible when it is being input, select the "Display Password" checkbox.
 - ▶ The device differentiates between upper and lower case.
 - ▶ The minimum length of the password is defined in the "Configuration" frame. The device always checks the minimum length of the password.
- Select the authorization profile in the "Access Role" field.
In this example, we select the `operator` authorization profile.
- To activate the user account, select the "Active" checkbox.
- Click "Set and back".

The dialog shows the user accounts that are set up.

User Name	Active	Password	Access Role	User locked	Policy Check	SNMP Auth Type	SNMP Encryption Type
admin	<input checked="" type="checkbox"/>	*****	administrator	<input type="checkbox"/>	<input type="checkbox"/>	hmacmd5	des
user	<input checked="" type="checkbox"/>	*****	guest	<input type="checkbox"/>	<input type="checkbox"/>	hmacmd5	des
<user>	<input checked="" type="checkbox"/>	*****	operator	<input type="checkbox"/>	<input type="checkbox"/>	hmacmd5	des

Configuration: Number of Login Attempts: 0, Minimum Password Length: 6
 Password Policy: Minimum Upper Cases: 1, Minimum Lower Cases: 1, Minimum Numbers: 1, Minimum Special Characters: 1

Buttons: Set, Reload, Create, Remove, Help

Figure 32: *Device Security > User Management dialog*

- To permanently save the changes, you open the `Basic Settings > Load/Save` dialog and click "Save".

enable	Switch to the privileged EXEC mode.
configure	Switch to the Configuration mode.
users add <operator>	Creates the <operator> user account.
users password-policy-check <operator> enable	Activates the checking of the password for the <operator> user account based on the specified policy. In this way, you obtain a higher level of complexity for the password.
users password <operator> SECRET	Specifies the password "SECRET" for the <operator> user account. Enter at least 6 characters.
users access-role <operator> operator	Allocates the operator authorization profile to the <operator> user account.
users enable <operator>	Activates the <operator> user account.
show users	Shows the user accounts that are set up.
save	Saves the settings in the non-volatile memory of the device (NVM) in the "selected" configuration profile.

Note: Remember to allocate the password when you are setting up a new user account in the CLI.

3.2.6 Deactivating the user account

After a user account is deactivated, the device denies the related user access to the management functions. In contrast to completely deleting it, deactivating a user account allows you to keep the settings and reuse them in the future.

Prerequisite: User account with authorization profile `administrator`.

Perform the following work steps:

- To keep the user account settings and reuse them in the future, you temporarily deactivate the user account.

- Open the `Device Security > User Management` dialog. The dialog shows the user accounts that are set up.

User Name	Active	Password	Access Role	User locked	Policy Check	SNMP Auth Type	SNMP Encryption Type
admin	<input checked="" type="checkbox"/>	*****	administrator	<input type="checkbox"/>	<input type="checkbox"/>	hmacmd5	des
user	<input checked="" type="checkbox"/>	*****	guest	<input type="checkbox"/>	<input type="checkbox"/>	hmacmd5	des
<user>	<input checked="" type="checkbox"/>	*****	operator	<input type="checkbox"/>	<input type="checkbox"/>	hmacmd5	des

Figure 33: Device Security > User Management dialog

- In the row for the relevant user account, remove the selection from the "Active" checkbox.
- To temporarily save the changes, click "Set".
- To permanently save the changes, you open the `Basic Settings > Load/Save` dialog and click "Save".

```
enable
configure
users disable <user>
show users
save
```

Switch to the privileged EXEC mode.
 Switch to the Configuration mode.
 To disable user account.
 Shows the user accounts that are set up.
 Saves the settings in the non-volatile memory of the device (NVM) in the “selected” configuration profile.

- To permanently deactivate the user account settings, you delete the user account.

- Select the relevant user and click "Clear".
- To permanently save the changes, you open the `Basic Settings > Load/Save` dialog and click "Save".

```
users delete <user>
show users
save
```

Deletes the <user> user account.
 Shows the user accounts that are set up.
 Saves the settings in the non-volatile memory of the device (NVM) in the “selected” configuration profile.

3.2.7 Adjusting policies for passwords

The device allows you to check whether the passwords for the user accounts adhere to the specified policy. You obtain a higher level of complexity for the passwords when they adhere to the policy.

The user management of the device allows you to activate or deactivate the check separately in each user account. When the check is activated, the device accepts a changed password only if it fulfills the requirements of the policy.

In the default settings, practical values for the policy are set up on the device. You have the option of adjusting the policy to meet your requirements.

Prerequisite: User account with authorization profile `administrator`.

Perform the following work steps:

- Adjust the policy for passwords to meet your requirements.

- Open the `Device Security > User Management` dialog.

User Name	Active	Password	Access Role	User locked	Policy Check	SNMP Auth Type	SNMP Encryption Type
admin	<input checked="" type="checkbox"/>	*****	administrator	<input type="checkbox"/>	<input type="checkbox"/>	hmacmd5	des
user	<input checked="" type="checkbox"/>	*****	guest	<input type="checkbox"/>	<input type="checkbox"/>	hmacmd5	des
<user>	<input checked="" type="checkbox"/>	*****	operator	<input type="checkbox"/>	<input type="checkbox"/>	hmacmd5	des

Figure 34: Device Security > User Management dialog

In the "Configuration" frame you define the number user login attempts before the device locks out the user. You also define the minimum number of characters that defines a password.

- Specify the values to meet your requirements.
 - ▶ You specify the number of times that a user attempts to log on to the device in the "Number of Login Attempts" field. The field allows you to define this value in the range from 0 through 5.
In the above example, the value 0 deactivates the function.
 - ▶ The "Minimum Password Length" field allows values in the range from 6 through 64.

The dialog shows the policy set up in the "Password Policy" frame.

- Adjust the values to meet your requirements.
 - ▶ Values in the range 1 through 16 are allowed.
The value 0 deactivates the relevant policy.

To apply the entries specified in the "Configuration" and "Password Policy" frames, mark the "Policy Check" checkbox for a particular user.

- To temporarily save the changes, click "Set".
- To permanently save the changes, you open the `Basic Settings >` Load/Save dialog and click "Save".

<code>enable</code>	Switch to the privileged EXEC mode.
<code>configure</code>	Switch to the Configuration mode.
<code>passwords min-length 6</code>	Specifies the policy for the minimum length of the password.
<code>passwords min-lowercase-chars 1</code>	Specifies the policy for the minimum number of lower-case letters in the password.
<code>passwords min-numeric-chars 1</code>	Specifies the policy for the minimum number of digits in the password.
<code>passwords min-special-chars 1</code>	Specifies the policy for the minimum number of special characters in the password.
<code>passwords min-uppercase-chars 1</code>	Specifies the policy for the minimum number of upper-case letters in the password.
<code>show passwords</code>	Shows the policies that are set up.
<code>save</code>	Saves the settings in the non-volatile memory of the device (NVM) in the "selected" configuration profile.

3.3 SNMP Access

3.3.1 SNMPv1/v2 Community

The SNMP protocol allows you to monitor and configure the device via the network with a network management system (NMS). When the NMS accesses the device via SNMPv1 or SNMPv2, the NMS authenticates itself with the community.

With the default settings, you access the device via the `public` (read access) and `private` (read/write access) communities.

The community is contained in every SNMP packet. When it receives a packet, the device compares this community with the communities specified in the device. If the communities match, the device accepts the SNMP packet and grants access.

Make the following basic provisions to make undesired access to the device more difficult:

- Change the community for read/write access. Treat this community confidentially. Everyone who knows the community has the option to change the settings for the device.
- Specify a different community for read/write access than for read access.
- Use SNMPv1 or SNMPv2 only in environments protected from eavesdropping. The protocols do not use encryption. The SNMP packets contain the community in clear text. We recommend using SNMPv3 and deactivating the access via SNMPv1 and SNMPv2 in the device.

Prerequisite: User account with authorization profile `administrator`.

Perform the following work steps:

- Change the community for read/write access.

- Open the `Device Security > Management Access > SNMPv1/v2 Community` dialog.

The dialog shows the communities that are set up.

Community	Name
Write	private
Read	public

Loading data ok

Figure 35: `Device Security > Management Access > SNMPv1/v2 Community` dialog

- In the row for the `Write` community, click the "Name" field. Enter the community.
 - ▶ Up to 32 alphanumeric characters are allowed.
 - ▶ The device differentiates between upper and lower case.
 - ▶ Specify a different community than for read access.
- To temporarily save the changes, click "Set".
- To permanently save the changes, you open the `Basic Settings > Load/Save` dialog and click "Save".

```
enable
configure
snmp community rw
<community name>
show snmp community
save
```

Switch to the privileged EXEC mode.

Switch to the Configuration mode.

Specifies the community for read/write access.

Shows the communities that are set up.

Saves the settings in the non-volatile memory of the device (NVM) in the "selected" configuration profile.

- Deactivate the access via SNMPv1 or SNMPv2 in the device.

- Open the `Device Security > Management Access > Server` dialog, "SNMP" tab.

The dialog shows the settings of the SNMP server.

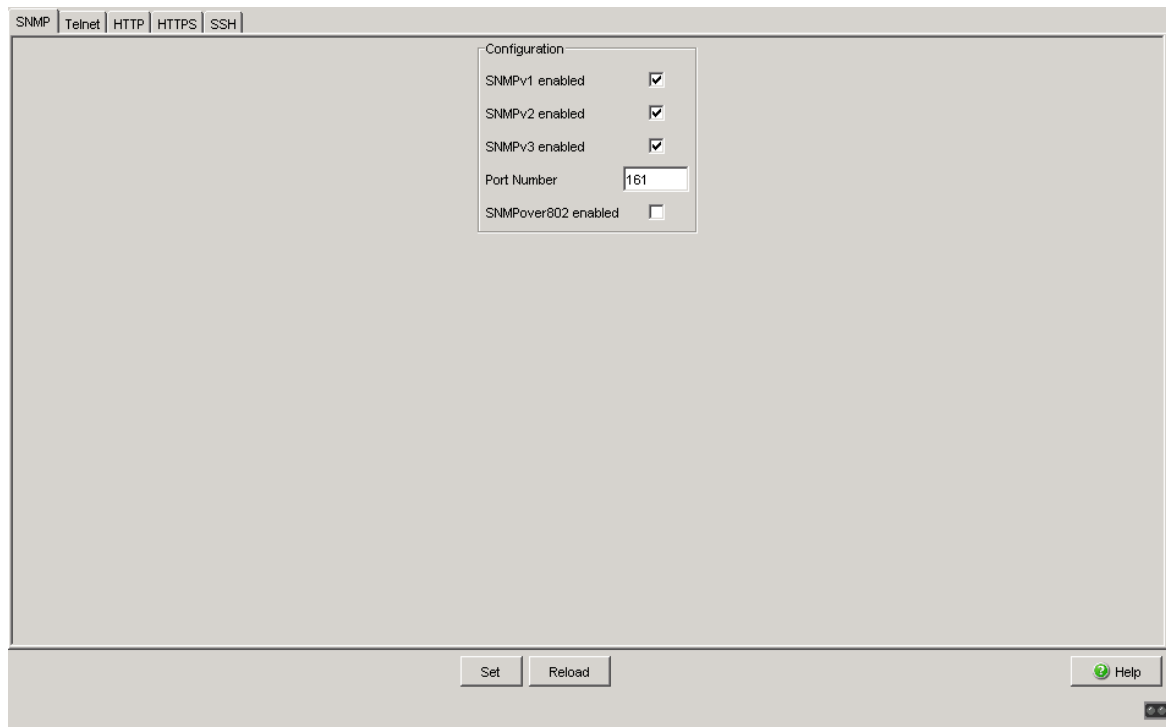


Figure 36: SNMP tab in the `Device Security > Management Access > Server` dialog

- To deactivate the SNMPv1 protocol, you remove the selection from the "SNMPv1 enabled" checkbox.
- To deactivate the SNMPv2 protocol, you remove the selection from the "SNMPv2 enabled" checkbox.
- To temporarily save the changes, click "Set".
- To permanently save the changes, you open the `Basic Settings > Load/Save` dialog and click "Save".

enable
configure

Switch to the privileged EXEC mode.
Switch to the Configuration mode.

```
no snmp access version v1
no snmp access version v2
show snmp access
save
```

Deactivates the SNMPv1 protocol.

Deactivates the SNMPv2 protocol.

Shows the settings of the SNMP server.

Saves the settings in the non-volatile memory of the device (NVM) in the “selected” configuration profile.

3.3.2 SNMPv3 access

The SNMP protocol allows you to monitor and configure the device via the network with a network management system (NMS). When the NMS accesses the device via SNMPv3, the NMS authenticates itself with a user's login data.

The prerequisite for network management access is that the same SNMPv3 parameters are specified in the device and in the NMS.

- ▶ When a new user account is being set up in the device, the default settings for the "SNMP Auth Type" and "SNMP Encryption Type" parameters are such that the Industrial HiVision network management software can access the device with it immediately.
- ▶ To monitor or configure the device with a different NMS, you adjust the following parameters in the relevant user account to match the settings in your NMS.

"SNMP Auth Type" parameter

- `hmacmd5`
Authentication with HMAC-MD5
- `hmacsha`
Authentication with HMAC-SHA

"SNMP Encryption Type" parameter


- `none`
Authentication unencrypted
- `des`
Authentication encrypted with DES
- `aesCfb128`
Authentication encrypted with AES-128 in Cipher Feedback mode.

The device allows you to specify the "SNMP Auth Type" and "SNMP Encryption Type" parameters individually in each user account.

Prerequisite: User account with authorization profile `administrator`.

Perform the following work steps:

- Adjust the SNMPv3 parameters in the user account to match the settings in your NMS.

 Open the `Device Security > User Management` dialog.

The dialog shows the user accounts that are set up.

User Name	Active	Password	Access Role	User locked	Policy Check	SNMP Auth Type	SNMP Encryption Type
admin	<input checked="" type="checkbox"/>	*****	administrator	<input type="checkbox"/>	<input type="checkbox"/>	hmacmd5	des
user	<input checked="" type="checkbox"/>	*****	guest	<input type="checkbox"/>	<input type="checkbox"/>	hmacmd5	des
<user>	<input checked="" type="checkbox"/>	*****	operator	<input type="checkbox"/>	<input type="checkbox"/>	hmacmd5	des

Configuration: Number of Login Attempts: 0, Minimum Password Length: 6

Password Policy: Minimum Upper Cases: 1, Minimum Lower Cases: 1, Minimum Numbers: 1, Minimum Special Characters: 1

Buttons: Set, Reload, Create, Remove, Help

Figure 37: Device Security > User Management dialog

- Click the row of the relevant user account in the "SNMP Auth Type" field. Select the desired setting.
- Click the row of the relevant user account in the "SNMP Encryption Type" field. Select the desired setting.
- To temporarily save the changes, click "Set".
- To permanently save the changes, you open the `Basic Settings > Load/Save` dialog and click "Save".

enable
configure

Switch to the privileged EXEC mode.
Switch to the Configuration mode.

```
users snmpv3 authentication  
  <user> md5 | sha1
```

Allocates the HMAC-MD5 or HMAC-SHA protocol for authentication requests to the <user> user account.

```
users snmpv3 encryption  
  <user> des | aescfb128 |  
  none
```

Allocates the DES or AES-128 algorithm to the <user> user account. With this algorithm, the device encrypts authentication requests. The value `none` removes the encryption.

```
show users
```

Shows the user accounts that are set up.

```
save
```

Saves the settings in the non-volatile memory of the device (NVM) in the “selected” configuration profile.

4 Managing configuration profiles


If you change the settings of the device during operation, the device stores the changes in its memory (RAM). After a reboot the settings are lost.

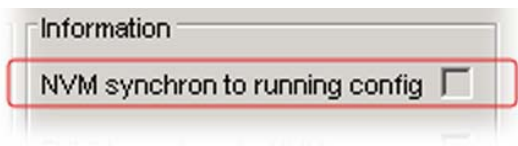
In order to keep the changes after a reboot, the device offers the possibility of saving additional settings in a configuration profile in the non-volatile memory (NVM). In order to make it possible to quickly switch to other settings, the non-volatile memory offers storage space for multiple configuration profiles.

4.1 Detecting changed settings

Changes made to settings during operation are stored by the device in its memory (RAM). The configuration profile in non-volatile memory (NVM) remains unchanged until you explicitly save it. Until then, the configuration profiles in memory and non-volatile memory differ.

This device helps you recognize changed settings. If the configuration profile in the memory (RAM) differs from the "selected" configuration profile in the non-volatile memory (NVM), you can recognize the difference based on the following criteria:

- The status bar at the top of the menu displays the icon  . If the configuration profiles match, the icon is hidden.
- The checkbox in the Basic Settings > Load/Save dialog, "Information" frame is unmarked. If the configuration profiles match, the checkbox is marked.



```
show config status
Configuration Storage sync State
-----
running-config to NV.....out of sync
...
```

4.2 Saving settings

Prerequisite: User account with authorization profile `administrator`.

4.2.1 Saving the configuration profile in the device

If you change the settings of the device during operation, the device stores the changes in its memory (RAM). In order to keep the changes after a reboot, save the configuration profile in non-volatile memory (NVM).

■ Saving a configuration profile

The device always stores the settings in the "selected" configuration profile in non-volatile memory (NVM).

Perform the following work steps:

- Open the Basic Settings > Load/Save dialog.

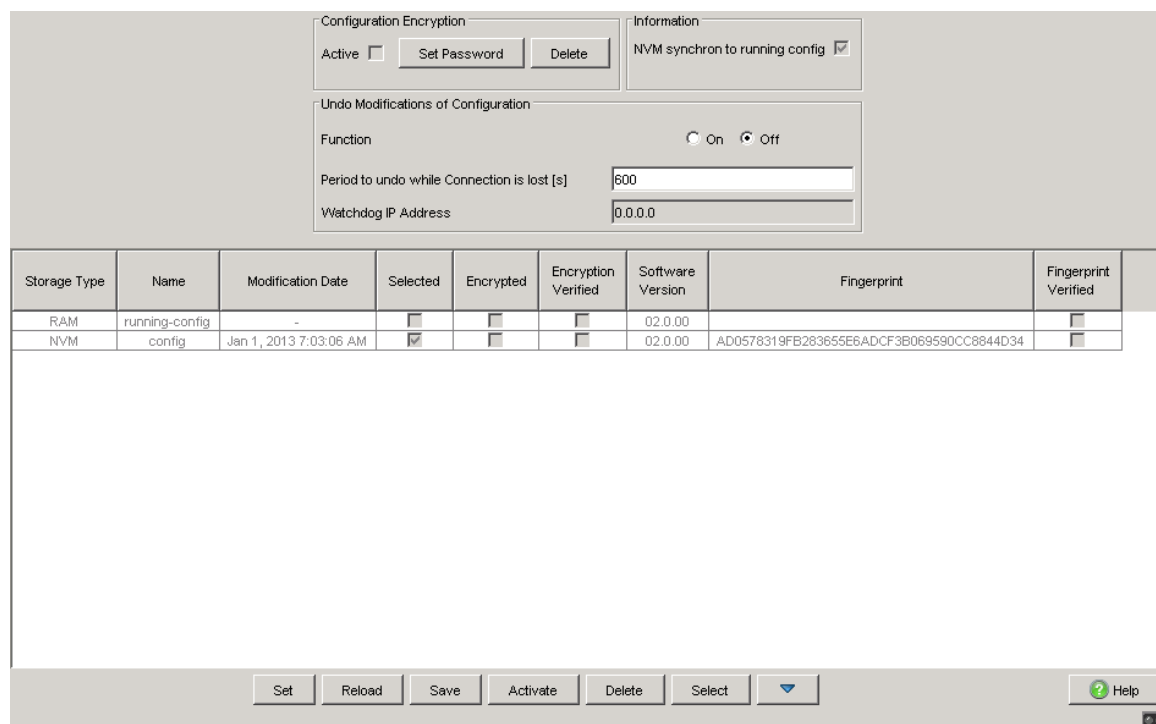


Figure 38: Basic Settings > Load/Save dialog

- Make sure that the desired configuration profile is "selected". You can recognize the "selected" configuration profile by the fact that the checkbox is selected in the "Selected" column.
- Click the "Set" button.

	<p>show config profiles nvm</p> <p>enable</p> <p>save</p>	<p>Displays the configuration profiles contained in non-volatile memory (NVM).</p> <p>Switch to the privileged EXEC mode.</p> <p>Saves the settings in the non-volatile memory of the device (NVM) in the "selected" configuration profile.</p>
--	---	---

■ **Copying settings to a configuration profile**

The device allows you to store the settings saved in memory (RAM) in a configuration profile other than the "selected" configuration profile. In this way you create a new configuration profile in non-volatile memory (NVM) or overwrite an existing one.

Perform the following work steps:

- Open the Basic Settings > Load/Save dialog.

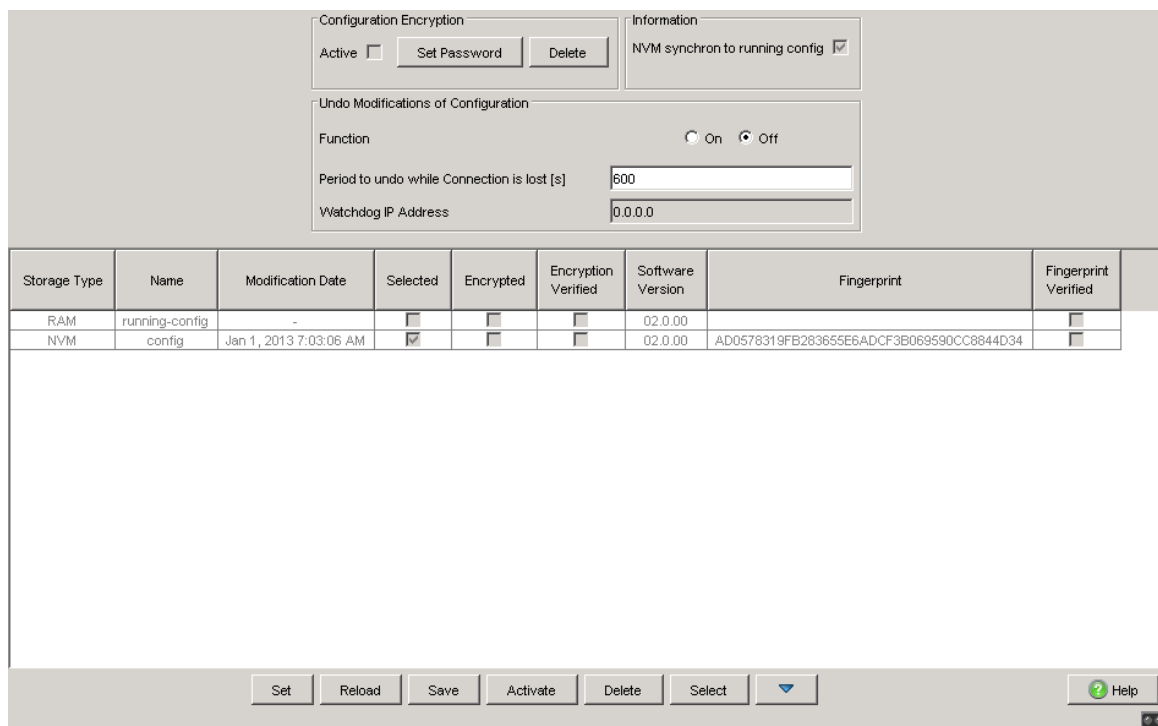


Figure 39: Basic Settings > Load/Save dialog

- Click the button, then "Save As...".
The dialog shows the "Save As..." window.

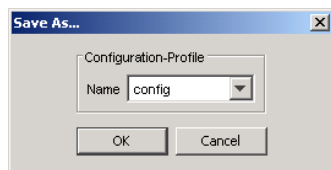


Figure 40: Save As... window in the *Basic Settings > Load/Save dialog*

- In the "Name" field, change the name of the configuration profile. If you keep the proposed name, the device will overwrite an existing configuration profile of the same name.
- Click the "OK" button.

The new configuration profile is marked as "selected".

```
show config profiles nvm
```

Displays the configuration profiles contained in non-volatile memory (NVM).

```
enable
```

Switch to the privileged EXEC mode.

```
copy config running-config  
nvm profile <string>
```

Save the current settings in the configuration profile named <string> in non-volatile memory (NVM). If present, the device overwrites a configuration profile of the same name. The new configuration profile is marked as "selected".

■ Selecting a configuration profile

If the non-volatile memory (NVM) contains several configuration profiles, you have the option to select any configuration profile there. The device always stores the settings in the "selected" configuration profile. Upon reboot, the device loads the settings of the "selected" configuration profile into memory (RAM).

Perform the following work steps:

- Open the Basic Settings > Load/Save dialog.

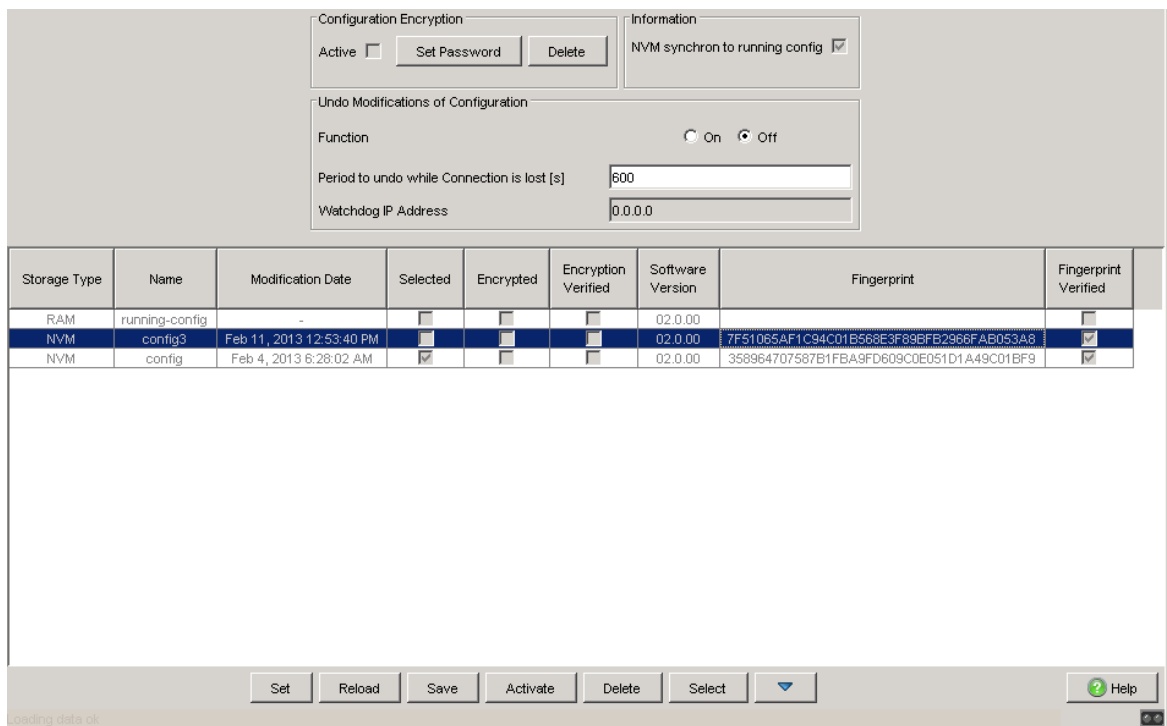


Figure 41: Basic Settings > Load/Save dialog

The table shows the configuration profiles present in the device. You can recognize the "selected" configuration profile by the fact that the checkbox is selected in the "Selected" column.

- Select the line of the desired configuration profile stored in non-volatile memory (NVM).
- Click the "Select" button.

In the "Selected" column, the checkbox of the configuration profile is now selected.

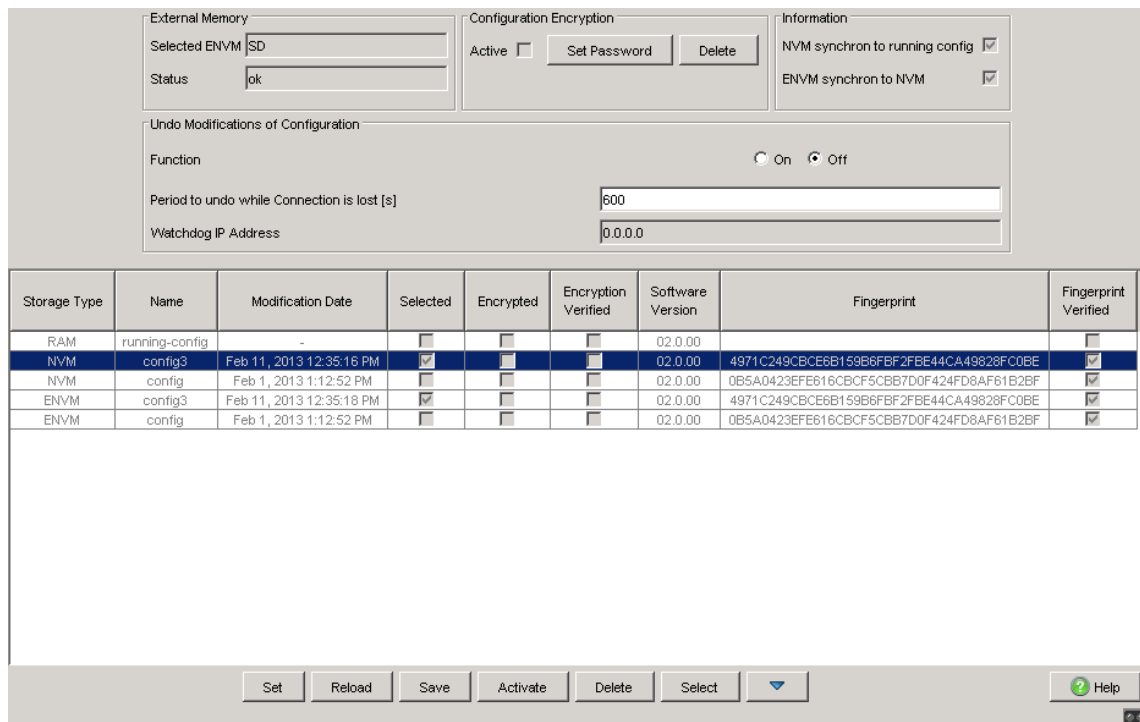


Figure 42: Basic Settings > Load/Save dialog

- enable Switch to the privileged EXEC mode.
- show config profiles nvm Displays the configuration profiles contained in non-volatile memory (NVM).
- configure Switch to the Configuration mode.
- config profile select nvm 1 Identifier of the configuration profile. Take note of the adjacent name of the configuration profile.
- save Saves the settings in the non-volatile memory of the device (NVM) in the "selected" configuration profile.

4.2.2 Exporting a configuration profile

The device offers you the option of saving a configuration profile to a server as an XML file. If you use the graphical user interface, you have the option to save the XML file directly to your PC.

Prerequisite:

- ▶ To save the file on a server, you need a configured server on the network.
- ▶ To save the file to an SCP or SFTP server, you also need the username and password for accessing this server.

Perform the following work steps:

- Open the `Basic Settings > Load/Save` dialog.

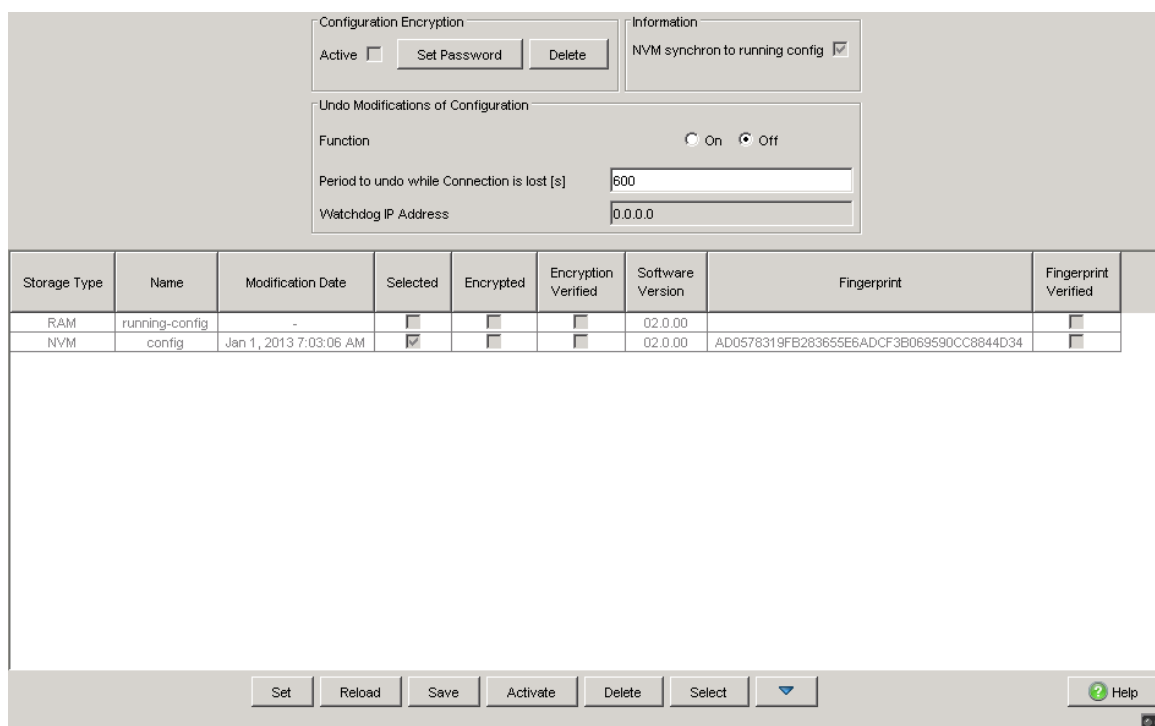



Figure 43: Basic Settings > Load/Save dialog

- Select the line of the desired configuration profile.
- Click the  button, then "Export...".
The dialog displays the "Export..." window.

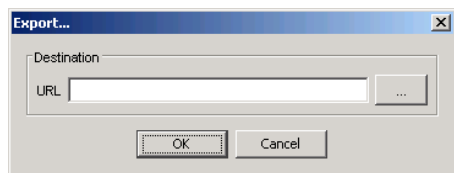


Figure 44: Export... window in the Basic Settings > Load/Save dialog

- You set the storage location and file name in the "Destination" frame:
 - To save the file on your PC, click the " ..." button and specify the storage location and file name.
 - To save a file to a TFTP server, specify the storage location and file name in the following form:
tftp://<IP address>/<path>/<file name>
 - To save the file to an SCP or SFTP server, specify the storage location and file name in the following form:
scp:// or sftp://<user>:<password>@<IP address>/<path>/<file name>
- Click the "OK" button.

The configuration profile is now saved as an XML file in the specified location.

<pre>show config profiles nvm</pre>	Displays the configuration profiles contained in non-volatile memory (NVM).
<pre>enable</pre>	Switch to the privileged EXEC mode.
<pre>copy config running-config remote tftp://<IP-Adresse>/ <Pfad>/<Dateiname></pre>	Save the configuration profile in memory (RAM) on a TFTP server.
<pre>copy config nvm remote tftp://<IP-Adresse>/ <Pfad>/<Dateiname></pre>	Save the selected configuration profile in non-volatile memory (NVM) on a TFTP server.
<pre>copy config nvm profile config3 remote tftp://<IP-Adresse>/ <Pfad>/<Dateiname></pre>	Save the configuration profile <code>config3</code> in non-volatile memory (NVM) on a TFTP server.

4.3 Loading settings

Through loading of settings, the device allows you to quickly switch to other settings if required.

Prerequisite: User account with authorization profile `administrator`.

4.3.1 Activating a configuration profile

The non-volatile memory of the device can accommodate several configuration profiles. If you activate a configuration profile stored there, you change the settings on the device on the fly without rebooting.

Perform the following work steps:

- Open the Basic Settings > Load/Save dialog.

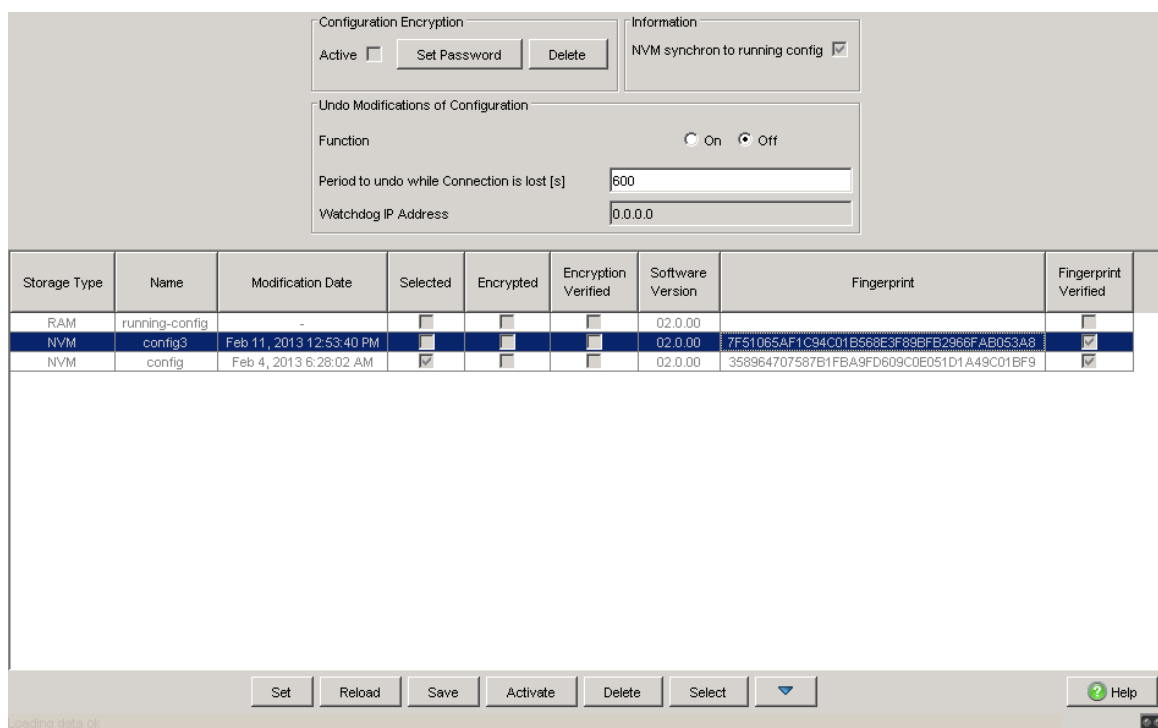


Figure 45: Basic Settings > Load/Save dialog

- Select the line of the desired configuration profile.
- Click the "Activate" button.

The device copies the settings to memory (RAM) and disconnects from the graphical user interface. The device immediately uses the settings of the configuration profile on the fly.

- Reload the graphical user interface.
- Login again.

In the "Selected" column, the checkbox of the configuration profile that was just activated is selected.

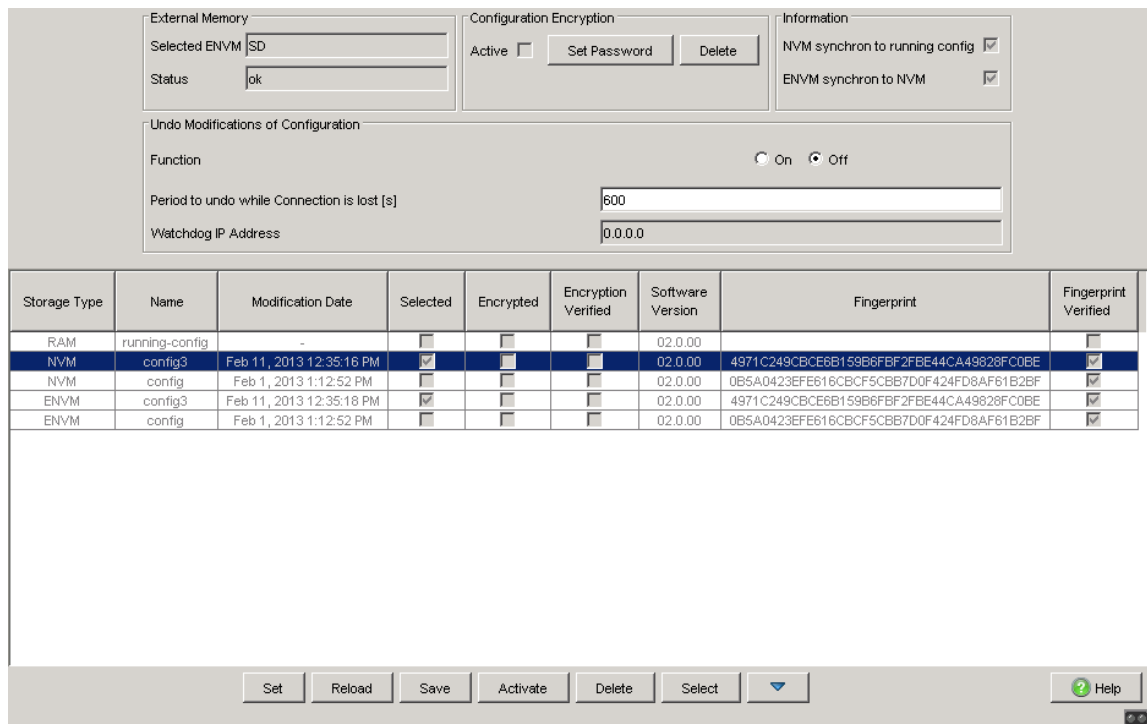


Figure 46: Basic Settings > Load/Save dialog

```
show config profiles nvm
enable
copy config nvm profile
config3 running-config
```

Displays the configuration profiles contained in non-volatile memory (NVM).
 Switch to the privileged EXEC mode.
 Activate the configuration profile `config3` in non-volatile memory (NVM).
 The device copies the settings into memory (RAM) and disconnects the CLI connection. The device immediately uses the settings of the configuration profile `config3` on the fly.

4.3.2 Importing a configuration profile

The device allows you to import from a server a configuration profile saved as an XML file. If you use the graphical user interface, you have the option to import the XML file directly from your PC.

Prerequisite:


- ▶ To save the file on a server, you need a configured server on the network.
- ▶ To save the file to an SCP or SFTP server, you also need the username and password for accessing this server.

Perform the following work steps:

- Open the Basic Settings > Load/Save dialog.

Storage Type	Name	Modification Date	Selected	Encrypted	Encryption Verified	Software Version	Fingerprint	Fingerprint Verified
RAM	running-config	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	02.0.0.0		<input type="checkbox"/>
NVM	config	Jan 1, 2013 7:03:06 AM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	02.0.0.0	AD0578319FB26365E6ADCF3B069590CC8844D34	<input type="checkbox"/>

Figure 47: Basic Settings > Load/Save dialog

- Click the  button, then "Import...".
The dialog shows the "Import..." window.

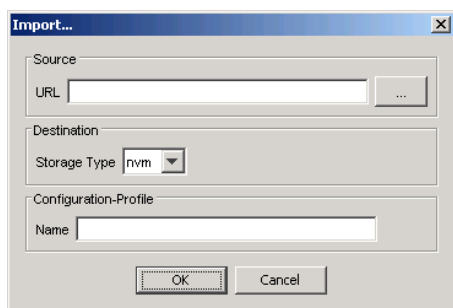


Figure 48: *Import...* window in the *Basic Settings > Load/Save dialog*

- In the "Source" frame, specify the storage location and file name:
 - To import the file from your PC, click the " ..." button and select the storage location and file name.
 - To import the file from a TFTP server, specify the storage location and file name in the following form:
tftp://<IP address>/<path>/<file name>
 - To import the file from an SCP or SFTP server, specify the storage location and file name in the following form:
scp:// or sftp://<user>:<password>@<IP address>/<path>/<file name>
- In the "Destination" frame, specify the memory into which the device copies settings during import.
- In the "Name" field, change the name of the configuration profile. If you keep the proposed name, the device will overwrite an existing configuration profile of the same name.
- Click the "OK" button.

The device copies the settings into the specified memory.

If you specified the value `ram` in the "Destination" frame, the device disconnects the graphical user interface and uses the settings immediately on the fly.

```
enable
copy config
remote tftp://<IP-Adresse>/
<Pfad>/<Dateiname>
running-config
```

Switch to the privileged EXEC mode.

Import a configuration profile from a TFTP server into memory (RAM).

The device copies the settings into memory (RAM) and disconnects the CLI connection. The device immediately uses these settings on the fly.

```
copy config remote
  sftp://<Benutzername>:<Pass
  wort>@<IP-Adresse>/<pfad>/
  <Dateiname> running-config
```

Import a configuration profile from an SFTP server to memory (RAM).

The device copies the settings into memory (RAM) and disconnects the CLI connection. The device immediately uses these settings on the fly.

```
copy config
  remote tftp://<IP-Adresse>/
  <Pfad>/<Dateiname>
  nvm profile config3
```

Import a configuration profile from a TFTP server, save in non-volatile memory (NVM) as configuration profile `config3`.

4.4 Resetting the device to the factory defaults

If you reset the settings in the device to the delivery state, the device deletes the configuration profiles in the volatile memory and in the non-volatile memory.

The device then reboots and loads the factory settings.

4.4.1 With the graphical user interface or CLI


Prerequisite: User account with authorization profile `administrator`.

Perform the following work steps:

- Open the `Basic Settings > Load/Save` dialog.

Storage Type	Name	Modification Date	Selected	Encrypted	Encryption Verified	Software Version	Fingerprint	Fingerprint Verified
RAM	running-config	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	02.0.00		<input type="checkbox"/>
NVM	config	Jan 1, 2013 7:03:06 AM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	02.0.00	AD0578319FB26365E6ADCF3B069590CC8844D34	<input type="checkbox"/>

Figure 49: Basic Settings > Load/Save dialog

- Click the  button, then "Back to factory defaults...".
The dialog displays a warning message.
- Click the "OK" button.

The device deletes the configuration profiles in the volatile memory and in the non-volatile memory.

After a brief period, the device restarts and loads the delivery settings.

enable
clear factory

Switch to the privileged EXEC mode.

Deleting the configuration profiles in the volatile memory (RAM) and in non-volatile memory (NVM). After a brief period, the device restarts and loads the delivery settings.

4.4.2 In the System Monitor

Prerequisite: Your PC is connected via terminal cable with the V.24 connection of the device.

Perform the following work steps:

- Restart the device.
- To switch to the System Monitor, press `1` within 3 seconds when prompted during reboot.
The device loads the System Monitor.
- To switch from the main menu to the `Manage configurations` menu, press `4`.
- To execute the `Clear configs and boot params` command, press `1`.
- To load the factory settings, press the Enter key.
The device deletes the configuration profiles in the memory (RAM) and in the non-volatile memory (NVM).

If an external memory is connected, the device also deletes the configuration profiles saved on the external memory.
- To switch to the main menu, press `q`.
- To reboot the device with factory settings, press `q`.

4.5 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.

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.

5 Synchronizing the System Time in the Network

Many applications rely on a time that is as correct as possible. The necessary accuracy, and thus the allowable deviation from the actual time, depends on the application area.

Examples of application areas include:

- ▶ Log entries
- ▶ Time stamping of production data
- ▶ Process control

The device offers the following options for synchronizing the time on the 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.

PTP is always the better choice if the involved devices support this protocol. PTP is more accurate, has advanced methods of error correction, and causes a low network load. The implementation of PTP is comparatively easy.

Note: According to the PTP and SNTP standards, both protocols function in parallel in the same network. However, since both protocols influence the system time of the device, situations may occur in which the two protocols conflict with each other.

The device also has two special outputs for synchronizing other devices. One output makes the device time available as an IRIG-B signal; a second output makes it available as a PPS frequency signal (1 pulse per second).

5.1 Basic settings

In the `Time > Basic Settings` dialog, you specify general settings for the time.

5.1.1 Setting the time

If no reference time source is available to you, you have the option to set the time in the device.

After a cold start or reboot, if no real-time clock is available or if the real-time clock contains an invalid time, the device initializes its clock with January 1, 00:00h. After the power supply is switched off, the device buffers the settings of the real-time clock up to 24 hours.

Alternatively, you configure the settings in the device so that it automatically obtains the current time from a PTP clock or from an SNTP server.

Perform the following work steps:

- Open the `Time > Basic Settings` dialog.
 - ▶ The "System Time (UTC)" field shows the current UTC (Universal Time Coordinated) of the device. UTC is the time relating to the coordinated world time measurement. UTC is the same worldwide and does not take local time shifts into account.
 - ▶ The time in the "System Time" field comes from the "System Time (UTC)" plus the "Local Offset [min]" value and a possible shift due to daylight saving time.

Note: PTP sends the International Atomic Time (TAI). The TAI time is 35 s ahead of UTC (as of July 1, 2012). If the PTP reference time source of the UTC offset is set correctly, the device automatically corrects this difference on the display in the "System Time (UTC)" field.

- In order to cause the device to apply the time of your PC to the "System Time" field, click the "Set Time from PC" button. Based on the value in the "Local Offset [min]" field, the device calculates the time in the "System Time (UTC)" field: The "System Time (UTC)" comes from the "System Time" minus the "Local Offset [min]" value and a possible shift due to daylight saving time.

- ▶ The "Time Source" field displays the origin of the time data. The device automatically selects the source with the greatest accuracy. The source is initially `local`. If PTP is active and if the device receives a valid PTP message, the device sets its time source to `ptp`. If SNTP is active and if the device receives a valid SNTP packet, the device sets its time source to `sntp`. The device prioritizes PTP ahead of SNTP.
- ▶ The "Local Offset [min]" value specifies the time difference between the local time and the "System Time (UTC)".
- In order to cause the device to determine the time zone on your PC, click the "Set Offset from PC" button. The device calculates the local time difference from UTC and enters the difference into the "Local Offset [min]" field.

Note: The device provides the option to obtain the local offset from a DHCP server.

- To temporarily save the changes, click "Set".
- To permanently save the changes, you open the `Basic Settings > Load/Save` dialog and click "Save".

```
enable
configure
clock set <YYYY-MM-DD>
<HH:MM:SS>
clock timezone offset
<-780..840>
save
```

Switch to the privileged EXEC mode.

Switch to the Configuration mode.

Set the system time of the device.

Enter the time difference between the local time and the received UTC time in minutes.

Saves the settings in the non-volatile memory of the device (NVM) in the "selected" configuration profile.

5.1.2 Automatic daylight saving time changeover

If you operate the device in a time zone in which there is a summer time change, you set up the automatic daylight saving time changeover on the "Daylight Saving Time" tab.

When daylight saving time is enabled, the device sets the local system time forward by 1 hour at the beginning of daylight saving time. At the end of daylight saving time, the device sets the local system time back again by 1 hour.

Perform the following work steps:

- Open the `Time > Basic Settings` dialog, "Daylight Saving Time" tab.
- To select a preset profile for the start and end of daylight saving time, click the "Profile..." button in the "Admin Status" frame.
- If no matching daylight saving time profile is available, you can define the changeover times in the fields "Summertime Begin" and "Summertime End".
For both time points, you define the month, the week within this month, the weekday, and the time of day.
- To enable automatic changeover to daylight saving time, select the `On` value in the "Admin Status" frame.
- To temporarily save the changes, click "Set".
- To permanently save the changes, you open the `Basic Settings > Load/Save` dialog and click "Save".

```
enable
configure
clock summer-time mode
<disable|recurring|eu|usa>

clock summer-time recurring
start
clock summer-time recurring
end
save
```

Switch to the privileged EXEC mode.

Switch to the Configuration mode.

Configure the automatic daylight saving time changeover: turn on or off or activate with a profile.

Enter the start time for the changeover.

Enter the end time for the changeover.

Saves the settings in the non-volatile memory of the device (NVM) in the "selected" configuration profile.

5.2 SNTP

The Simple Network Time Protocol (SNTP) allows 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 UTC is the same worldwide and ignores local time shifts.

SNTP is a simplified version of NTP (Network Time Protocol). The data packets are identical with SNTP and NTP. Accordingly, both NTP and SNTP servers serve as a time source for SNTP clients.

Note: Statements in this chapter relating to external SNTP servers also apply to NTP servers.

SNTP knows the following operation modes for the transmission of time:

- ▶ **Unicast:** In unicast operation mode, an SNTP client sends requests to an SNTP server and expects a response from this server.
- ▶ **Broadcast:** In broadcast operation mode, an SNTP server sends SNTP messages to the network in defined intervals. SNTP clients receive these SNTP messages and evaluate them.

IP destination address	Send SNTP packets to
0.0.0.0	Nobody
224.0.1.1	Multicast address for SNTP messages
255.255.255.255	Broadcast address

Table 6: Target address classes for broadcast operation mode

Note: An SNTP server in broadcast operation mode also responds to direct requests via unicast from SNTP clients. In contrast, SNTP clients work in either unicast or broadcast operation mode.

5.2.1 Preparation

Perform the following work steps:

- 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 delays of the SNTP messages. To minimize delays and their variance, place an SNTP server in each network segment. Each of these SNTP servers synchronizes its own system time as an SNTP client with its parent SNTP server (SNTP cascade). The highest SNTP server in the SNTP cascade has the most direct access to a reference time source.

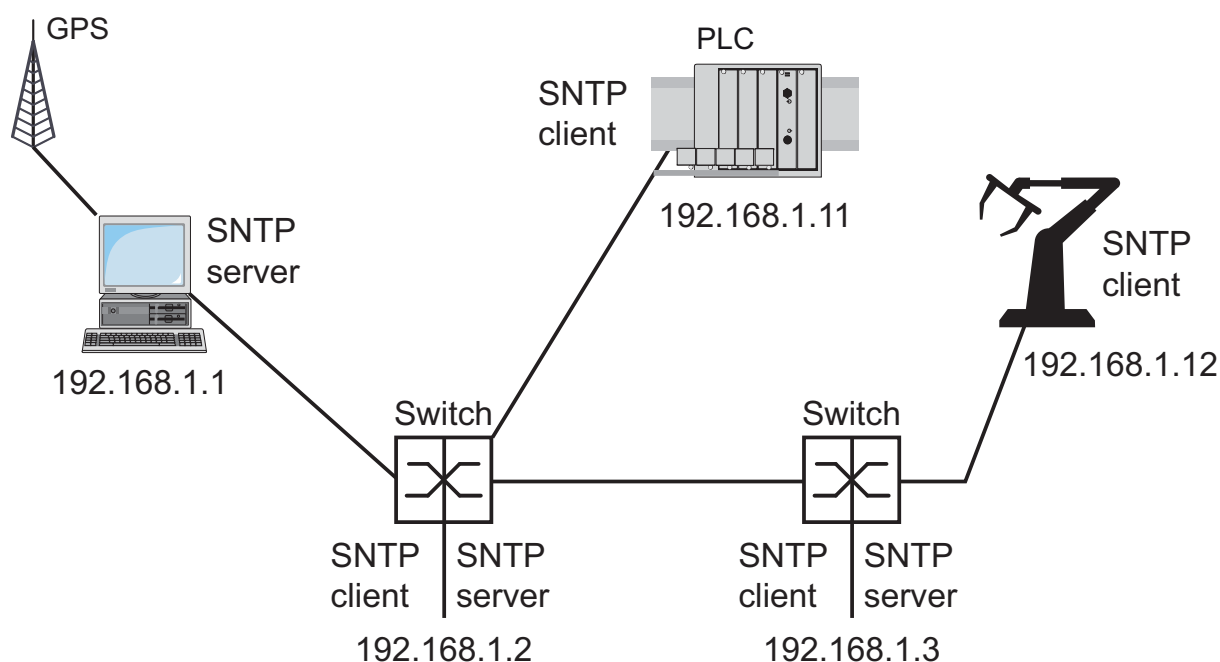


Figure 50: Example of SNTP cascade

Note: For precise time distribution, between SNTP servers and SNTP clients you preferably use network components (routers and switches) that forward the SNTP packets with a low and uniform transmission time (latency).

- ▶ An SNTP client sends its requests to up to 4 configured SNTP servers. If there is no response from the 1st SNTP server, the SNTP client sends its requests to the 2nd SNTP server. If this request is also unsuccessful, it sends the request to the 3rd and finally the 4th SNTP server. If none of these SNTP servers responds, the SNTP client loses its synchronization. The SNTP client periodically sends requests to each SNTP server until a server delivers a valid time.

Note: The device provides the option of obtaining a list of SNTP server IP addresses from a DHCP server.

- If no reference time source is available to you, determine a device with an SNTP server as a reference time source. Adjust its system time at regular intervals.

5.2.2 Defining settings of the SNTP client

As an SNTP client, the device obtains the time information from SNTP or NTP servers and synchronizes its system clock accordingly.

Perform the following work steps:

- Open the `Time > SNTP > Client` dialog.

Index	Description	Address	Target UDP Port	Status	Active
1	NTP Server	192.168.1.0	123	success	<input checked="" type="checkbox"/>

Figure 51: Time > SNTP > Client dialog

- Set the SNTP operation mode.
In the "Configuration" frame, select one of the following values in the "Mode" field:
 - ▶ unicast
The device sends requests to an SNTP server and expects a response from this server.
 - ▶ broadcast
The device waits for broadcast messages from SNTP servers on the network
- To synchronize the time only once, select the checkbox "Disable Client after successful Synchronization".
After synchronization, the device switches the SNTP client function back off again.

- ▶ The table shows the SNTP server to which the SNTP client sends a request in unicast operation mode. The table contains up to four SNTP server definitions.
- To add an SNTP server, click "Create". Enter the connection data of the SNTP server.
- To activate the SNTP client function, select the `On` value in the "Admin Status" frame.
- To temporarily save the changes, click "Set".
- ▶ The "Status" field shows the current status of the SNTP client function.
- To permanently save the changes, you open the `Basic Settings > Load/Save` dialog and click "Save".

Device	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
SNTP client function	Off	On	On	On	On
Configuration: Mode	unicast	unicast	unicast	unicast	unicast
Request interval	30	30	30	30	30
SNTP server address(es)	–	192.168.1.1	192.168.1.2 192.168.1.1	192.168.1.2 192.168.1.1	192.168.1.3 192.168.1.2 192.168.1.1

Table 7: SNTP client settings for the example

5.2.3 Specifying SNTP server settings

When the device operates as an SNTP server, it provides its system time in coordinated world time (UTC) in the network.

Perform the following work steps:

- Open the `Time > SNTP > Server` dialog.

The screenshot shows the 'Time > SNTP > Server' configuration dialog. It features three main sections: 'Operation', 'Configuration', and 'State'. In the 'Operation' section, the 'On' radio button is selected. The 'Configuration' section contains several fields: 'Listen UDP Port' is set to 123, 'Broadcast Admin Mode' is unchecked, 'Broadcast Destination Address' is set to 0.0.0.0, 'Broadcast Port' is 123, 'Broadcast VLAN ID' is 1, and 'Broadcast Send Interval [s]' is 128. The 'Disable Server at local Time Source' checkbox is also unchecked. The 'State' section shows 'syncToLocal'. At the bottom of the dialog are 'Set', 'Reload', and 'Help' buttons.

Figure 52: Time > SNTP > Server dialog

- To activate the SNTP server function, select the `On` value in the "Admin Status" frame.

- To turn on broadcast operation mode, select the checkbox "Broadcast Admin Mode" in the "Configuration" frame.
In the broadcast operation mode, the SNTP server sends SNTP messages to the network in defined intervals. The SNTP server also responds to the requests from SNTP clients in unicast operation mode.
 - In the "Broadcast Destination Address" field, you set the IP address to which the SNTP server sends the SNTP packets. Set a broadcast address or a multicast address.
 - In the "Broadcast Port" field, you enter the number of the UDP port to which the SNTP server sends the SNTP packets in broadcast operation mode.
 - In the "Broadcast VLAN ID" field, you enter the ID of the VLAN in which the SNTP server sends the SNTP packets in broadcast operation mode.
 - In the "Broadcast Send Interval [s]" field, you define the interval in which the SNTP server sends the SNTP packets in broadcast operation mode.
- To temporarily save the changes, click "Set".
- ▶ The "Status" field displays the current status of the SNTP server function.
- To permanently save the changes, you open the `Basic Settings > Load/Save` dialog and click "Save".

Device	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
SNTP Server Function	On	On	On	Off	Off
Listen UDP Port	123	123	123	123	123
Broadcast Admin Mode	Not selected	Not selected	Not selected	Not selected	Not selected
Broadcast Destination Address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Broadcast Port	123	123	123	123	123
Broadcast VLAN ID	1	1	1	1	1
Broadcast Send Interval	128	128	128	128	128
Disable Server at local Time Source	Not selected	Not selected	Not selected	Not selected	Not selected

Table 8: SNTP server settings for the example

5.3 PTP

In order for LAN-controlled applications to work without latency, precise time management is required. With PTP (Precision Time Protocol), IEEE 1588 describes a method that enables precise synchronization of clocks in the network.

PTP enables synchronization with an accuracy of a few 100 ns. PTP uses multicast for the synchronization messages, which keeps the network load low.

5.3.1 Types of clocks

PTP defines the roles of “master” and “slave” for the clocks in the network:

- ▶ A master clock (reference time source) distributes its time.
- ▶ A slave clock synchronizes itself with the timing signal received from the master clock.

■ Boundary clock

The transmission time (latency) in routers and switches has a measurable effect on the precision of the time transmission. To correct such inaccuracies, PTP defines what are known as boundary clocks.

In a network segment, a boundary clock is the reference time source (master clock) to which the subordinate slave clocks synchronize. Typically routers and switches take on the role of boundary clock.

The boundary clock in turn obtains the time from a higher-level reference time source (Grandmaster).

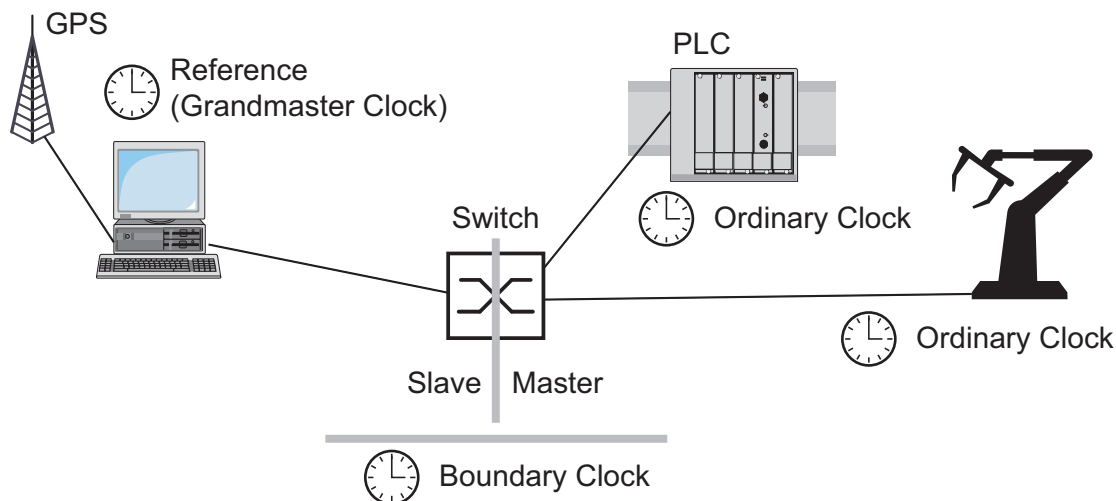


Figure 53: Position of the boundary clock in a network

■ **Transparent clock**

Switches typically take on the role of transparent clock to enable high accuracy across the cascades. The transparent clock is a slave clock that corrects its own transmission time when forwarding synchronization messages received.

■ **Ordinary clock**

PTP designates the clock in a terminal device as an “ordinary clock.” An ordinary clock functions either as a master clock or slave clock.

5.3.2 Best Master Clock algorithm

The devices participating in PTP designate a device in the network as a reference time source (Grandmaster). Here the “Best Master Clock” algorithm is used, which determines the accuracy of the clocks available in the network.

The “Best Master Clock” algorithm evaluates the following criteria:

- ▶ "Priority 1"
- ▶ "Class"
- ▶ "Clock Accuracy"
- ▶ "Clock Variance"
- ▶ "Priority 2"

The algorithm first evaluates priority 1 of the participating devices. The device with the smallest value for priority 1 becomes the reference time source (Grandmaster). If the value is the same for multiple devices, the algorithm takes the next criterion, and if this is also the same, it takes the next criterion after this one. If all the values are the same for multiple devices, the smallest value in the "Clock Identifier" field decides which device becomes the reference time source (Grandmaster).

The device offers you the option in the settings of the boundary clock to individually define the values for "Priority 1" and "Priority 2". This allows you to influence which device will be the reference time source (Grandmaster) in the network.

5.3.3 Delay measurement

The delay of the synchronization messages between the devices affects the accuracy. The delay measurement allows the devices to take into account the average delay.

PTP version 2 offers the following methods for delay measurement:

- ▶ **End-to-End (E2E)**
The slave clock measures the delay of synchronization messages to the master clock.
- ▶ **End-to-End optimized (E2E-optimized)**
The slave clock measures the delay of synchronization messages to the master clock.
This method is available only for transparent clocks. The device sends the synchronization messages sent via multicast only to the master clock, keeping the network load low. If the device receives a synchronization message from another master clock, it sends the synchronization messages only to this new port.
If the device knows no master clock, it sends synchronization messages to all device ports.
- ▶ **Peer-to-Peer (P2P)**
The slave clock measures the delay of synchronization messages to the master clock.
In addition, the master clock measures the delay to each slave clock, even across blocked ports. This requires that the master and slave clock support Peer-to-Peer (P2P).
In case of interruption of a redundant ring, for example, the slave clock becomes the master clock and the master clock becomes the slave clock. This switch occurs without loss of precision, because the clocks already know the delay in the other direction.

Note: When you select the value `P2P` then the device allows you to select the value `IEEE 802.3` exclusively in the "Network Protocol" field.

5.3.4 PTP domains

The device transmits synchronization messages only from and to devices in the same PTP domain. The device allows you to set the domain for the boundary clock and for the transparent clock individually.

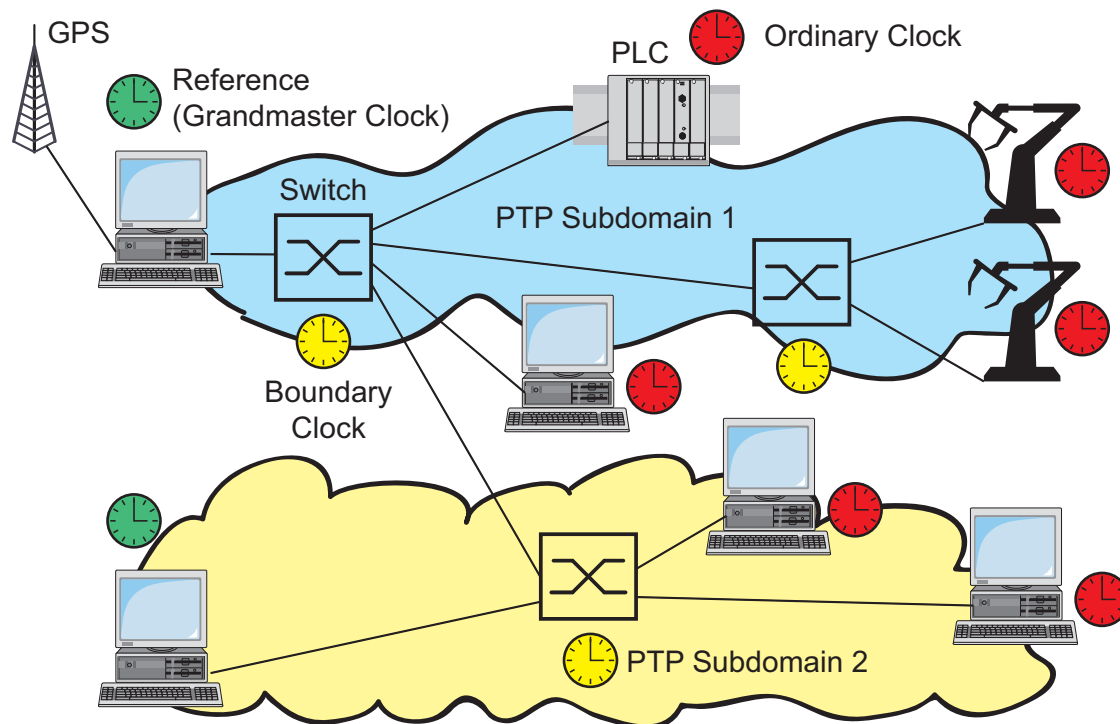


Figure 54: Example of PTP domains

5.3.5 Using PTP

In order to synchronize the clocks precisely with PTP, only use switches with a boundary clock or transparent clock as nodes.

Perform the following work steps:

- To gain an overview of the distribution of clocks, draw a network plan with the devices involved in PTP.
- Define the role for each participating switch (boundary clock or transparent clock). In the device, this setting is called "PTP Mode".

PTP mode	Application
v2-boundary-clock	As a boundary clock, the device distributes synchronization messages to the slave clocks in the subordinate network segment. The boundary clock in turn obtains the time from a higher-level reference time source (Grandmaster).
v2-transparent-clock	As a transparent clock, the device forwards received synchronization messages after they have been corrected by the delay of the transparent clock.

Table 9: Possible settings for PTP mode

- Turn on PTP on each participating switch.
PTP is then configured on a largely automatic basis.
- Turn on PTP on the terminal devices.
- In order to influence which device in the network will become the reference time source (Grandmaster), change the default value for "Priority 1" and "Priority 2" for the boundary clock.

5.4 IRIG-B/PPS

Your device has the following outputs on which it provides highly accurate time and frequency signals for other devices:

- ▶ **IRIG-B:** On the IRIG-B output, the device sends either the coordinated world time (UTC) or its local system time at a frequency of 100 pulses per second. The time signals correspond to the IRIG time code standard, which offers different time formats for selection.
- ▶ **PPS:** The PPS output (pulse per second) provides a highly accurate frequency signal. The cycle duration of the pulse is 1 second (200 ms high level, 800 ms low level).

On the two inputs, only connect devices that have appropriate signal inputs and can process the signals.

5.4.1 Preparation

Perform the following work steps:

- Check the terminal device to be connected in regard to its suitability for the respective output signal.
- Clarify which IRIG time formats the terminal device to be connected processes.
- The IRIG-B output provides the time as coordinated world time (UTC) or as local time. Find out which option is better suited to your application.

Code	Time format
<code>irig-b000</code>	Signal contains BCDtoy, CF, SBS (see key at end of table).
<code>irig-b001</code>	Signal contains BCDtoy, CF.
<code>irig-b002</code>	Signal contains BCDtoy.
<code>irig-b003</code>	Signal contains BCDtoy, SBS (initial setting).
<code>irig-b004</code>	Signal contains BCDtoy, BCDyear, CF, SBS.
<code>irig-b005</code>	Signal contains BCDtoy, BCDyear, CF.
<code>irig-b006</code>	Signal contains BCDtoy, BCDyear.
<code>irig-b007</code>	Signal contains BCDtoy, BCDyear, SBS.
Key	
BCDtoy	Binary Coded Decimal time of year (time during the year as a dual-coded decimal value)
BCDyear	Binary Coded Decimal year (year as a dual-coded decimal value)
CF	Control Functions (according to IEEE 1344)
SBS	Straight Binary Seconds of day (second of day, 0...86400)

Table 10: Allowable codes for different IRIG time formats

5.4.2 Turning on IRIG-B

Perform the following work steps:

- Open the `Time > IRIG-B/PPS` dialog, "IRIG-B" tab.

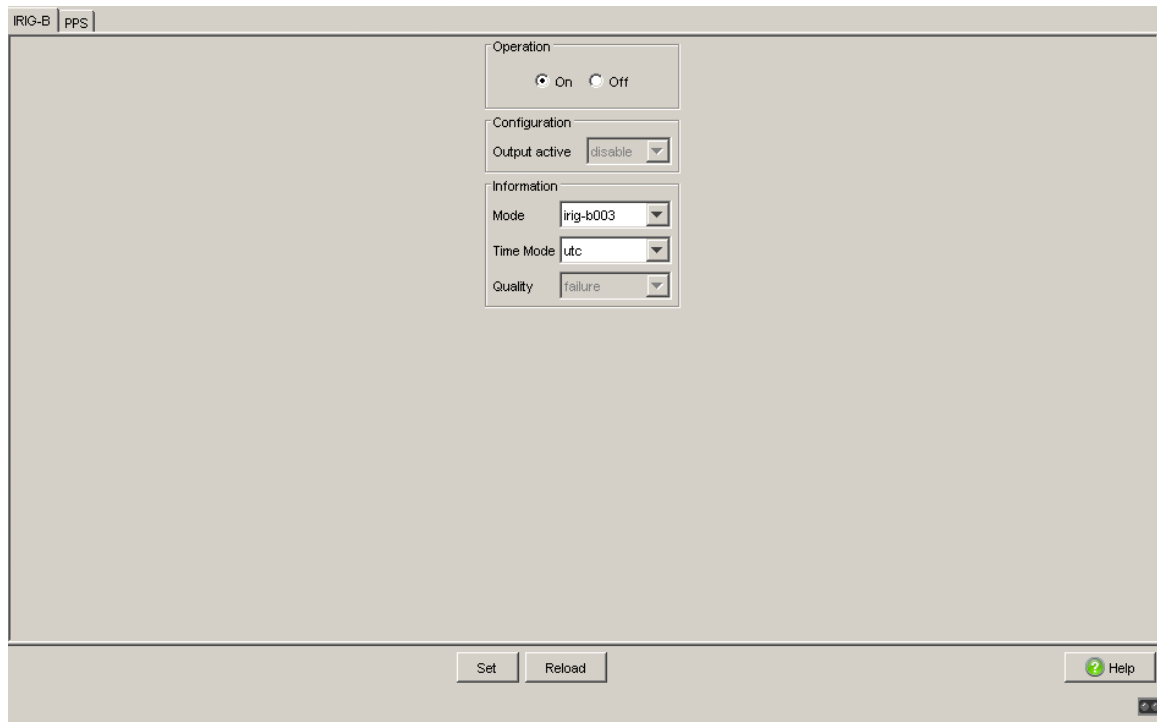


Figure 55: Time > IRIG-B/PPS dialog, "IRIG-B" tab.

- In the "Mode" field, select the desired IRIG time format.
- In the "Time Mode" field, select the time to be output.
- To turn on the output time signals, choose the `On` value in the "Admin Status" frame.
- To temporarily save the changes, click "Set".
- To permanently save the changes, you open the `Basic Settings > Load/Save` dialog and click "Save".

5.4.3 Turning on PPS

Perform the following work steps:

- Open the `Time > IRIG-B/PPS` dialog, "PPS" tab.



Figure 56: Time > IRIG-B/PPS dialog, "PPS" tab.

- To turn on the output of the frequency signals, select the `On` value in the "Admin Status" frame.
- To temporarily save the changes, click "Set".
- To permanently save the changes, you open the `Basic Settings > Load/Save` dialog and click "Save".

6 Network Load Control

The device features a number of functions that reduce the network load:

- ▶ Direct packet distribution
- ▶ Multicasts
- ▶ Rate limiter
- ▶ Prioritization - QoS
- ▶ Differentiated Services
- ▶ Flow control

6.1 Direct Packet Distribution

The device reduces the network load with direct packet distribution.

On each of its ports, the device learns the sender MAC address of received data packets. The device stores the combination “port and MAC address” in its MAC address table (FDB).

By applying the “store-and-forward” method, the device buffers data received and checks it for validity before forwarding it. The device rejects invalid and defective data packets.

6.1.1 Learning MAC addresses

If the device receives a data packet, it checks whether the MAC address of the sender is already stored in the MAC address table (FDB). If the MAC address of the sender is unknown, the device generates a new entry. The device then compares the destination MAC address of the data packet with the entries stored in the MAC address table (FDB):

- ▶ The device sends packets with a known destination MAC address directly to ports that have already received data packets from this MAC address.
- ▶ The device floods data packets with unknown destination addresses, that is, the device forwards these data packets to all ports.

6.1.2 Aging of learned MAC addresses

Addresses that have not been detected by the device for an adjustable period of time (aging time) are deleted from the MAC address table (FDB) by the device. A reboot or resetting of the MAC address table deletes the entries in the MAC address table (FDB).

6.1.3 Static address entries

In addition to learning the sender MAC address, the device also provides the option to set MAC addresses manually. These MAC addresses remain configured and survive resetting of the MAC address table (FDB) as well as rebooting of the device.

Static address entries allow the device to forward data packets directly to selected device ports. If you do not specify a destination port, the device discards the corresponding data packets.

You manage the static address entries in the graphical user interface (GUI) or in the CLI.

Prerequisite: User account with authorization profile `administrator` or `operator`.

Perform the following work steps:

- Create a static address entry.

- Open the `Switching > Filter for MAC Addresses` dialog.

Address	Status	VLAN ID	2/1	2/2	2/3	2/4
00 13 3b 00 01 8a	learned	1	-	-	learned	-
00 13 3b 0c 34 a0	learned	1	-	-	learned	-
00 13 3b 0c 34 a4	learned	1	-	-	learned	-
00 80 63 67 6f d1	learned	1	-	-	learned	-
00 80 63 97 50 0e	learned	1	-	-	learned	-
ec e5 55 01 29 10	learned	1	-	-	learned	-
ec e5 55 16 3e 00	mgmt	1	-	-	-	-

Figure 57: Switching > Filter for MAC Addresses dialog

- To add a user-configurable MAC address, click the "Create" button.

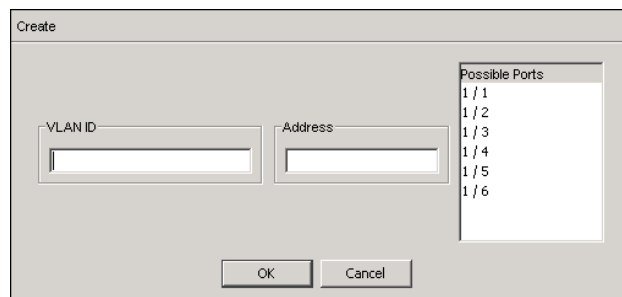


Figure 58: Create window in the *Switching > Filter for MAC Addresses* dialog

- In the "VLAN ID" field, specify the VLAN to which the table entry applies.
- In the "Address" field, define the destination MAC address to which the table entry applies.
- In the "Possible Ports" field, select the device ports to which the device sends data packets with the specified destination MAC address in the specified VLAN.
 - Select exactly one device port if you have defined a unicast MAC address in the "Address" field.
 - Select one or more device ports if you have defined a multicast MAC address in the "Address" field.
 - Do not select any device port if you want the device to discard data packets with the destination MAC address.
- Click the "OK" button.
- To temporarily save the changes, click "Set".
- To permanently save the changes, you open the *Basic Settings > Load/Save* dialog and click "Save".

```
enable
configure
mac-filter <MAC address>
  <VLAN ID>
interface 1/1
mac-filter <MAC address>
  <VLAN ID>
save
```

Switch to the privileged EXEC mode.

Switch to the Configuration mode.

Create the MAC address filter, consisting of a MAC address and VLAN ID.

Select interface 1 port 1.

Assign the port to a previously created MAC address filter.

Saves the settings in the non-volatile memory of the device (NVM) in the "selected" configuration profile.

Convert a learned MAC address into a static address entry.

Open the Switching > Filter for MAC Addresses dialog.

Address	Status	VLAN ID	2/1	2/2	2/3	2/4
00 13 3b 00 01 8a	learned	1	-	-	learned	-
00 13 3b 0c 34 a0	learned	1	-	-	learned	-
00 13 3b 0c 34 a4	learned	1	-	-	learned	-
00 80 63 67 6f d1	learned	1	-	-	learned	-
00 80 63 97 50 0e	learned	1	-	-	learned	-
ec e5 55 01 29 f0	learned	1	-	-	learned	-
ec e5 55 f6 3e 00	mgmt	1	-	-	-	-

Set Reload Create Edit Entry ? Help

Figure 59: Switching > Filter for MAC Addresses dialog

- To convert a learned MAC address into a static address entry, select the value `permanent` in the "Status" column.
- To temporarily save the changes, click "Set".
- To permanently save the changes, you open the `Basic Settings > Load/Save` dialog and click "Save".

Disable a static address entry.

Open the Switching > Filter for MAC Addresses dialog.

Address	Status	VLAN ID	2/1	2/2	2/3	2/4
00 13 3b 00 01 8a	learned	1	-	-	learned	-
00 13 3b 0c 34 a0	learned	1	-	-	learned	-
00 13 3b 0c 34 a4	learned	1	-	-	learned	-
00 80 63 67 6f d1	learned	1	-	-	learned	-
00 80 63 97 50 0e	learned	1	-	-	learned	-
ec e5 55 01 29 f0	learned	1	-	-	learned	-
ec e5 55 16 3e 00	mgmt	1	-	-	-	-

Set Reload Create Edit Entry Help

Figure 60: Switching > Filter for MAC Addresses dialog

- To disable a static address entry, select the value `invalid` in the "Status" column.
- To temporarily save the changes, click "Set".

```
enable
configure
interface 1/1
no mac-filter <MAC address>
  <VLAN ID>
exit
no mac-filter <MAC address>
  <VLAN ID>
exit
save
```

Switch to the privileged EXEC mode.
 Switch to the Configuration mode.
 Select interface 1 port 1.
 Cancel the assignment of the MAC address filter on the port.
 Switch to the Configuration mode.
 Delete the MAC address filter, consisting of a MAC address and VLAN ID.
 Switch to the privileged EXEC mode.
 Saves the settings in the non-volatile memory of the device (NVM) in the "selected" configuration profile.

Delete learned MAC addresses.

To delete the learned addresses from the MAC address table (FDB), open the `Basic Settings > Restart` dialog and click "Reset MAC Address Table" there.

`clear mac-addr-table`

Delete the learned MAC addresses from the MAC address table (FDB).

6.2 Multicasts

By default, the device floods data packets with a multicast address, that is, the device forwards the data packets to all ports. This leads to an increased network load.

The use of IGMP snooping can reduce the network load caused by multicast data traffic. IGMP snooping allows the device to send multicast data packets only on those ports to which devices “interested” in multicast are connected.

6.2.1 Example of a Multicast Application

Surveillance cameras transmit images to monitors in the machine room and in the monitoring room. With an IP multicast transmission, the cameras transmit their graphic data over the network in multicast packets.

The Internet Group Management Protocol (IGMP) organizes the multicast data traffic between the multicast routers and the monitors. The switches in the network between the multicast routers and the monitors monitor the IGMP data traffic continuously (“IGMP snooping”).

Switches register logins for receiving a multicast stream (IGMP report). The device then creates an entry in the MAC address table (FDB) and forwards multicast packets only to the ports on which it has previously received IGMP reports.

6.2.2 IGMP snooping

The Internet Group Management Protocol (IGMP) describes the distribution of multicast information between routers and connected receivers on Layer 3. “IGMP snooping” describes the function of a switch of continuously monitoring IGMP traffic and optimizing its own transmission settings for this data traffic.

The IGMP snooping function in the device operates according to RFC 4541 (Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches).

Multicast routers with an active IGMP function periodically request (query) registration of multicast streams in order to determine the associated IP multicast group members. IP multicast group members reply with a Report message. This Report message contains all the parameters required by IGMP. The multicast router enters the IP multicast group address from the Report message in its routing table. This causes it to forward data packets with this IP multicast group in the destination address field according to its routing table.

Receivers log out with a “Leave” message when leaving a multicast group (IGMP version 2 and higher) and do not send any more Report messages. The multicast router removes the routing table entry of a receiver if it does not receive any more Report messages from this receiver within a certain time (aging time).

If several IGMP multicast routers are in the same network, then the device with the smaller IP address takes over the query function. If there are no multicast routers on the network, then you have the option to turn on the query function in an appropriately equipped switch.

A switch that connects one multicast receiver with a multicast router analyzes the IGMP information with the IGMP snooping method.

The IGMP snooping method also makes it possible for switches to use the IGMP function. A switch stores the MAC addresses derived from IP addresses of the multicast receivers as recognized multicast addresses in its MAC address table (FDB). In addition, the switch identifies the ports on which it has received reports for a specific multicast address. In this way the switch transmits multicast packets exclusively on ports to which multicast receivers are connected. The other ports do not receive these packets.

A special feature of the device is the possibility of determining the processing of data packets with unknown multicast addresses. Depending on the setting, the device discards these data packets or forwards them to all ports. By default, the device transmits the data packets only to ports with connected devices, which in turn receive query packets. You also have the option of additionally sending known multicast packets to query ports.

■ Setting IGMP Snooping

Perform the following work steps:

- Open the `Switching > IGMP Snooping > Global` dialog.
- Under "Admin Status", you turn the IGMP snooping function of the device on or off globally.
When the IGMP snooping function is off, the device behaves as follows:
 - ▶ The device ignores the received query and report messages.
 - ▶ The device sends (floods) received data packets with a multicast address as the destination address on all ports.
- To temporarily save the configuration, click "Set".

Under the global activation option of the IGMP snooping function, you define individual settings for ports ("Interface" tab) or VLANs ("VLAN" tab). These settings are only effective if the IGMP snooping function is enabled globally for the device.

- Setting the IGMP snooping settings for a port:

- Open the "Interface" tab.

Interface		VLAN						
Port	Active	Group Membership Interval	Max Response Time	MRP Expiration Time	Fast Leave Admin Mode	Static Query Port	VLAN IDs	
2/1	<input checked="" type="checkbox"/>	260	10	260	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	
2/2	<input checked="" type="checkbox"/>	260	10	260	<input type="checkbox"/>	<input type="checkbox"/>	1	
2/3	<input checked="" type="checkbox"/>	260	10	260	<input type="checkbox"/>	<input type="checkbox"/>	1	
2/4	<input checked="" type="checkbox"/>	260	10	260	<input type="checkbox"/>	<input type="checkbox"/>	1	

Figure 61: Port tab in the `Switching > IGMP Snooping > Configuration` dialog

- To enable IGMP snooping on a particular port, select the "Active" checkbox on the line of the desired port.
- To temporarily save the configuration, click "Set".
- Setting the IGMP snooping settings for a VLAN:

- Open the "VLAN" tab.

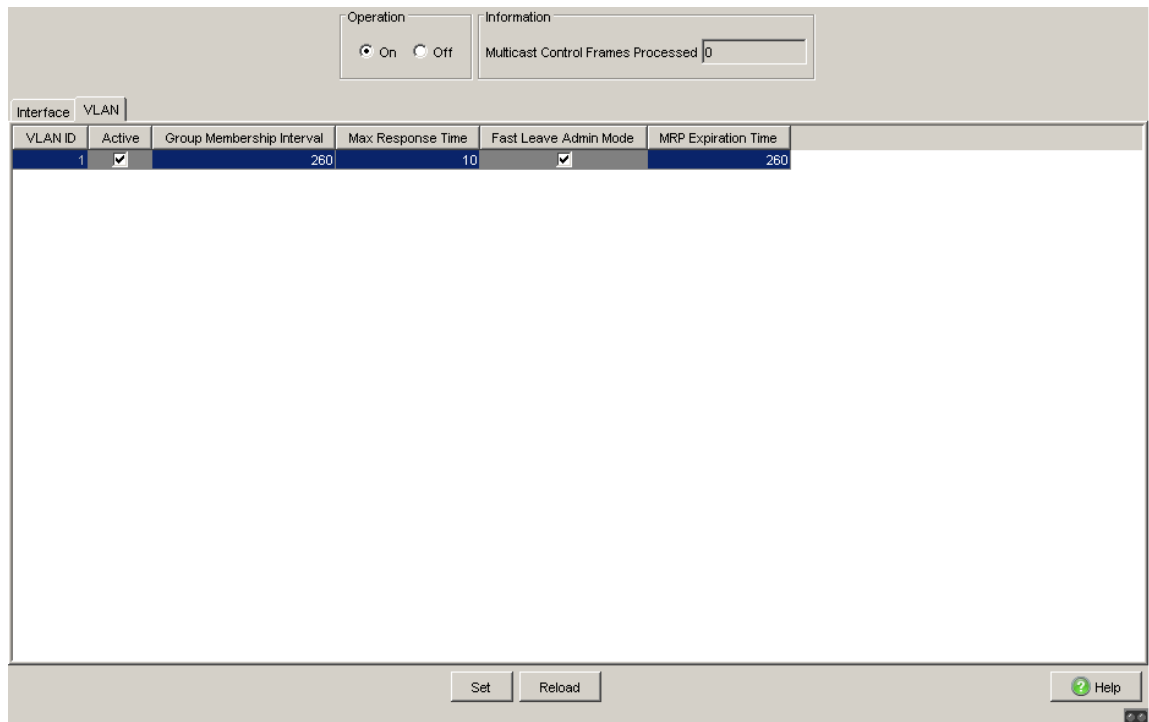


Figure 62: VLAN tab in the Switching > IGMP Snooping > Configuration dialog

- To enable IGMP snooping for a specific VLAN, select the "Active" checkbox on the table line of the desired VLAN.
- To temporarily save the configuration, click "Set".

■ Setting the IGMP querier function

The device itself optionally sends active query messages; alternatively, it responds to query messages or detects other multicast queriers in the network (IGMP querier function).

Prerequisite: The IGMP snooping function is activated globally.

Perform the following work steps:

- Define the settings for the IGMP querier function.

- Open the Switching > IGMP Snooping > Querier dialog.

VLAN ID	Active	Current State	Election Participate Mode	Address	Protocol Version	Max Response Time	Last Querier Address	Last Querier Version
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0.0.0.0	2	N/A	0.0.0.0	N/A

Figure 63: Switching > IGMP Snooping > Querier dialog

- In the "Admin Status" frame, turn the IGMP querier function of the device on or off globally.
- To enable the IGMP querier function for a specific VLAN, select the "Active" checkbox on the line of the desired VLAN.
- ▶ When the device recognizes another multicast querier in the corresponding VLAN when "Election Participate Mode" is activated, it carries out a simple selection process: If the IP source address of the other multicast querier is lower than its own, the device switches to the passive state, in which it does not send out any more query requests.

- ▶ Under "Address", you specify the IP multicast address that the device inserts as the sender address in generated query requests. You use the address of the multicast router.
- To temporarily save the configuration, click "Set".

■ IGMP Snooping Enhancements (Table)

The `Switching > IGMP Snooping > Snooping Enhancements` dialog provides you access to enhanced settings for the IGMP snooping function. You activate or deactivate the settings on a per port basis in a VLAN.

The following settings are possible:

- ▶ `Static`
Use this setting to set the port as a static query port. The device sends all IGMP messages on a static query port, even if it has previously received no IGMP query messages on this port. If the static option is disabled, the device sends IGMP messages on this port only if it has previously received IGMP query messages. If that is the case, the entry shows `L` ("learned").
- ▶ `Learn by LLDP`
A port with this setting automatically discovers other Hirschmann devices via LLDP (Link Layer Discovery Protocol). The device then learns the IGMP query status of this port from these Hirschmann devices and configures the IGMP query function accordingly. The `ALA` entry indicates that the Learn by LLDP function is enabled. If the device has found another Hirschmann device on this port in this VLAN, the entry also shows an `A` ("Automatic").
- ▶ `Forward All`
With this setting, the device sends the data packets addressed to a multicast address on this port. The setting is suitable in the following situations, for example:
 - For diagnostic purposes.
 - For devices in an MRP ring: After the ring is switched, the Forward All function allows rapid reconfiguration of the network for data packets with registered multicast destination addresses. Activate the Forward All function on all ring ports.

Prerequisite: The IGMP snooping function is activated globally.

To configure enhanced IGMP snooping settings, proceed as follows:

- Open the Switching > IGMP Snooping > Snooping Enhancements dialog.
- Double-click the desired port in the desired VLAN.
- To activate one or more functions, select the corresponding options.
- Click the "OK" button.
- To temporarily save the configuration, click "Set".

enable	Switch to the privileged EXEC mode.
vlan database	Switch to the VLAN mode.
igmp-snooping vlan-id 1	Activate the Forward All function for slot 1 / port 1
forward-all 1/1	in VLAN 1.

■ Configuring multicasts

The device allows you to configure the exchange of multicast data packets. The device provides different options depending on whether the data packets are to be sent to unknown or known multicast receivers.

The settings for unknown multicast addresses are global for the entire device. The following options can be selected:

- ▶ The device discards unknown multicasts.
- ▶ The device sends unknown multicasts on all ports.
- ▶ The device sends unknown multicasts exclusively on ports that have previously received query messages (query ports).

Note: The exchange settings for unknown multicast addresses also apply to the reserved IP addresses from the "Local Network Control Block" (224.0.0.0-224.0.0.255). This behavior may affect higher-level routing protocols.

For each VLAN, you define the sending of multicast packets to known multicast addresses individually. The following options can be selected:

- ▶ The device sends known multicasts on the ports that have previously received query messages (query ports) and to the registered ports. Registered ports are ports with multicast receivers registered with the corresponding multicast group. This option ensures that the transfer works with basic applications without further configuration.
- ▶ The device sends out known multicasts only on the registered ports. The advantage of this setting is that it uses the available bandwidth optimally through direct distribution.

Prerequisite: The IGMP snooping function is activated globally.

To configure multicasts, proceed as follows:

- Open the `Switching > IGMP Snooping > Multicasts` dialog.
- In the "Configuration" frame, you specify how the device sends data packets to unknown multicast addresses.
 - ▶ Send to Query Ports
The device sends packets with unknown multicast address to all query ports.
 - ▶ Send to All Ports
The device sends data packets with an unknown multicast address to all ports.
 - ▶ Discard
The device discards all packets with an unknown multicast address.
- In the "Known Multicasts" column, you specify how the device sends data packets to known multicast addresses in the corresponding VLAN. Click the relevant field and select the desired option.
- To temporarily save the configuration, click "Set".

6.3 Rate limiter

The rate limiter function allows you to limit the data traffic on the ports in order to ensure stable operation even when there is a high level of traffic. The rate limitation is performed individually for each port, as well as separately for inbound and outbound traffic.

If the data rate on a port exceeds the defined limit, the device discards the overload on this port.

Rate limitation occurs entirely on layer 2. In the process, the rate limiter function ignores protocol information on higher levels such as IP or TCP. This may affect the TCP traffic.

To minimize these effects, use the following options:

- ▶ Limit the rate limitation to certain frame types, for example, broadcasts, multicasts, and unicasts with unknown destination addresses.
- ▶ Limit the outbound data traffic instead of the inbound traffic. The outbound rate limitation works better with TCP flow control due to device-internal buffering of the data packets.
- ▶ Increase the aging time for learned unicast addresses ([see on page 146 “Aging of learned MAC addresses”](#)).

To configure the rate limiter function, proceed as follows:

- Open the `Switching > Rate Limiter` dialog.

Port	Threshold	Threshold Unit	Broadcast Mode	Multicast Mode	Unknown Unicast Mode
1/1	20	percent	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1/2	0	percent	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1/3	0	percent	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1/4	0	percent	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1/5	0	percent	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1/6	0	percent	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 64: *Switching > Rate Limiter dialog*

- ▶ On the "Input" tab, you configure the load limitation for inbound data traffic. Turn the rate limiter on or off and set limits for the data rate. The settings apply on a per port basis and are broken down by type of traffic:
 - ▶ Received broadcast data packets
 - ▶ Received multicasts
 - ▶ Received unicast data packets with an unknown destination address

To turn on the outbound rate limitation on a port, configure and activate the limitation for at least one category. In the "Threshold Unit" column, you choose whether you define the threshold values in percent of the inbound bandwidth of the port or in data packets per second. The threshold value 0 turns off rate limitation.

- On the "Egress" tab, you configure the rate limitation for outbound data traffic. This setting is disabled by default (value 0). To enable the rate limitation of the outbound traffic on one port, set a value between 1 and 100 in the "Bandwidth [%]" column. The percentage refers to the outbound bandwidth of the port.
- To temporarily save the configuration, click "Set".

6.4 QoS/Priority

QoS (Quality of Service) is a procedure defined in IEEE 802.1D. It is used to distribute resources in the network. QoS allows you to prioritize the data of important applications.

Prioritizing prevents data traffic with lower priority from interfering with delay-sensitive data traffic, especially when there is a heavy network load. Delay-sensitive data traffic includes, for example, voice, video, and real-time data.

6.4.1 Description of Prioritization

For data traffic prioritization, traffic classes are defined in the device. The device prioritizes higher traffic classes over lower traffic classes. The number of traffic classes depends on the device type.

To provide for optimal data flow for delay-sensitive data, you assign higher traffic classes to this data. You assign lower traffic classes to data that is less sensitive to delay.

■ Assigning traffic classes to the data

The device automatically assigns traffic classes to inbound data (traffic classification). The device takes the following classification criteria into account:

- ▶ Methods according to which the device carries out assignment of received data packets to traffic classes:
 - ▶ `trustDot1p`: The device uses the priority of the data packet contained in the VLAN tag.
 - ▶ `trustIpDscp`: The device uses the QoS information contained in the IP header (ToS/DiffServ).
 - ▶ `untrusted`: The device ignores possible priority information within the data packets and uses the priority of the receiving port directly.
- ▶ The priority assigned to the receiving port.

Both classification criteria are configurable.

During traffic classification, the device uses the following rules:

- ▶ When the receiving port is set to `trustDot1p` (state on delivery), the device uses the data packet priority contained in the VLAN tag. When the data packets do not contain a VLAN tag, the device is guided by the priority of the receiving port.
- ▶ When the receiving port is set to `trustIpDscp`, the device uses the QoS information (ToS/DiffServ) in the IP header. When the data packets do not contain IP packets, the device is guided by the priority of the receiving port.
- ▶ When the receiving port is set to `untrusted`, the device is guided by the priority of the receiving port.

■ **Prioritizing traffic classes**

For prioritization of traffic classes, the device uses the following methods:

- ▶ „Strict“
When transmission of data of a higher traffic class is no longer taking place or the relevant data is still in the queue, the device sends data of the corresponding traffic class. If all traffic classes are prioritized according to the “strict” method, under high network load the device may permanently block the data of lower traffic classes.
- ▶ „Weighted Fair Queuing“
The traffic class is assigned a guaranteed bandwidth. This ensures that the device sends the data traffic of this traffic class even if there is a great deal of data traffic in higher traffic classes.

6.4.2 Handling of Received Priority Information

Applications label data packets with the following prioritization information:

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

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

- ▶ `trustDot1p`
The device assigns VLAN-tagged data packets to the different traffic classes according to their VLAN priorities. The corresponding allocation is configurable. The device assigns the priority of the receiving port to data packets it receives without a VLAN tag.
- ▶ `trustIpDscp`
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 corresponding allocation is configurable. The device prioritizes non-IP packets according to the priority of the receiving port.
- ▶ `untrusted`
The device ignores the priority information in the data packets and assigns the priority of the receiving port to them.

6.4.3 VLAN tagging

For the VLAN and prioritizing functions, the IEEE 802.1Q standard provides for integrating a MAC frame in the VLAN tag. The VLAN tag consists of 4 bytes and is between the source address field (“Source Address Field”) and type field (“Length / Type Field”).

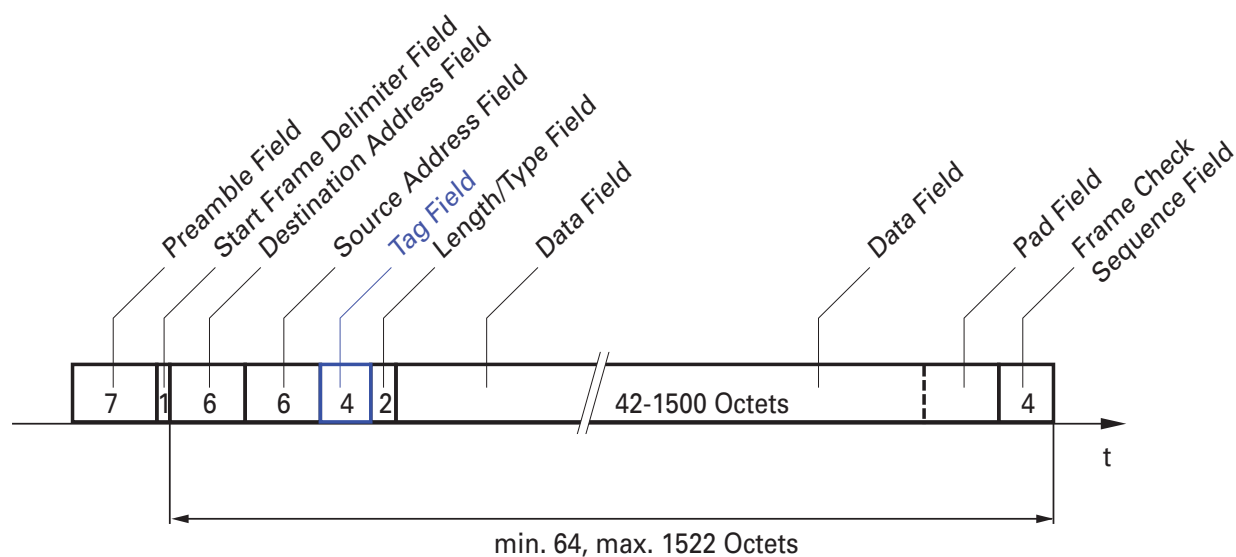


Figure 65: Ethernet data packet with tag

For data packets with VLAN tags, the device evaluates the following information:

- ▶ Priority information
- ▶ VLAN tagging, if VLANs are configured

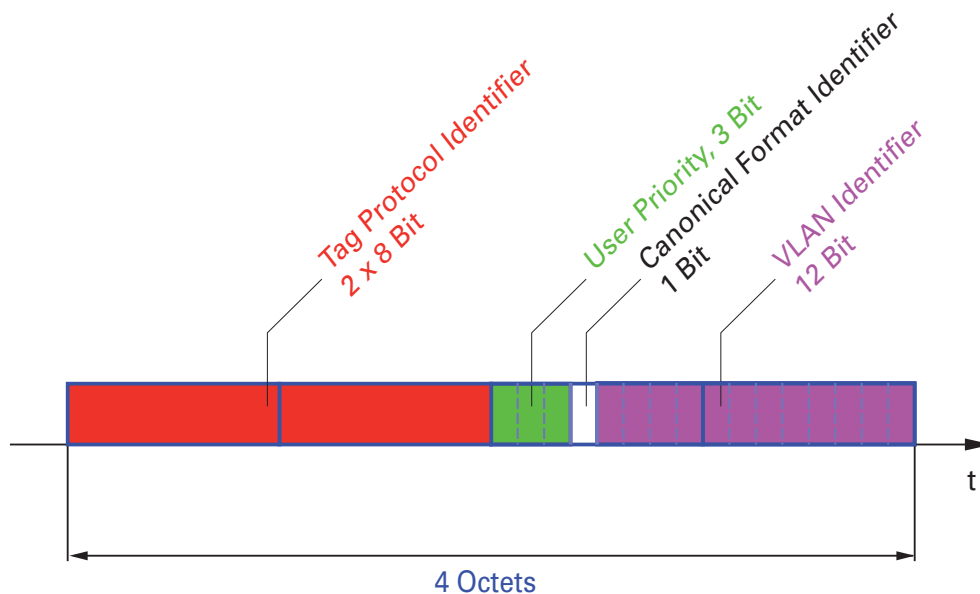


Figure 66: Structure of the VLAN tagging

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

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

When using VLAN prioritizing, consider the following special features:

- ▶ End-to-end prioritizing requires the VLAN tags to be transmitted to the entire network, which means that every network component needs to be VLAN-capable.
- ▶ Routers are not able to send and receive packets with VLAN tags through port-based router interfaces.

6.4.4 IP ToS

■ Type of Service

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



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

Table 11: ToS field in the IP header

6.4.5 Handling of traffic classes

The device provides the following options for handling traffic classes:

- ▶ Strict Priority
- ▶ Weighted Fair Queuing
- ▶ Strict Priority combined with Weighted Fair Queuing
- ▶ Queue Management

■ Description of Strict Priority

With the Strict Priority setting, the device first transmits data packets that have a higher traffic class (higher priority) before transmitting a data packet with the next highest traffic class. The device transmits a data packet with the lowest traffic class (lowest priority) when there are no other data packets remaining in the queue. In unfortunate cases, the device never sends packets with a low priority if there is a high volume of high-priority traffic waiting to be sent on this port.

In delay-sensitive applications, such as VoIP or video, Strict Priority allows Strict Priority data to be sent immediately.

■ 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 reserved values range from 0% through 100% of the available bandwidth, in steps of 1%.

- ▶ A reservation 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 of the corresponding port is available to you.

■ **Combining Strict Priority and Weighted Fair Queuing**

When combining Weighted Fair Queuing with Strict Priority, ensure that the highest traffic class of Weighted Fair Queuing is lower than the lowest traffic class of Strict Priority.

When you combine Weighted Fair Queuing with Strict Priority, a high Strict Priority network load can significantly reduce the bandwidth available for Weighted Fair Queuing.

6.4.6 Queue Management

■ Defining settings for Queue Management

- Open the Switching > QoS/Priority > Queue Management dialog.

Traffic Class	Strict Priority	Min Bandwidth [%]
0	<input type="checkbox"/>	5
1	<input type="checkbox"/>	20
2	<input type="checkbox"/>	30
3	<input checked="" type="checkbox"/>	0

Figure 67: Switching > QoS/Priority > Queue Management dialog

The total assigned bandwidth in the "Min Bandwidth [%]" column is 100%.

- To activate Weighted Fair Queuing for "Traffic Class" 0, proceed as follows:
 - ▶ Unmark the "Strict Priority" checkbox for the class.
 - ▶ In the "Min Bandwidth [%]" column enter 5.
- To activate Weighted Fair Queuing for "Traffic Class" 1, proceed as follows:
 - ▶ Unmark the "Strict Priority" checkbox for the class.
 - ▶ In the "Min Bandwidth [%]" column enter 20.
- To activate Weighted Fair Queuing for "Traffic Class" 2, proceed as follows:
 - ▶ Unmark the "Strict Priority" checkbox for the class.
 - ▶ In the "Min Bandwidth [%]" column enter 30.
- To activate Strict Priority Queuing for "Traffic Class" 3, proceed as follows:
 - ▶ Mark the "Strict Priority" checkbox for the class.

To temporarily save the configuration, click "Set".

```

enable                               Switch to the privileged EXEC mode.
configure                             Switch to the Configuration mode.
cos-queue weighted 0                 Enable Weighted Fair Queuing for traffic class 0.
cos-queue min-bandwidth: 0          Assign a weight of 5% to traffic class 0.
5
cos-queue weighted 1                 Enable Weighted Fair Queuing for traffic class 1.
cos-queue min-bandwidth: 1          Assign a weight of 20% to traffic class 1.
20
cos-queue weighted 2                 Enable Weighted Fair Queuing for traffic class 2.
cos-queue min-bandwidth: 2          Assign a weight of 30% to traffic class 2.
30
show cos-queue
Queue Id  Min. bandwidth  Scheduler type
-----  -
0          5                  weighted
1          20                 weighted
2          30                 weighted
3          0                  strict

```

6.4.7 Management prioritization

In order for you to have full access to the management of the device, even when there is a high network load, the device allows you to prioritize management packets.

When prioritizing management packets, 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.

6.4.8 Setting prioritization

■ Assigning the Port Priority

- Open the `QoS/Priority:Port` Configuration dialog.
- In the "Port Priority" column, you define the priority with which the device sends the data packets received on this port without a VLAN tag.
- In the "Trust Mode" column, you define the criteria the device uses to assign a traffic class to data packets received.
- To temporarily save the configuration, click "Set".

<pre>enable configure interface 1/1 vlan priority 3 exit</pre>	<p>Switch to the privileged EXEC mode.</p> <p>Switch to the Configuration mode.</p> <p>Switch to the Interface Configuration mode of interface 1/1.</p> <p>Assigns port priority 3 to interface 1/1.</p> <p>Switch to the Configuration mode.</p>
---	---

■ Assigning VLAN priority to a traffic class

- Open the `QoS/Priority:802.1D/p-Mapping` dialog.
- To assign a traffic class to a VLAN priority, insert the associated value in the "Traffic Class" column.
- To temporarily save the configuration, click "Set".

<pre>enable configure classofservice dotlp-mapping 0 2 classofservice dotlp-mapping 1 2 exit show classofservice dotlp-mapping</pre>	<p>Switch to the privileged EXEC mode.</p> <p>Switch to the Configuration mode.</p> <p>Assign traffic class 2 to VLAN priority 0.</p> <p>Also assign traffic class 2 to VLAN priority 1.</p> <p>Switch to the privileged EXEC mode.</p> <p>Display the assignment.</p>
---	--

■ Assign port priority to received data packets

```

enable
configure
interface 1/1

classofservice trust
  untrusted
classofservice
  dot1p-mapping 0 2
classofservice
  dot1p-mapping 1 2
vlan priority 1
exit
exit
show classofservice trust
Interface Trust Mode
-----
1/1      untrusted
1/2      dot1p
1/3      dot1p
1/4      dot1p
1/5      dot1p
1/6      dot1p
1/7      dot1p

```

Switch to the privileged EXEC mode.

Switch to the Configuration mode.

Switch to the Interface Configuration mode of interface 1/1.

Assign the "untrusted" mode to the interface.

Also assign traffic class 2 to VLAN priority 1.

Also assign traffic class 2 to VLAN priority 1.

Set the port priority to 1.

Switch to the Configuration mode.

Switch to the privileged EXEC mode.

Display the trust mode.

■ Assigning DSCP to a traffic class

- Open the `QoS/Priority:IP DSCP Mapping` dialog.
- Enter the desired value in the "Traffic Class" column.
- To temporarily save the configuration, click "Set".

```

enable
configure
classofservice
  ip-dscp-mapping cs1 1
show classofservice
  ip-dscp-mapping

```

Switch to the privileged EXEC mode.

Switch to the Configuration mode.

Assign traffic class 1 to DSCP CS1.

Show the IP DSCP assignments.

IP DSCP	Traffic Class
-----	-----
be	2
1	2
.	.
.	.
(cs1)	1
.	.

■ Assign the DSCP priority to received IP data packets

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.
classofservice trust ip-dscp	Assign the "trust ip-dscp" mode globally.
exit	Switch to the Configuration mode.
show classofservice trust	Display the trust mode.

Interface	Trust Mode
-----	-----
1/1	ip-dscp
1/2	dot1p
1/3	dot1p
.	.
.	.
1/5	dot1p
.	.

■ 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 interface 1/2.
traffic-shape bw 50	Limit the maximum bandwidth of port 1/2 to 50%.
exit	Switch to the Configuration mode.
exit	Switch to the privileged EXEC mode.
show traffic-shape	Display the traffic shaping configuration.

```

Interface      Shaping rate
-----
1/1            0 %
1/2            50 %
1/3            0 %
1/4            0 %

```

■ Configuring Layer 2 management priority

- Open the `QoS/Priority:Global` dialog.
- In the "VLAN Priority for Management packets" field, set the VLAN priority with which the device sends management data packets.
- To temporarily save the configuration, click "Set".

```

enable
network management priority
dot1p 7

show network parms

IPv4 Network
-----
...
Management VLAN priority.....7
...

```

Switch to the privileged EXEC mode.

Assign the VLAN priority of 7 to management packets. The device sends management packets with the highest priority.

Displays the management VLAN priority.

■ Configuring Layer 3 management priority

- Open the `QoS/Priority:Global` dialog.
- In the "IP DSCP Value for Management packets" field, set the DSCP value with which the device sends management data packets.
- To temporarily save the configuration, click "Set".

```

enable
network management priority
ip-dscp 56

show network parms

```

Switch to the privileged EXEC mode.

Assign the DSCP value of 56 to management packets. The device sends management packets with the highest priority.

Displays the management VLAN priority.



IPv4 Network

...

Management IP-DSCP value.....56

6.5 Flow Control

If a large number of data packets are received in the sending queue of a port at the same time, this can cause the port memory to overflow. This happens, for example, when the device receives data on a Gigabit port and forwards it to a port with a lower bandwidth. The device discards surplus data packets.

The flow control mechanism described in standard IEEE 802.3 ensures that no data packets are lost due to a port memory overflowing. Shortly before a port memory is completely full, the device signals to the connected devices that it is not accepting any more data packets from them.

- ▶ In full-duplex mode, the device sends a pause data packet.
- ▶ In half-duplex mode, the device simulates a collision.

The following figure shows how 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 is greater than the bandwidth of Workstation 4. This causes an overflow on the receive queue of port 4. The left funnel symbolizes this status.

If the flow control function on ports 1, 2 and 3 of the device is turned on. The device reacts before the funnel overflows. The funnel on the right illustrates ports 1, 2 and 3 sending a message to the transmitting devices to control the transmission speed. This results in the receiving port no longer being overwhelmed and is able to process the incoming traffic.

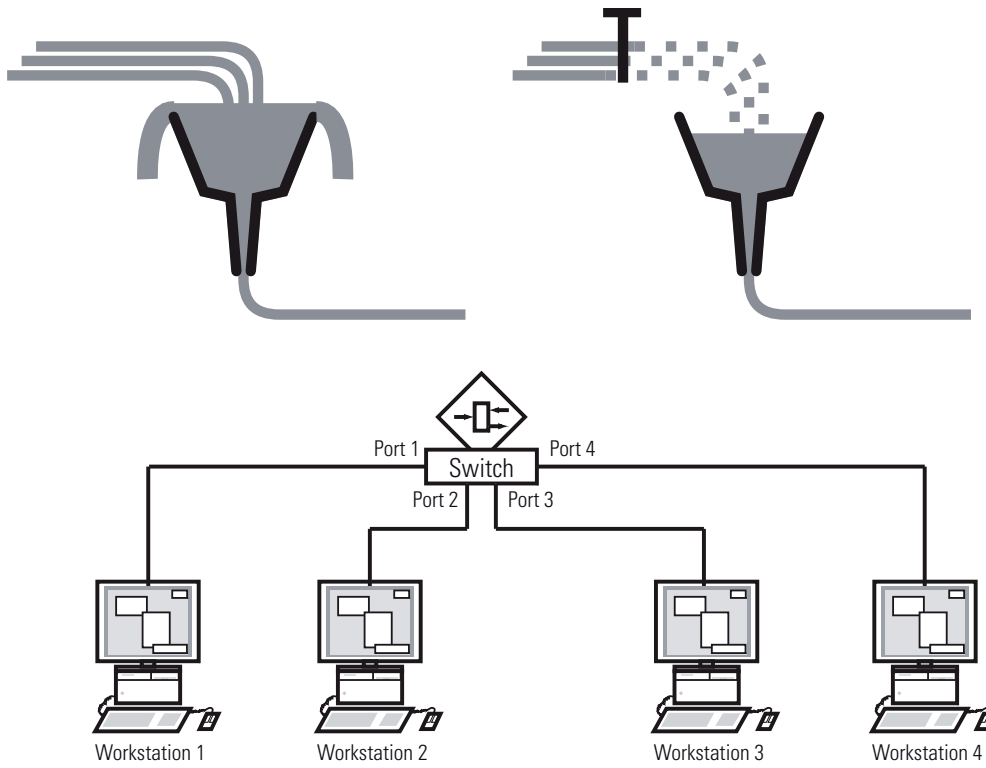


Figure 68: Example of flow control

6.5.1 Halfduplex or fullduplex link.

■ **Flow Control with a half duplex link**

In the example, there is a halfduplex link between Workstation 2 and the device.

Before the send queue of port 2 overflows, the device sends data back to Workstation 2. Workstation 2 detects a collision and stops transmitting.

■ **Flow Control with a full duplex link**

In the example, there is a fullduplex 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.

6.5.2 Setting the Flow Control

Perform the following work steps:

- Open the `Switching > Global` dialog.
- Select the "Activate Flow Control" checkbox.
With this setting you activate flow control in the device.
- Open the `Basic Settings > Port` dialog, "Configuration" tab.
- To turn on the flow control on a port, select the "Flow Control" option on the corresponding table line.
- To temporarily save the configuration, click "Set".

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.

7 VLANs

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. VLANs are an element of flexible network design. It is easier to reconfiguring logical connections centrally than cable connections.

The device supports independent VLAN learning in accordance with the IEEE 802.1Q standard which defines the VLAN function.

Although there are many benefits of using VLANs, the following lists the top benefits:

- ▶ **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 based on the function of the participants apart from their physical location or medium.
- ▶ **Clarity**
VLANs give networks a clear structure and make maintenance easier.

7.1 Examples of VLANs

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

Note: When configuring VLANs you use an interface for management that will remain unchanged. For this example, you use either interface 1/6 or the V.24 serial connection to configure the VLANs.

7.1.1 Example 1

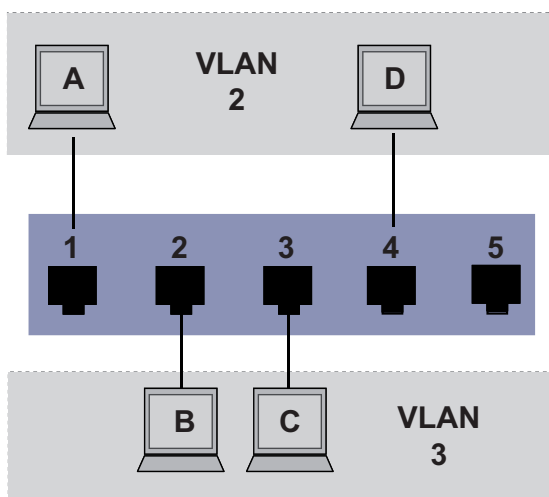


Figure 69: Example of a simple port-based VLAN

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 on which ports the device sends the frames from this VLAN.

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

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

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

Table 12: Ingress table

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

Table 13: Egress table

Proceed as follows to perform the example configuration:

Configure VLAN

Open the Switching > VLAN > Configuration dialog.

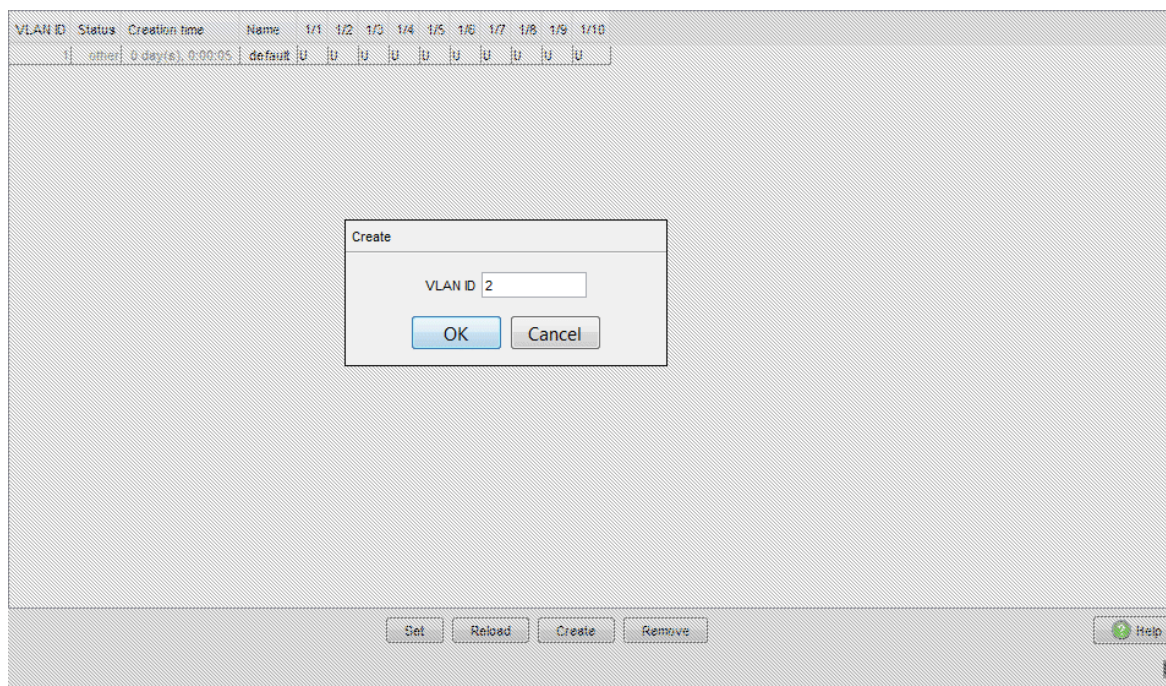


Figure 70: Creating and naming new VLANs

- To add a new VLAN to the table, click "Create".
- The "Create" window opens. Enter the new VLAN ID number, for example 2, in the text box.
- Click "OK".
- You give this VLAN the name `VLAN2` by clicking on the field and entering the name. Also change the name from `Default` to `VLAN1`.
- Repeat the previous steps and create another VLAN with the VLAN ID 3 and the name `VLAN3`.

```
enable
vlan database
vlan add 2
name 2 VLAN2

vlan add 3
name 3 VLAN3

name 1 VLAN1

exit
```

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

```

show vlan brief                Display the current VLAN configuration.
Max. VLAN ID..... 4042
Max. supported VLANs..... 16
Number of currently configured VLANs..... 3
vlan unaware mode..... 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 71: Defining the VLAN membership of the ports.

- Assign the ports of the device to the corresponding VLANs by clicking on the related table cell to open the selection menu and define the status. The selection options are:
 - ▶ - = currently not a member of this VLAN (GVRP allowed)
 - ▶ T = member of VLAN; send data packets with tag
 - ▶ U = Member of the VLAN; send data packets without tag
 - ▶ F = not a member of the VLAN (also disabled for GVRP)
 Because terminal devices usually interpret untagged data packets exclusively, you select the **U** setting here.
- To temporarily save the configuration, click "Set".
- Open the `Switching > VLAN > Port` dialog.

- Assign the Port VLAN ID of the related VLANs (2 or 3) to the individual ports - see table.

Port	Port-VLAN ID	Acceptable Frame Types	Ingress Filtering
1 / 1	2	admitAll	<input checked="" type="checkbox"/>
1 / 2	3	admitAll	<input checked="" type="checkbox"/>
1 / 3	3	admitAll	<input checked="" type="checkbox"/>
1 / 4	2	admitAll	<input checked="" type="checkbox"/>
1 / 5	1	admitAll	<input checked="" type="checkbox"/>
1 / 6	1	admitAll	<input type="checkbox"/>
		admitOnlyVlanTag	<input type="checkbox"/>

Set Reload Help

Figure 72: Assigning and saving "Port VLAN ID", "Acceptable Frame Types" and "Ingress Filtering"

- Because terminal devices usually send data packets as untagged, you select the `admitAll` setting for the "Acceptable Frame Types".
- The setting for "Ingress Filtering" has no effect on how this example functions.
- To temporarily save the configuration, click "Set".
- Open the `Basic Settings > External Memory` dialog.
- To save the configuration permanently in the external memory, activate the "Auto-save config on envm" checkbox and click "Set".

```
enable
configure
interface 1/1
```

```
vlan participation include 2
vlan pvid 2
exit
interface 1/2
```

Switch to the privileged EXEC mode.

Switch to the Configuration mode.

Switch to the Interface Configuration mode of interface 1/1.

Port 1/1 becomes member untagged in VLAN 2.

Port 1/1 is assigned the port VLAN ID 2.

Switch to the Configuration mode.

Switch to the interface configuration mode for interface 1/2.

```

vlan participation include 3
vlan pvid 3
exit
interface 1/3

vlan participation include 3
vlan pvid 3
exit
interface 1/4

vlan participation include 2
vlan pvid 2
exit
exit
show vlan id 3
VLAN ID          : 3
VLAN Name        : VLAN3
VLAN Type        : Static
Interface        Current   Configured   Tagging
-----
1/1              -         Autodetect   Tagged
1/2              Include   Include      Untagged
1/3              Include   Include      Untagged
1/4              -         Autodetect   Tagged
1/5              -         Autodetect   Tagged

```

Port 1/2 becomes member untagged in VLAN 3.
Port 1/2 is assigned the port VLAN ID 3.
Switch to the Configuration mode.

Switch to the Interface Configuration mode of Interface 1/3.

Port 1/3 becomes member untagged in VLAN 3.
Port 1/3 is assigned the port VLAN ID 3.
Switch to the Configuration mode.

Switch to the interface configuration mode of interface 1/4.

Port 1/4 becomes member untagged in VLAN 2.
Port 1/4 is assigned the port VLAN ID 2.
Switch to the Configuration mode.

Switch to the privileged EXEC mode.
Show details for VLAN 3.

7.1.2 Example 2

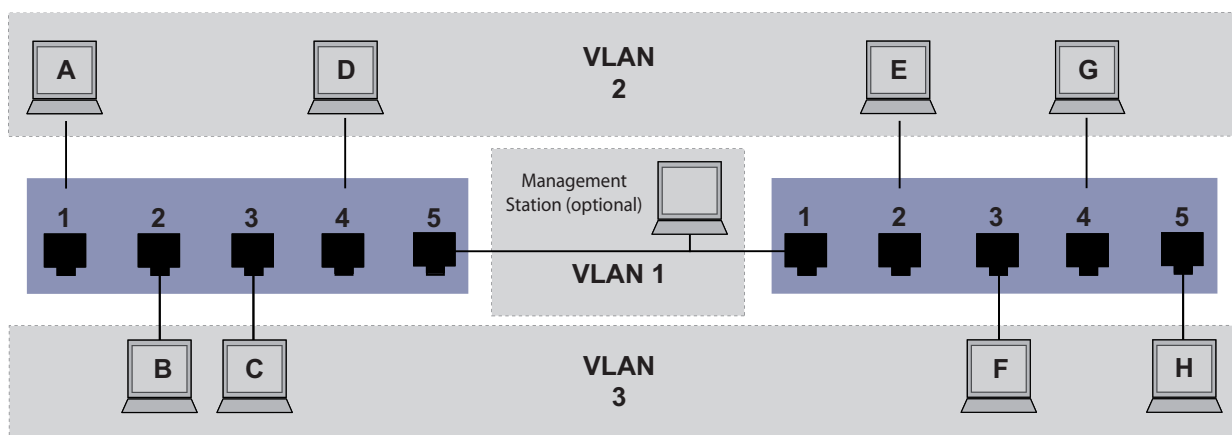


Figure 73: Example of a more complex VLAN configuration

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 on which ports the device sends the frames from this VLAN.

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

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

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

Table 14: Ingress table for device on left

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

Table 15: Ingress table for device on right

VLAN ID	Port				
	1	2	3	4	5
1					U

Table 16: Egress table for device on left

VLAN ID	Port
2	U U T
3	U U T

Table 16: Egress table for device on left

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

Table 17: Egress table for device on right

The communication relationships here are as follows: terminal devices on ports 1 and 4 of the left device and terminal devices on 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 on ports 2 and 3 of the left device and the terminal devices on 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, the devices use VLAN tagging (IEEE 801.1Q) within the VLAN with the ID 1 (Uplink). The letter T in the egress table of the ports indicates VLAN tagging.

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 > Configuration dialog.

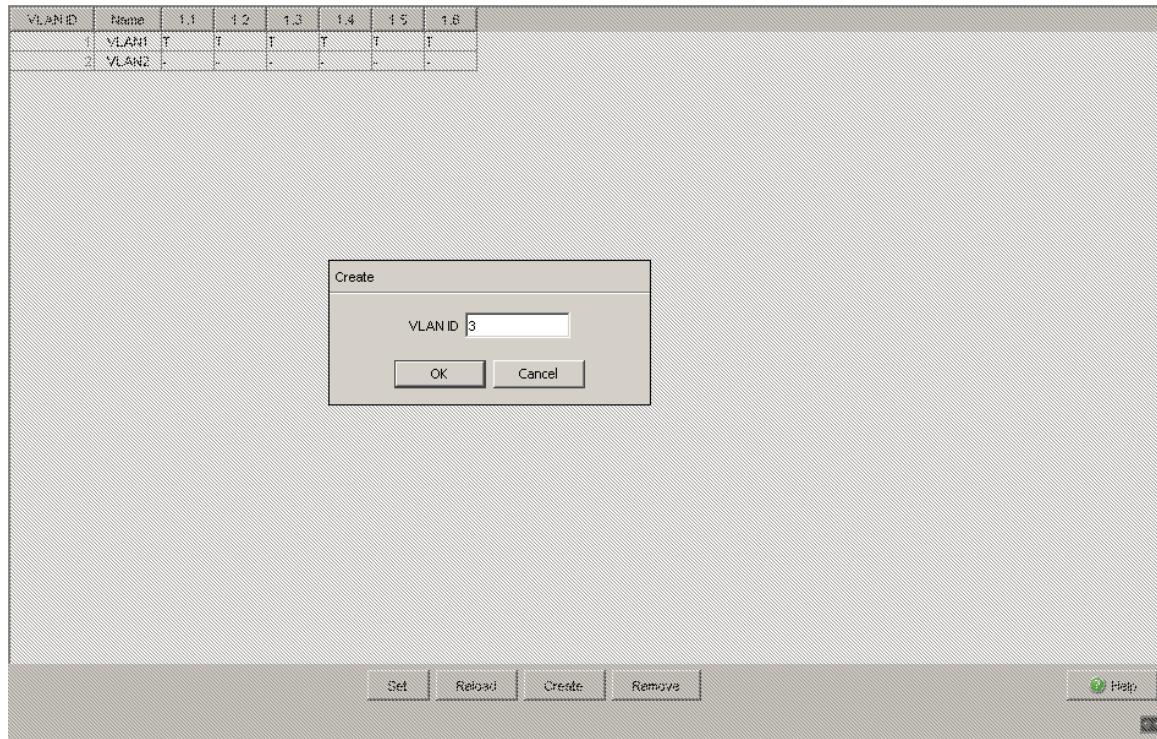


Figure 74: Creating and naming new VLANs

- To add a new VLAN to the table, click "Create".
- The "Create" window opens. Enter the new VLAN ID number, for example 2, in the text box.
- You give this VLAN the name VLAN2 by clicking on the field and entering the name. Also change the name from Default to VLAN1.
- Repeat the previous steps and create another VLAN with the VLAN ID 3 and the name VLAN3.

```
enable
vlan database
vlan add 2
name 2 VLAN2

vlan add 3
name 3 VLAN3

name 1 VLAN1

exit
```

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

```

show vlan brief                               Display the current VLAN configuration.
Max. VLAN ID.....                          4042
Max. supported VLANs.....                    16
Number of currently configured VLANs.....    3
vlan unaware mode.....                        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

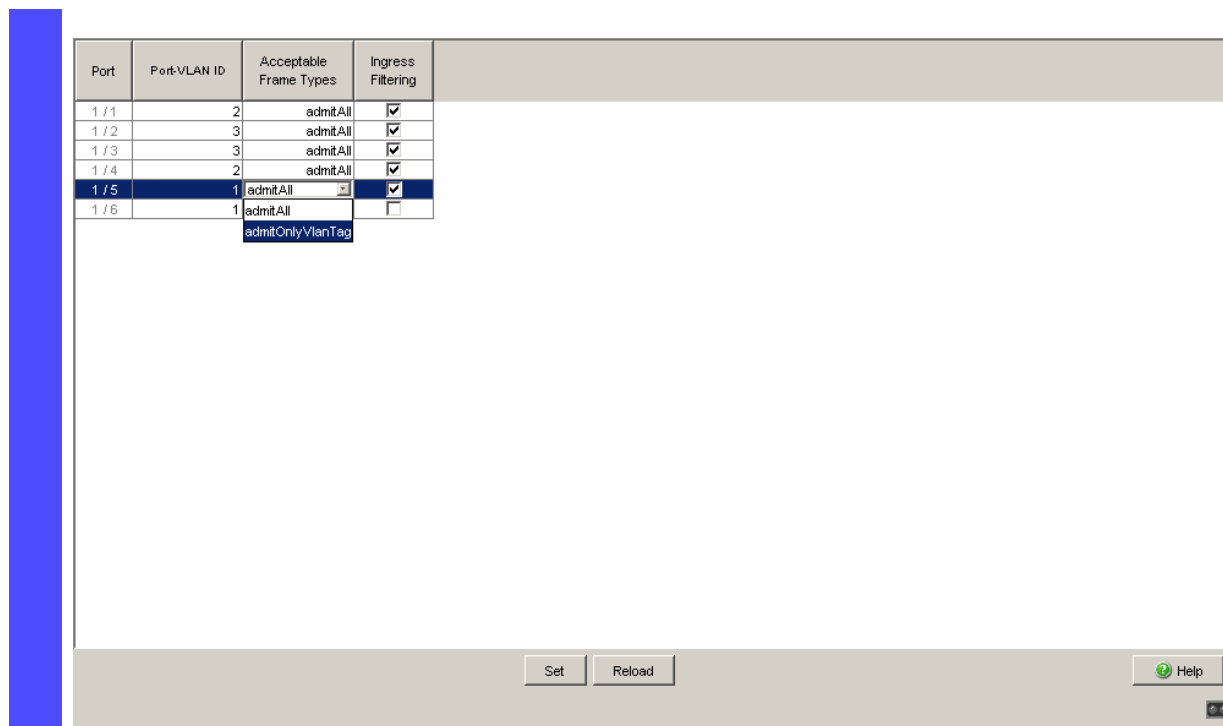


Figure 75: Defining the VLAN membership of the ports.

- 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.

- To temporarily save the configuration, click "Set".

- Open the Switching > VLAN > Port dialog.
- Assign the ID of the related VLANs (1 to 3) to the individual ports.

Port	Port-VLAN ID	Acceptable Frame Types	Ingress Filtering
1 / 1	2	admitAll	<input checked="" type="checkbox"/>
1 / 2	3	admitAll	<input checked="" type="checkbox"/>
1 / 3	3	admitAll	<input checked="" type="checkbox"/>
1 / 4	2	admitAll	<input checked="" type="checkbox"/>
1 / 5	1	admitAll	<input checked="" type="checkbox"/>
1 / 6	1	admitAll	<input type="checkbox"/>

admitOnlyVlanTag

Set Reload Help

Figure 76: Assigning and saving "Port VLAN ID", "Acceptable Frame Types" and "Ingress Filtering"

- 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.
- To temporarily save the configuration, click "Set".
- Open the Basic Settings > External Memory dialog.
- To save the configuration permanently in the external memory, activate the "Auto-save config on envm" checkbox and click "Set".

```
enable
configure
interface 1/1
```

```
vlan participation include 1
vlan participation include 2
vlan tagging 2 enable
```

Switch to the privileged EXEC mode.

Switch to the Configuration mode.

Switch to the Interface Configuration mode of interface 1/1.

Port 1/1 becomes member untagged in VLAN 1.

Port 1/1 becomes member untagged in VLAN 2.

Port 1/1 becomes member tagged in VLAN 2.

```

vlan participation include 3 Port 1/1 becomes member untagged in VLAN 3.
vlan tagging 3 enable      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
                             interface 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 id 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)
VLAN Routing.....disabled

Interface   Current   Configured   Tagging
-----
1/1         Include   Include      Tagged
1/2         -         Autodetect   Untagged
1/3         Include   Include      Untagged
1/4         -         Autodetect   Untagged
1/5         Include   Include      Untagged

```

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

7.2 Guest / Unauthenticated VLAN

The guest VLAN function allows a device to provide port-based Network Access Control (IEEE 802.1x) to non-802.1x capable supplicants. This feature provides a mechanism to allow guests to access external networks exclusively. When you connect non-802.1x capable supplicants to an active unauthorized 802.1x port, the supplicants send no responses to 802.1x requests. Since the supplicants send no responses, the port remains in the unauthorized state, and the supplicants have no access to external networks.

The guest VLAN supplicant function is a per-port basis configuration. When you configure a port as a guest VLAN and connect non-802.1x capable supplicants to this port, the device assigns the supplicants to the guest VLAN. Adding supplicants to a guest VLAN causes the port to change to the authorized state allowing the supplicants to access to external networks.

The Unauthenticated VLAN function allows the device to provide service to 802.1x capable supplicants which authenticate incorrectly. This function allows the unauthorized supplicants to have access to limited services. When you configure an unauthenticated VLAN on a port with 802.1x port authentication and the global operation enabled, the device places the port in an unauthenticated VLAN. When a 802.1x capable supplicant incorrectly authenticates on the port, the device adds the supplicant to the unauthenticated VLAN. If you also configure a guest VLAN on the port, then non-802.1x capable supplicants use the guest VLAN.

The reauthentication timer counts down when the port has an unauthenticated VLAN assigned. The unauthenticated VLAN reauthenticates when the "Reauthentication Period" expires and supplicants are present on the port. If no supplicants are present, the device places the port in the configured guest VLAN.

The following example explains how to create a Guest VLAN. Create an Unauthorized VLAN in the same manner.

- Open the `Switching > VLAN > Configuration` dialog.
- To add a new VLAN to the table, click "Create".
- The "Create" window opens. In the "VLAN ID" text box, enter 10.
- To close the "Create" window and add the new VLAN to the table, click "OK".

- Edit the name of the new VLAN by double clicking on the "Name" cell of the new entry and entering `Guest`.
- To add a new VLAN to the table, click "Create".
- The "Create" window opens. In the "VLAN ID" text box, enter `20`.
- To close the "Create" window and add the new VLAN to the table, click "OK".
- Edit the name of the new VLAN by double clicking on the "Name" cell of the new entry and entering `Unauth`.
- Open the `Network Security > 802.1X Port Authentication > Global` dialog.
- Activate the 802.1x global function in the "Operation" frame, by clicking `On`.
- Open the `Network Security > 802.1X Port Authentication > Port Configuration` dialog.
- In the port 1/4 "Port Control" cell, select `auto`.
- In the port 1/4 "Guest VLAN ID" cell, enter `10`.
- In the port 1/4 "Unauthenticated VLAN ID" cell, enter `20`.
- To temporarily save the configuration, click "Set".
- Open the `Basic Settings > External Memory` dialog.
- To save the configuration permanently in the external memory, activate the "Auto-save config on envm" checkbox and click "Set".

```

enable
vlan database
vlan add 10
vlan add 20
name 10 Guest
name 20 Unauth
exit
configure
dot1x system-auth-control
enable
dot1x port-control auto
interface 1/4

dot1x guest-vlan 10
dot1x unauthenticated-
vlan 20
exit

```

Switch to the privileged EXEC mode.

Switch to the VLAN mode.

Create VLAN 10.

Create VLAN 20.

Rename VLAN 10 to Guest.

Rename VLAN 20 to Unauth.

Switch to the privileged EXEC mode.

Switch to the Configuration mode.

Enable the 802.1X function globally.

Enable port control on port 1/4.

Switch to the Interface Configuration mode of interface 1/4.

Assign the guest vlan to port 1/4.

Assign the unauthorized vlan to port 1/4.

Switch to the Configuration mode.

7.3 RADIUS VLAN assignment

The RADIUS VLAN assignment feature allows for a RADIUS VLAN ID attribute to be associated with an authenticated client. When a client authenticates successfully, and the RADIUS server sends a VLAN attribute, the device associates the client with the RADIUS assigned VLAN. As a result, the device adds the physical port as an untagged member to the appropriate VLAN and sets the port VLAN ID (PVID) with the given value.

7.4 VLAN unaware mode

The VLAN-unaware function defines the operation of the device in a LAN segmented by VLANs. The device accepts packets and frames and processes them according to its inbound rules. Based on the IEEE 802.1Q specifications, the function governs how the device processes VLAN tagged frames or packets.

Use the VLAN aware mode to apply the user-defined VLAN topology configured by the network administrator. The device uses VLAN tagging in combination with the IP or Ethernet address when forwarding packets or frames. The device processes inbound and outbound frames or packets according to the defined rules. VLAN configuration is a manual process.

Use the VLAN unaware mode to forward traffic as received, without any modification. For example, the device transmits tagged packets when received as tagged and transmits untagged packets when received as untagged. Regardless of VLAN assignment mechanisms, the device assigns packets to VLAN ID 1 and to a multicast group, indicating that the packet flood domain is according to the VLAN.

8 Operation Diagnosis

The device provides you with the following diagnostic tools:

- ▶ Sending Traps
- ▶ Monitoring the device status
- ▶ Out-of-band signaling via signal contact
- ▶ Port status indication
- ▶ Event counter at port level
- ▶ Detecting non-matching duplex modes
- ▶ SFP status display
- ▶ Topology Discovery
- ▶ Detecting IP address conflicts
- ▶ Detecting loops
- ▶ Reports
- ▶ Monitoring data traffic on a port (port mirroring)
- ▶ Syslog
- ▶ Event log
- ▶ Cause and Action management during Selftest

8.1 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.

8.1.1 List of SNMP traps

The following table shows a short list of possible traps 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, after successful initialisation of the network management.
linkDown	This is sent if the connection to a port is interrupted.
linkUp	This is sent when connection is established to a port.
newRoot	This is sent if the sending agent becomes the new root of the spanning tree.
topologyChange	This is sent when the port changes from blocking to forwarding or from forwarding to blocking.
alarmRisingThreshold	This is sent if the RMON input exceeds its upper threshold.
alarmFallingThreshold	This is sent if the RMON input goes below its lower threshold.
hm2AgentPortSecurity Violation	This is sent if an MAC address detected on this port does not correspond to the current settings for – hm2AgentPortSecurityEntry.
hm2DiagSelftestAction Trap	This trap is sent if a selftest action is performed as configured for the four categories task, resource, software, and hardware.
hm2MrpReconfig	This is sent if the configuration of the MRP Ring changes.
hm2DiagIfaceUtilization Trap	This is sent if the interface threshold exceeds the configured upper or lower limits.
hm2LogAuditStartNext Sector	This is sent when the audittrail has filled one sector and starts a new one.
hm2PtpSynchronization Change	This is sent if Ptp synchronization status is changed.
hm2ConfigurationSaved Trap	This is sent after the device has successfully saved its configuration locally.
hm2ConfigurationChanged Trap	This is sent if you change the configuration of the device after saving locally for the first time.
hm2PlatformStpInstance LoopInconsistentStartTrap	This is sent if this port in this STP instance enters loop inconsistent state.
hm2PlatformStpInstance LoopInconsistentEndTrap	This is sent if this port in this STP instance exits loop inconsistent state upon reception of a BPDU.

Table 18: Possible traps

8.1.2 Traps for configuration activity

After you save a configuration in memory, the device sends a `hm2ConfigurationSavedTrap`. This trap contains both the Non-Volatile Memory (NVM) and External Non-Volatile Memory (ENVM) state variables indicating whether the running configuration is in sync with the NVM, and with the ENVM. You also trigger this trap by copying a config file to the device replacing the active saved configuration.

Furthermore, the device sends a `hm2ConfigurationChangedTrap`, whenever you change the local configuration, indicating a mismatch between the running and saved configuration.

8.1.3 Configuring Traps

- Open the `Diagnostics > Status Configuration > Alarms (Traps)` dialog.

This dialog allows you to determine which events trigger a trap and where the device sends these messages.

- Click "Create".
- In the "Name" column you enter the name that the device uses to identify itself as the source of the trap.
- In the "Address" frame, enter the IP address of the management station to which the device sends traps.
- In the "Active" column you select the entries that the device should take into account when the device sends traps.

The device generates traps for changes selected in the dialogs `Diagnostics > Status Configuration > Device Status` and `Diagnostics > Status Configuration > Security Status`. Create at least 1 SNMP Manager that receives traps.

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

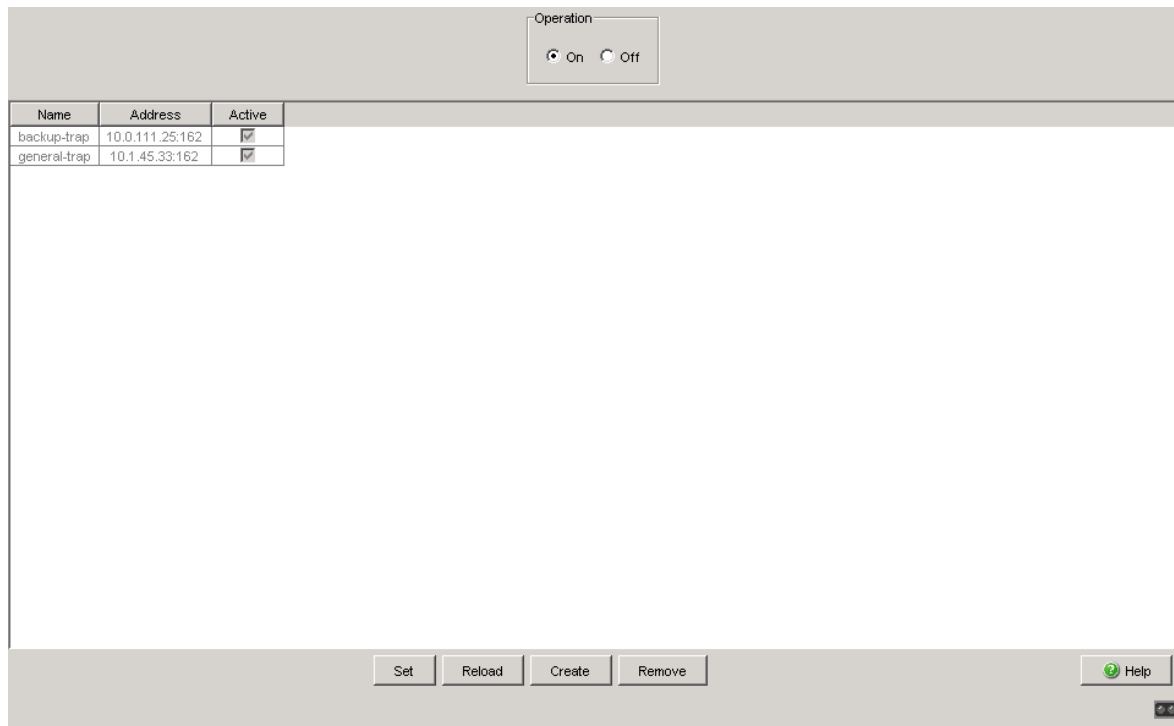


Figure 77: Alarms dialog

8.1.4 ICMP Messaging

The device allows you to use the Internet Control Message Protocol (ICMP) for diagnostic applications, for example ping and trace route. The device also uses ICMP for time-to-live and discarding messages in which the device forwards an ICMP message back to the packet source device.

Use the ping network tool to test the path to a particular host across an IP network. The traceroute diagnostic tool displays paths and transit delays of packets across a network. The CLI handbook contains a description of the ping and traceroute tools.

8.2 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 by sending a trap when the device status changes
- ▶ detect the device status in the `Basic Settings > System` dialog of the graphical user interface
- ▶ query the device status in the Command Line Interface

The "Global" tab of the `Diagnostics > Status Configuration > Device Status` dialog allows you to configure the device to send a trap to the management station for the following events:

- ▶ Loss of the redundancy (in ring manager mode)
- ▶ The interruption of link connection(s). Configure at least one port for this feature. In the "Port" tab of the `Diagnostics > Status Configuration > Device Status` dialog in the "Propagate Connection Error" row, you specify which ports the device signals if the link is down.

Select the corresponding entries to decide which events the device status includes.

8.2.1 Events which can be monitored

Name	Meaning
Ring redundancy	Enable this function to monitor if ring redundancy is present.
Connection error	Enable this function to monitor every port link event in which the "Propagate Connection Error" checkbox is active.

Table 19: "Device Status" events

8.2.2 Configuring the Device Status

- Open the "Global" tab of the `Diagnostics > Status Configuration > Device Status` dialog.
- In the "Monitor" column, you select the events to monitor.
- To send a trap to the management station, activate the "Generate Trap" function in the "Trap Configuration" frame.
- Configure at least one SNMP-Manager in the `Diagnostics > Status Configuration > Alarms (Traps)` dialog.

<code>enable</code>	Switch to the privileged EXEC mode.
<code>configure</code>	Switch to the Configuration mode.
<code>device-status trap</code>	Enable a trap to be sent if the device status changes.
<code>device-status monitor ring-redundancy</code>	Sets the monitoring of the ring-redundancy

In order to enable the device to monitor an active link without a connection, first enable the global function, then enable the individual ports.

- Open the "Global" tab of the `Diagnostics > Status Configuration > Device Status` dialog.
- In the "Monitor" column, you select the "Connection error" function.
- Open the "Port" tab of the `Diagnostics > Status Configuration > Device Status` dialog.
- In the "Propagate Connection Error" row, you select the ports to monitor.

<code>enable</code>	Switch to the privileged EXEC mode.
<code>configure</code>	Switch to the Configuration mode.
<code>device-status monitor link-failure</code>	Sets the monitoring of the network connection
<code>interface 1/1</code>	Select interface 1 port 1.
<code>device-status link-alarm</code>	Sets the monitoring of a active link without a connection for this port.

Note: The above CLI commands activate monitoring and trapping for the supported components. If you want to activate or deactivate monitoring 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 ? for the CLI prompt.)

8.2.3 Displaying the Device Status

□ Open the Basic Settings > System dialog.

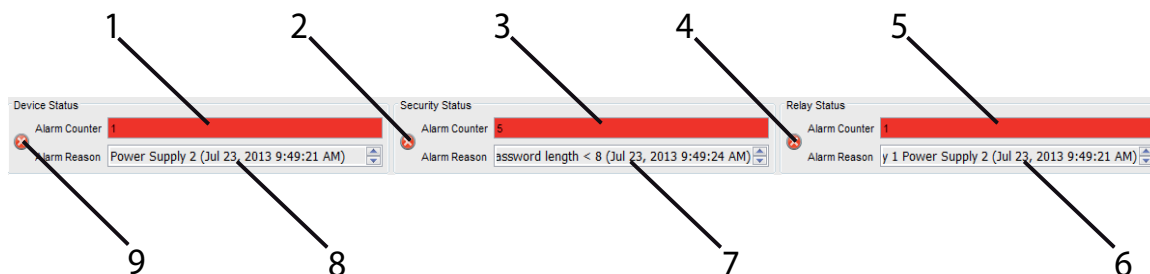


Figure 78: Device, security and relay status/alarm display

- 1 - Number of existing device alarms
- 2 - The symbol displays the security status
- 3 - Number of existing security alarms
- 4 - The symbol displays the relay status
- 5 - Number of existing relay alarms
- 6 - Cause and Start of existing relay alarms
- 7 - Cause and Start of existing security alarms
- 8 - Cause and Start of existing device alarms
- 9 - The symbol displays the device status

```
show device-status all
```

In the EXEC Privilege mode, display the device status and the setting for the device status determination.

8.3 Security Status (DEVMON)

The Security Status provides an overview of the overall security of the device. Many processes aid in system visualization by recording the security status of the device and then presenting its condition in graphic form. The device displays the overall security status in the `Basic Settings > System` dialog, "Security Status" frame.

In the "Global" tab of the `Diagnostics > Status Configuration > Security Status` dialog the device displays its current status as "Error" or "Ok" in the "Security Status" frame. The device determines this status from the individual monitoring results.

The device enables you to configure the following functions:

- ▶ signal the device security status by sending a trap when the device status changes
- ▶ detect the device security status in the `Basic Settings > System` dialog of the graphical user interface
- ▶ query the security status in the Command Line Interface

8.3.1 Events which can be monitored

Select the events which the device includes in the security status alert by activating the parameter in the "Monitor" column.

Name	Meaning
Password default settings unchanged	After installation change the passwords to increase security. The device monitors if the default passwords remain unchanged.
Minimum Password Length < 8	Create passwords more than 8 characters long to maintain a high security posture. When active the device monitors the "Minimum Password Length" setting.
Password Policy settings deactivated	The device monitors the settings located in the <code>Device Security > User Management</code> dialog for password policy requirements.
User account password Policy Check deactivated	The device monitors the settings of the "Policy Check" checkbox. When "Policy Check" is inactive the device sends a trap.
Telnet server active	The device monitors when you enable the Telnet function.
HTTP server active	The device monitors when you enable the HTTP connection function.
SNMP unencrypted	The device monitors when you enable the SNMPv1 or v2 connection function.
Access to System Monitor with V.24 possible	The device monitors the System Monitor status.
Link interrupted on enabled device ports	The device monitors the link status of active ports.
Write access using HiDiscovery possible	The device monitors when you enable the HiDiscovery read/write access function.
IEC61850-MMS active	The device monitors the IEC 61850-MMS protocol activation setting.

Table 20: "Security Status" events

8.3.2 Configuring the Security Status

- Open the "Global" tab of the `Diagnostics > Status Configuration > Security Status` dialog.
- In the "Monitor" column, you select the events to monitor.
- To send a trap to the management station, activate the "Generate Trap" function in the "Trap Configuration" frame.
- Configure at least one SNMP-Manager in the `Diagnostics > Status Configuration > Alarms (Traps)` dialog.

`enable`

`configure`

`security-status monitor
pwd-change`

`security-status monitor
pwd-min-length`

`security-status monitor
pwd-policy-config`

`security-status monitor
pwd-policy-inactive`

`security-status monitor
telnet-enabled`

`security-status monitor
http-enabled`

`security-status monitor
snmp-unsecure`

`security-status monitor
sysmon-enabled`

`security-status monitor
iec61850-mms-enabled`

`security-status trap`

Switch to the privileged EXEC mode.

Switch to the Configuration mode.

Sets the monitoring of default password change for 'user' and 'Admin'.

Sets the monitoring of minimum length of the password (smaller 8) .

To monitor the password policy configuration. The device changes the security status to the value `error` if the value for at least one of the following password policies is 0: "minimum upper cases", "minimum lower cases", "minimum numbers", "minimum special characters".

Sets the monitoring whether at least one user is configured with inactive policy check. The device changes the security status to the value `error` if the function "policy check" is inactive for at least one user account.

Sets the monitoring of the activation of telnet on the switch.

Sets the monitoring of the activation of http on the switch.

To monitor SNMP security. (When enabling SNMPv1/v2, or disabling v3 encryption).

To monitor the activation of System Monitor 1 on the device.

To monitor the activation of the IEC 61850-MMS protocol.

Enable the device to send a trap if the device status changes.

In order to enable the device to monitor an active link without a connection, first enable the global function then, enable the individual ports.

- Open the "Global" tab of the `Diagnostics > Status Configuration > Security Status` dialog.
- In the "Monitor" column, activate the "Link interrupted on enabled device ports" function.
- Open the "Port" tab of the `Diagnostics > Status Configuration > Device Status` dialog.
- In the "Link interrupted on enabled device ports" row, you select the ports to monitor.

```
enable
configure
security-status monitor
no-link-enabled
interface 1/1
security-status
no-link
```

Switch to the privileged EXEC mode.

Switch to the Configuration mode.

Sets the monitoring of no link detection.

Select interface 1 port 1.

Sets the monitoring of no link detection status of interface 1 port 1.

8.3.3 Displaying the Security Status

- Open the Basic Settings > System dialog.

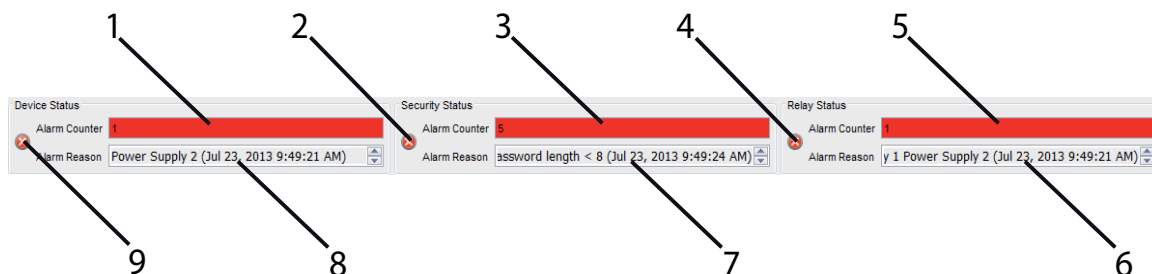


Figure 79: Device, security and relay status/alarm display

- 1 - Number of existing device alarms
- 2 - The symbol displays the security status
- 3 - Number of existing security alarms
- 4 - The symbol displays the relay status
- 5 - Number of existing relay alarms
- 6 - Cause and Start of existing relay alarms
- 7 - Cause and Start of existing security alarms
- 8 - Cause and Start of existing device alarms
- 9 - The symbol displays the device status

```
show security-status all
```

In the EXEC Privilege mode, display the security status and the setting for the security status determination.

8.4 Port Event Counter

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 `Basic Settings > Restart` dialog, you can reset the event counters to zero using "Cold start..." or "Reset port counters".

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

The event counters may be observed by selecting the `Diagnostics:Ports:Statistics Table` dialog.

Counter	Indication of known possible weakness
Received fragments	<ul style="list-style-type: none"> – Non-functioning controller of the connected device – Electromagnetic interference in the transmission medium
CRC error	<ul style="list-style-type: none"> – Non-functioning controller of the connected device – Electromagnetic interference in the transmission medium – Inoperable component in the network
Collisions	<ul style="list-style-type: none"> – Non-functioning controller of the connected device – Network over extended/lines too long – Collision or a detected fault with a data packet

Table 21: Examples indicating known weaknesses

- To reset the counters, click in the `Basic Settings > Restart` dialog "Reset port counters".
- To monitor the current status of the event counters, open the `Basic Settings > Port` dialog, "Statistics" tab, and click the "Reload" button.

8.4.1 Detecting Non-matching Duplex Modes

Problems occur when 2 ports directly connected to each other have mismatching duplex modes. These problems are difficult to track down. The automatic detection and reporting of this situation has the benefit of recognizing mismatching duplex modes before problems occur.

This situation arises from an incorrect configuration, for example, if you deactivate the automatic configuration on 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	

Table 22: 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
3	On	Half duplex	Late collisions	Duplex problem detected	Duplex problem, EMI, network extension
4	On	Half duplex	CRC error	OK	EMI
5	On	Full duplex	None	OK	
6	On	Full duplex	Collisions	OK	EMI
7	On	Full duplex	Late collisions	OK	EMI
8	On	Full duplex	CRC error	OK	EMI
9	Off	Half duplex	None	OK	
10	Off	Half duplex	Collisions	OK	
11	Off	Half duplex	Late collisions	Duplex problem detected	Duplex problem, EMI, network extension
12	Off	Half duplex	CRC error	OK	EMI
13	Off	Full duplex	None	OK	
14	Off	Full duplex	Collisions	OK	EMI
15	Off	Full duplex	Late collisions	OK	EMI
16	Off	Full duplex	CRC error	Duplex problem detected	Duplex problem, EMI


Table 22: Evaluation of non-matching of the duplex mode (cont.)

8.5 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
- ▶ serial number of media module
- ▶ temperature in ° C
- ▶ transmission power in mW
- ▶ receive power in mW

Open the Diagnostics > Ports > SFP dialog.

Port	Module type	Serial Number	Supported	Temperature in °Celsius	Tx Power in mW	Rx Power in mW	Tx Power in dBm	Rx Power in dBm	Rx Power State
1.1	M-FAST SFP-SM E	UB7016Q	<input checked="" type="checkbox"/>	42	0.0637	0.1979	-11.9	-7.0	
1.2	M-FAST SFP-MM	3635793	<input checked="" type="checkbox"/>	unsupported	unsupported	unsupported	N/A	N/A	

Reload Help

Figure 80: SFP Modules dialog

8.6 Topology Discovery

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 neighboring devices on the shared LAN. Evaluation of the devices occur when the receiving device has its LLDP function active.
- ▶ receive connection and management information from neighbor devices on the shared LAN, provided these adjacent devices also have LLDP active.
- ▶ build a management information database 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: 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.

- ▶ 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
- ▶ 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 queries this information from devices that have LLDP active. This information allows the network management station to form a description of the network topology.

Non-LLDP devices normally block the special multicast LLDP IEEE MAC address used for information exchange. Non-LLDP devices therefore discard LLDP packets. When positioning a non-LLDP capable device between 2 LLDP capable devices, the non-LLDP capable device prohibits information exchanges between the 2 LLDP capable devices.

The Management Information Base (MIB) for a device with LLDP capability holds the LLDP information in the LLDP-MIB and in the private HM2-LLDP-EXT-HM-MIB and HM2-LLDP-MIB.

8.6.1 Displaying the Topology Discovery Results

To show the topology of the network:

- Open the `Diagnostics > LLDP > Topology Discovery` dialog, "LLDP" tab.

If you use a port to connect several devices, for example via a hub, the table contains a line for each connected device.

Activating "Display FDB Entries" at the bottom of the table allows you to display devices without active LLDP support in the table. In this case, the device also includes information from its FDB (forwarding database).

If you connect the port to devices with the topology discovery function active, then the devices exchange LLDP Data Units (LLDPDU) and the topology table displays these neighboring devices.

When a port connects devices without an active topology discovery exclusively, the table contains a line for this port to represent the connected devices. This line contains the number of connected devices.

The FDB address table contains MAC addresses of devices that the topology table hides for the sake of clarity.

8.7 Detecting Loops

Loops in the network, even temporary loops, cause connection interruptions or data losses. The automatic detection and reporting of this situation allows you to detect it faster and diagnose it more easily.

An incorrect configuration causes loops, 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 trigger the device to send a report.

BPDUs sent from the designated port and received on either a different port of the same device or the same port within a short time, is a typical effect of a loop.

8.8 Reports

The following lists reports and buttons available for diagnostics:

- ▶ **System Log file**
The log file is an HTML file in which the device writes every important device-internal event.
- ▶ **Audit Trail**
Logs successful CLI commands and user comments. The file also includes SNMP logging.
- ▶ **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.

8.8.1 Global Settings

Using this dialog you enable or disable where the device sends reports. For example, to a Console, a Syslog Server, or a CLI connection. You also set at which severity level the device writes events into the reports.

- Open the `Diagnostics > Report > Global` dialog.
- To send a report to the console configure the desired level in the "Console Logging" frame "Severity" text box using the pull down menu.
- To enable the operation, click `On`.

The device buffers logged events in 2 separate storage areas so that the device keeps log entries for urgent events. Define the minimum severity for events that the device logs to the buffered storage area with a higher priority.

- To send events to the buffer, configure the desired level in the "Buffered Logging" frame "Severity" text box using the pull down menu.

When you activate the logging of SNMP requests, the device logs the requests as events in the syslog. The "Log SNMP Get Request" function logs user requests for device configuration information. The "Log SNMP Set Request" function logs device configuration events. Define the minimum level for events that the device logs in the syslog.

- Select the "Log SNMP Get Request" checkbox if you want to send reading SNMP requests to the device as events to the syslog server.
- Select the "Log SNMP Set Request" checkbox if you want to send writing SNMP requests to the device as events to the syslog server.
- Choose the desired severity level for the get and set requests.

When active, the device logs configuration changes made using the CLI commands, to the audit trail. This feature is based on the IEEE 1686 standard for Substation Intelligent Electronic Devices.

- Open the `Diagnostics > Report > Global` dialog.
- To activate the function, in the "CLI Logging" frame, click `On`.

The "Download JAR-File" button allows you to save a Java Applet of the graphical user interface (GUI) on your PC as a JAR file. This applet allows you the option of administering the device, instead of using a web browser.

The device creates the file name of the applet automatically in the format <device type><software version>_<software revision of applet>.jar.

- Click "Download JAR-File".
- Select the directory in which you want to save the applet.
- Click "Save".

The "Download Support Information" button allows you to save the following system information data in one ZIP file on your PC:

- ▶ System log (systemlog.html)
- ▶ System information (systeminfo.html)
- ▶ Audit trail (audittrail.html)
- ▶ Support information (supportinfo.html)
- ▶ Running configuration (runningconfig.xml)
- ▶ Default configuration (defaultconfig.xml)

The device creates the file name of the support information automatically in the format <IP address>_<system name>.zip.

- Click "Download Support Information".
- Select the directory in which you want to save the support information.
- Click on "Save".

8.8.2 Syslog

The device enables you to send messages about important device internal events to one or more syslog servers (up to 8). Additionally, you also include SNMP requests to the device as events in the syslog.

Note: To display the logged events, open the dialog `Diagnostics > Report > Audit Trail` or `Diagnostics > Report > System Log`.

- Open the `Diagnostics > Syslog` dialog.
- Activate the syslog function in the "Operation" frame.
- Click on "Create".
- Enter the IP address of the syslog server, in the "IP Address" column.
- Enter the UDP port on which the syslog server receives log entries, in the "Port" column.
- Enter the minimum seriousness level an event must attain for the device to send a log entry to this syslog server in the "Minimum Severity" column.
- To enable the syslog server entry to which the device sends the logs, select the "Active" control box.

Configure the following settings for read and write SNMP requests in the "SNMP Logging" frame:

- Open the `Diagnostics > Report > Global` dialog.
- Select the "Log SNMP Get Request" checkbox if you want to send reading SNMP requests to the device as events to the syslog server.
- Select the "Log SNMP Set Request" checkbox if you want to send writing SNMP requests to the device as events to the syslog server.
- Choose the desired severity level for the get and set requests.

```

enable
configure
logging host add 1 addr
    10.0.1.159 severity 3

logging syslog operation
exit
show logging host

```

No.	Server IP	Port	Max. Severity	Type	Status
1	10.0.1.159	514	error	systemlog	active

```

configure
logging snmp-requests get
    operation
logging snmp-requests get
    severity 5

logging snmp-requests set
    operation
logging snmp-requests set
    severity 5

exit
show logging snmp
Log SNMP GET requests      : enabled
Log SNMP GET severity      : notice
Log SNMP SET requests      : enabled
Log SNMP SET severity      : notice

```

Switch to the privileged EXEC mode.

Switch to the Configuration mode.

Add a new recipient of the log messages . The “3” indicates the seriousness of the message sent by the device. “3” means “error”.

Enable the Syslog function.

Switch to the privileged EXEC mode.

Display the syslog host settings.

Switch to the Configuration mode.

Create log events from reading SNMP requests.

The “5” indicates the seriousness of the message that the device allocates to messages from reading SNMP requests. “5” means “note”.

Create log events from writing SNMP requests.

The “5” indicates the seriousness of the message that the device allocates to messages from writing SNMP requests. “5” means “notice”.

Switch to the privileged EXEC mode.

Display the SNMP logging settings.

8.8.3 System Log

The device allows you to call up a log file of the system events. The table in the `Diagnostics > Report > System Log` dialog lists the logged events.

- To update the content of the log, click “Reload”.
- To search the content of the log for a key word, click “Search”.
- To archive the content of the log as an html file, click “Save”.

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

8.8.4 Audit Trail

The `Diagnostics > Report > Audit Trail` dialog contains system information and changes to the device configuration performed through CLI and SNMP. In the case of device configuration changes, the dialog displays Who changed What and When. To log changes to the device configuration, use in the `Diagnostics > Report > Audit Trail` dialog the functions "Log SNMP Get Request" and "Log SNMP Set Request".

The `Diagnostics > Syslog` dialog allows you to configure up to 8 Syslog servers to which the device sends Audit Trails.

The following list contains log events:

- ▶ changes to configuration parameters
- ▶ CLI commands except show commands
- ▶ automatic changes to the System Time
- ▶ watchdog events
- ▶ locking a user after several unsuccessful login attempts
- ▶ special CLI command 'logging audit-trail <string>' which logs the comment
- ▶ user login, either locally or remote, via CLI
- ▶ manual, user-initiated, logout
- ▶ timed logout after a user-defined period of CLI inactivity
- ▶ file transfer operation including a Firmware Update
- ▶ configuration changes via HiDiscovery
- ▶ automatic configuration or firmware updates via the external memory
- ▶ blocked management access due to invalid login
- ▶ rebooting
- ▶ opening and closing SNMP over HTTPS tunnels
- ▶ detected power failures

8.9 Network Analysis with TCPDump

Tcpdump is a packet-sniffing UNIX utility used by network administrators to sniff and analyze traffic on a network. A couple of reasons for sniffing traffic on a network is to verify connectivity between hosts, or to analyze the traffic traversing the network.

Tcpdump on the device provides the possibility to decode or capture packets received and transmitted by the Management CPU. This function is available using the `debug` CLI command. Refer to the CLI Handbook for further information about the Tcpdump function.

8.10 Monitoring Data Traffic on the Ports (Port Mirroring)

The port mirroring function enables you to copy the data traffic from several ports to a single port of the device for diagnostic purposes.

The ports from which the device copies data are source ports. The port to which the device copies the data are destination port. the device uses physical ports as source or destination ports.

In port mirroring, the device copies valid incoming **and** outgoing data packets of the source port to the destination port. The feature has no affect on the data traffic copied from the source ports during port mirroring.

A management tool connected on the destination port, for example, an RMON probe, monitors the data traffic on the source ports in the sending and receiving directions.

- Select the `Diagnostics > Ports > Port Mirroring` dialog.

This dialog allows you to configure and activate the port mirroring function of the device. The device displays unavailable ports as inactive. For example, the port currently in use as the destination port, or if you have already selected the maximum number of ports.

- Select the source ports whose data traffic you want to review from the list of physical ports by checkmarking the relevant boxes.
- Select the destination port to which you have connected your management tool from the drop-down list in the "Destination Port" frame.

The device displays the ports that are available in the drop-down list. The device omits ports currently used as source ports.

- To enable the function, activate `On` in the "Operation" frame.

The “Reset configuration” button in the dialog allows you to reset the port mirroring settings of the device to the delivery state.

Note: When port mirroring is active, the device uses the specified destination port solely for reviewing data, in this state the port blocks normal data traffic.

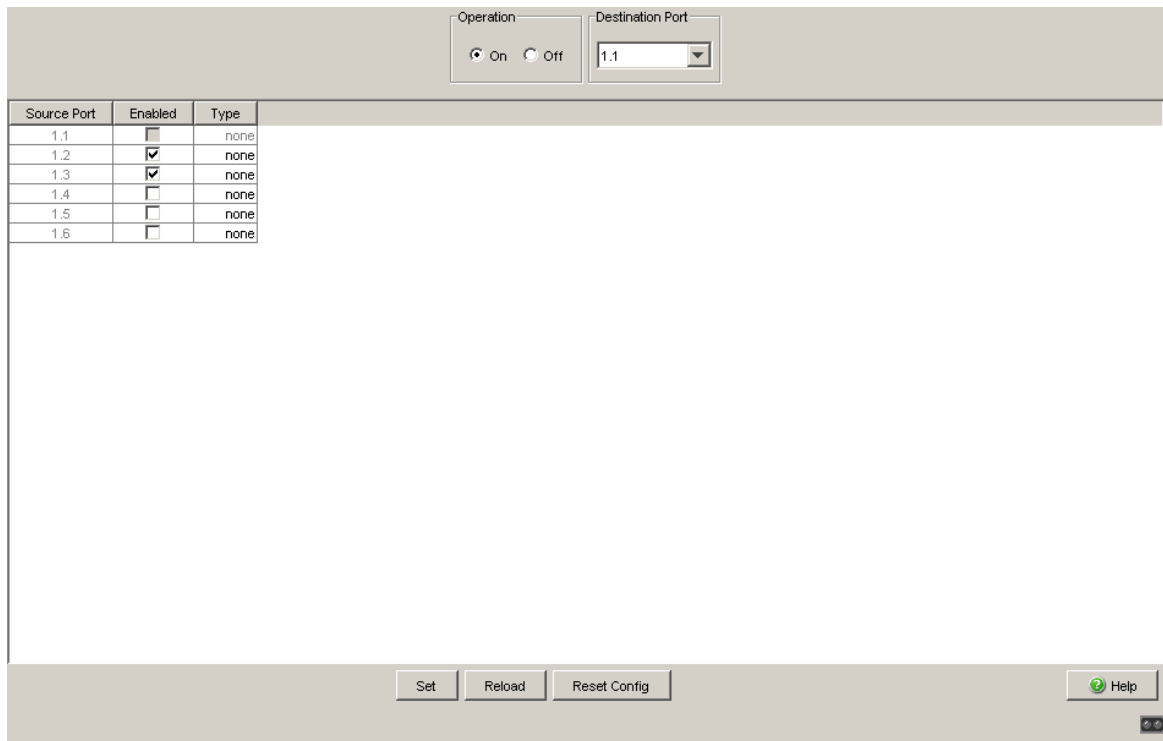


Figure 81: Port Mirroring dialog

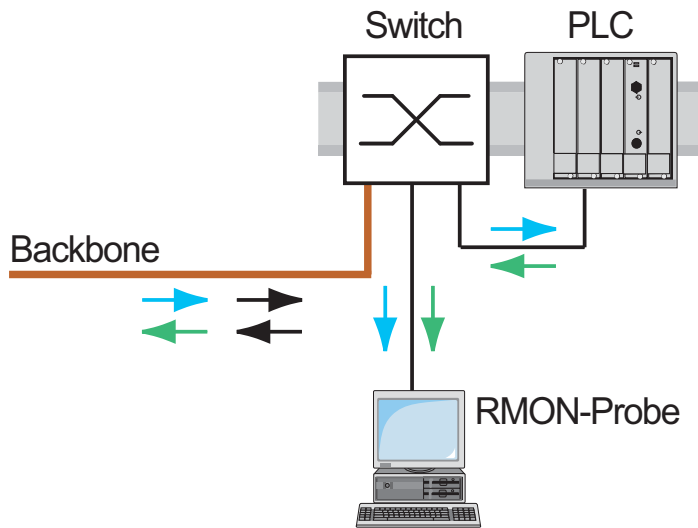


Figure 82: Port mirroring

8.11 Cause and Action management during Selftest

The device checks its assets during the boot process and occasionally thereafter. The device checks system task availability or termination and the available amount of memory. Furthermore, the device checks for application functionality and if there is any hardware degradation in the chip set.

When the device detects a loss in integrity, the device responds to the degradation with a user-defined action. The following categories are available for configuration.

- ▶ "Task" - action to be taken when a task is unsuccessful.
- ▶ "Resources" - action to be taken due to the lack of resources.
- ▶ "Software" - action taken for loss of software integrity. For example, code segment checksum or access violations.
- ▶ "Hardware" - action taken due to hardware degradation

Configure each category to produce an action when the device detects a loss in integrity. The following actions are available for configuration.

- ▶ `log only` - this action writes a message to the logging file.
- ▶ `send trap` - a trap will be sent to the management station.
- ▶ `reboot` - an error in the category, when activated, will cause the device to reboot

- Open the `Diagnostics > System > Selftest` dialog.
- Select the action to perform for a cause, in the "Action" column.

```
enable
configure
selftest action task log-
only
selftest action resource
send-trap
selftest action software
send-trap
selftest action hardware
reboot
```

Switch to the privileged EXEC mode.

Switch to the Configuration mode.

To send a message to the event log when a task is unsuccessful.

To send a flag to the management station when there is a lack of resources.

To send a flag to the management station when there is a loss of software integrity.

To reboot the device when hardware degradation occurs.

Disabling these functions lets you decrease the time required to restart the device after a cold start. You find these options in the `Diagnostics > System > Selftest` dialog, "Configuration" frame.

- ▶ "RAM Test" - to enable or disable the ramtest function during a cold start.
- ▶ "Activate SysMon1" - to enable or disable the System Monitor function during a cold start.
- ▶ "Reload default config on error" - to enable or disable the reloading of the standard device configuration if no readable configuration is available during a restart.

Note: Device access is in jeopardy when you disable the System Monitor 1, for example, misplacement or misconfiguration of the administrator password.

```
selftest ramtest
no selftest ramtest
selftest system-monitor
no selftest system-monitor
show selftest action

show selftest settings
```

Enable RAM selftest on cold start.
Switch off the "ramtest" function.
Enable the "SysMon1" function.
Switch off the "SysMon1" function.
Show status of the actions to be taken in the event of device degradation.
Show ramtest and sysmon settings in event of a cold start.

8.12 Copper Cable Test

Use this feature to test copper cables attached to an interface for a short or open circuit. The test interrupts traffic flow, when in progress, on this port.

The table displays the state and lengths of each individual pair. The device returns a result with the following meaning:

- ▶ normal - indicates that the cable is operating properly
- ▶ open - indicates an interruption in the cable
- ▶ short circuit - indicates a short circuit in the cable
- ▶ untested - indicates an untested cable
- ▶ Unknown - cable unplugged

9 Advanced functions of the device

9.1 Auto Disable

If the configuration displays a port as enabled, but the device detects an error or change in the condition, the software shuts down that port. In other words, the device software disables the port because of a detected error or change in the 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 reduces the possibility that this port causes the network to be instable.

Auto disable is available for the following functions:

- ▶ Link Flap
- ▶ CRC Error
- ▶ Duplex Mismatch
- ▶ BPDU Rate
- ▶ Port MAC Lock

In the following example, you allow the device to enable ports disabled due to conditions defined in the "CRC/Fragments" tab of the `Diagnostics > Ports > Port Monitor` dialog.

- Open the `Diagnostics > Ports > Auto Disable` dialog.
- Activate the "CRC Error" checkbox in the "Configuration" frame.
- Specify the delay time as 120 s in the "Reset Timer [s]" column for the ports you want to enable.
- Activate the ports you want to enable automatically.

Note: The "Reset" button allows you to enable the port before the "Reset Timer [s]" counts down.

```
enable
configure
auto-disable reason crc-
error
interface 1/1

auto-disable timer 120

auto-disable operation

auto-disable reset
```

Switch to the privileged EXEC mode.

Switch to the Configuration mode.

Activate the auto-disable CRC function.

Switch to the Interface Configuration mode of interface 1/1.

Specifies the elapse reset timer as 120 s for this port.

Activate the auto-disable function settings for this port.

Allows you to enable the port before the "Reset Timer [s]" counts down.

9.2 MRP-IEEE

The IEEE 802.1ak amendment to the IEEE 802.1Q standard introduced the Multiple Registration Protocol (MRP) to replace the Generic Attribute Registration Protocol (GARP). The IEEE also modified and replaced the GARP applications, GARP Multicast Registration Protocol (GMRP) and GARP VLAN Registration Protocol (GVRP), with the Multiple MAC Registration Protocol (MMRP) and the Multiple VLAN Registration Protocol (MVRP).

To confine traffic to the required areas of a network, the MRP applications distribute attribute values to MRP enabled devices across a LAN. The MRP applications register and de-register multicast group memberships and VLAN identifiers.

Note: The Multiple Registration Protocol (MRP) requires a loop free network. To help prevent loops in your network, use a network protocol such as the Media Redundancy Protocol, Spanning Tree Protocol, or Rapid Spanning Tree Protocol with MRP.

9.2.1 MRP Operation

Each participant contains an applicant component and an MRP Attribute Declaration (MAD) component. The applicant component is responsible for forming the attribute values and their registration and de-registration. The MAD component generates MRP messages for transmission and processes messages received from other participants. The MAD component encodes and transmits the attributes to other participants in MRP Data Units (MRPDU). In the switch, an MRP Attribute Propagation (MAP) component distributes the attributes to participating ports.

A participant exists for each MRP application and each LAN port. For example, a participant application exists on an end device and another application exists on a switch port. The Applicant state machine records the attribute and port for each MRP participant declaration on an end device or switch. Applicant state machine variable changes trigger the transmission of MRPDUs to communicate the declaration or withdrawal.

To establish an MMRP instance, an end device first sends a Join empty (JoinMt) message with the appropriate attributes. The switch then floods the JoinMt to the participating ports and to the neighboring switches. The neighboring switches flood the message to their participating port, and so on, establishing a path for the group traffic.

■ MRP Timers

The default timer settings help prevent unnecessary attribute declarations and withdraws. The timer settings allow the participants to receive and process MRP messages before the Leave or LeaveAll timers expire.

Maintain the following relationships when you reconfigure the timers:

- ▶ To allow for re-registration after a Leave or LeaveAll event, even if there is a lost message, set the LeaveTime to:
 $\geq (2x \text{JoinTime}) + 60$, in 1/100 s.
- ▶ To minimize the volume of rejoining traffic generated following a LeaveAll, set the value chosen for the LeaveAll timer larger than the LeaveTime.

The following list contains various MRP events that the device transmits:

- ▶ Join - Controls the interval for the next Join message transmission
- ▶ Leave - Controls the length of time that a switch waits in the Leave state before changing to the withdraw state
- ▶ LeaveAll - Controls the frequency with which the switch generates LeaveAll messages

The Periodic timer, when expired, initiates a Join request MRP message that the switch sends to participants on the LAN. The switches use this message to prevent unnecessary withdraws.

9.2.2 MMRP

When a device receives broadcast, multicast or unknown traffic on a port, the device floods the traffic to the other ports. This process causes unnecessary use of bandwidth on the LAN.

The Multiple MAC Registration Protocol (MMRP) allows you to control the traffic flooding by distributing an attribute declaration to participants on a LAN. The attribute values that the MAD component encodes and transmits on the LAN in MRP messages are Group service requirement information and 48-bit MAC addresses.

The switch stores the attributes in a filtering database as MAC address registration entries. The forwarding process uses the filtering database entries solely to transmit dat through those ports necessary to reach Group member LANs.

Switches facilitate the group distribution mechanisms based on the Open Host Group concept, receiving frames on the active ports and forward exclusively on ports with group members. This way, any MMRP participants requiring frames transmitted to a particular group or groups, requests membership in the group. MAC service users send frames to a particular group from anywhere on the LAN. A group receives these frames on the LANs attached to registered MMRP participants. MMRP and the MAC Address Registration Entries thus restrict the frames to required segments of a loop-free LAN.

In order to maintain the registration and deregistration state and to receive traffic, a port declares interest periodically. Every MMRP enabled device on a LAN maintains a filtering database and forwards traffic having the group MAC addresses to listed participants.

■ MMRP Example

In this example, Host A intends to listen to traffic destined to group G1. Switch A processes the MMRP Join request received from Host A and sends the request to both of the neighboring switches. The devices on the LAN now recognize that there is a host interested in receiving traffic destined for group G1. When Host B starts transmitting data destined for group G1, the data flows on the path of registrations and Host A receives it.

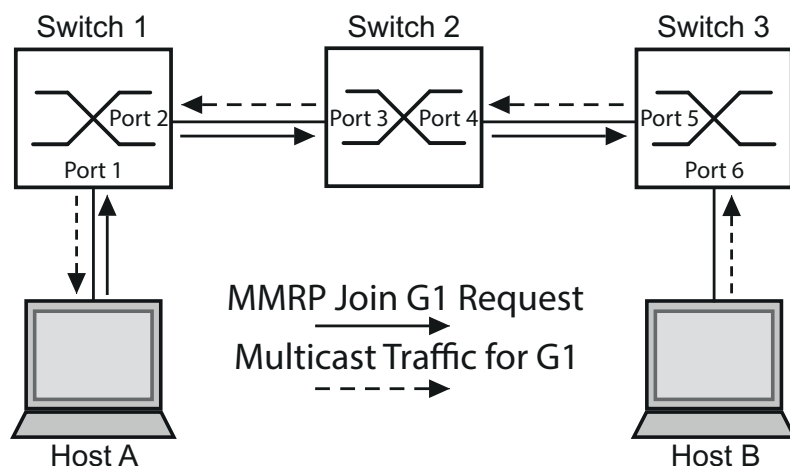


Figure 83: MMRP Network for MAC address Registration

To enable MMRP on the switches, proceed as follows:

- Open the `Switching > MRP-IEEE > MMRP` dialog, "Configuration" tab.
- To activate ports 1 and 2 as MMRP participants, mark "Active" for ports 1 and 2 on switch 1.
- To activate ports 3 and 4 as MMRP participants, mark "Active" for ports 3 and 4 on switch 2.
- To activate ports 5 and 6 as MMRP participants, mark "Active" for ports 5 and 6 on switch 3.
- To send periodic events allowing the switch to maintain the registration of the MAC address group, enable the "Periodic State Machine". In the "Configuration" frame, click "On".
- To enable the MMRP function globally, in the "Operation" frame, click "On".

To enable the MMRP ports on switch 1, use the following CLI commands. Substituting the appropriate interfaces in the CLI commands, enable the MMRP functions and ports on switches 2 and 3.

<code>enable</code>	Switch to the privileged EXEC mode.
<code>configure</code>	Switch to the Configuration mode.
<code>interface 1/1</code>	Switch to the Interface Configuration mode of interface 1/1.
<code>mrp-ieee mmrp operation</code>	Enable MMRP on the port.
<code>interface 1/2</code>	Switch to the interface configuration mode for interface 1/2.
<code>mrp-ieee mmrp operation</code>	Enable MMRP on the port.
<code>exit</code>	Switch to the Configuration mode.

<code>mrp-ieee mrp periodic-state-machine</code>	Enable the MMRP periodic state machine globally.
<code>mrp-ieee mmrp operation</code>	Enable MMRP globally.

9.2.3 MVRP

The Multiple VLAN Registration Protocol (MVRP) is an MRP application that provides dynamic VLAN registration and withdraw services on a LAN.

MVRP provides a maintenance mechanism for the Dynamic VLAN Registration Entries, and for transmitting the information to other switches. This information allows MVRP-aware devices to establish and update their VLAN membership information. When members are present on a VLAN, the information indicates through which ports the switch forwards traffic to reach those members.

The main purpose of MVRP is to allow switches to discover some of the VLAN information that you otherwise manually set up. Discovering this information allows switches to overcome the limitations of bandwidth consumption and convergence time in large VLAN networks.

■ MVRP Example

Set up a network comprised of MVRP aware switches (1 - 4) connected in a ring topology with end device groups, A1, A2, B1, and B2 in 2 different VLANs, A and B. With STP enabled on the switches, the ports connecting switch 1 to switch 4 are in the discarding state, preventing a loop condition.

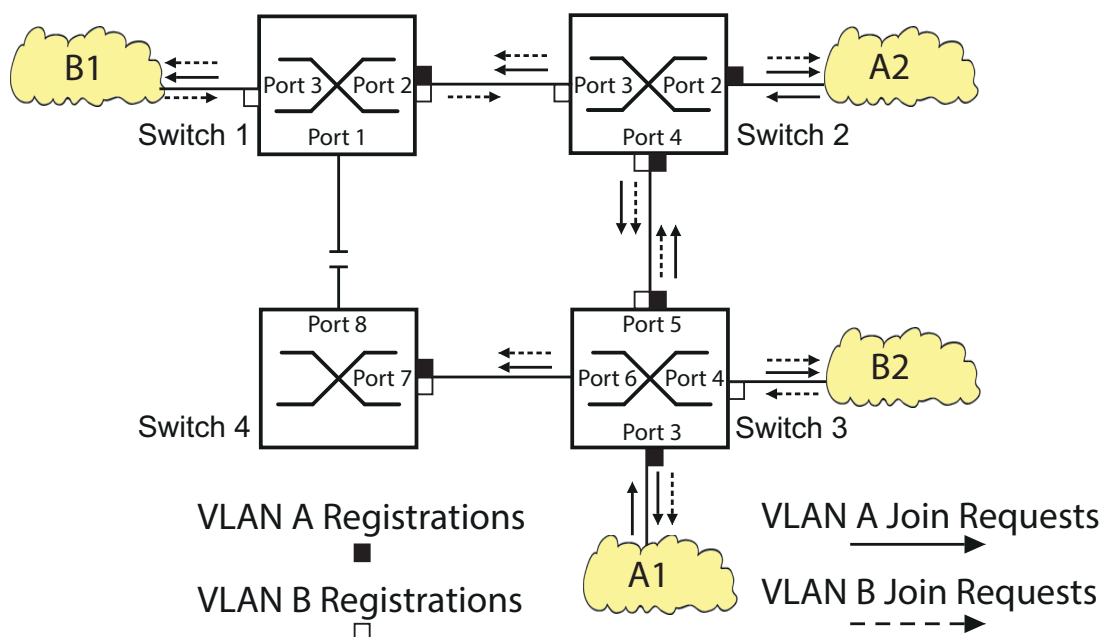


Figure 84: MVRP Example Network for VLAN Registration

In the MVRP example network, the LANs first send a Join request to the switches. The switch enters the VLAN registration in the forwarding database for the port receiving the frames. The switch then propagates the request to the other ports, and sends the request to the neighboring LANs and switches. This process continues until the switches have registered the VLANs in the forwarding database of the receive port.

To enable MVRP on the switches, use the following work steps.

- Open the `Switching > MRP-IEEE > MVRP` dialog, "Configuration" tab.
- To activate ports 1 through 3 as MVRP participants, mark "Active" for ports 1 through 3 on switch 1.
- To activate ports 2 through 4 as MVRP participants, mark "Active" for ports 2 through 4 on switch 2.
- To activate ports 3 through 6 as MVRP participants, mark "Active" for ports 3 through 6 on switch 3.
- To activate ports 7 and 8 as MVRP participants, mark "Active" for ports 7 and 8 on switch 4.
- To maintain the registration of the VLANs, in the "Configuration" frame enable the "Periodic State Machine", mark the "On" radio button.
- To enable the function MVRP globally, in the "Operation" frame, mark the "On" radio button.

To enable the MVRP ports on switch 1, use the following CLI commands. Substituting the appropriate interfaces in the CLI commands, enable the MVRP functions and ports on switches 2, 3 and 4.

<code>enable</code>	Switch to the privileged EXEC mode.
<code>configure</code>	Switch to the Configuration mode.
<code>interface 1/1</code>	Switch to the Interface Configuration mode of interface 1/1.
<code>mrp-ieee mvrp operation</code>	Enable MVRP on the port.
<code>interface 1/2</code>	Switch to the interface configuration mode for interface 1/2.
<code>mrp-ieee mvrp operation</code>	Enable MVRP on the port.
<code>exit</code>	Switch to the Configuration mode.
<code>mrp-ieee mvrp periodic-state-machine</code>	Enables the periodic state machine on this device.
<code>mrp-ieee mvrp operation</code>	Enables MMRP on this device.

9.3 CLI Client

The device supports an CLI client that directly opens a connection to the SSH server using the TCP Port configured in the "SSH" tab of the `Device Security > Management Access > Server` dialog. The CLI client allows you to configure the device using CLI commands.

A prerequisite to using the CLI client is that you activate the SSH-server function in the "SSH" tab of the `Device Security > Management Access > Server` dialog.

For detailed information on CLI commands, review the "Command Line Interface" reference manual.

9.4 IEC 61850/MMS

IEC 61850/MMS is an industrial communication protocol standardized by the International Electrotechnical Commission (IEC). You use the protocol in substation automation, for example, in the control technology of energy suppliers.

This packet-oriented protocol is based on the TCP/IP transport protocol and uses the Manufacturing Messaging Specification (MMS) for the client-server communication. The IEC 61850 defines a standardized object-oriented configuration language that comprises, among other things, functions for SCADA and the Intelligent Electronic Devices (IED). The standard also defines how the devices use the MMS protocol to transmit data between the IEDs.

Part 6 of the IEC 61850 standard defines the Substation Configuration Language (SCL). SCL data allows the devices of a substation to exchange SCL files and to have a complete interoperability between the devices. You store the properties of the device, described with SCL, in an ICD file on the device.

9.4.1 Switch model for IEC 61850

The Technical Report, IEC 61850 90-4, specifies a bridge model. The bridge model represents the functions of a switch as objects of an Intelligent Electronic Device (IED). An MMS client, for example, the control room software, uses these objects to monitor and configure the device.

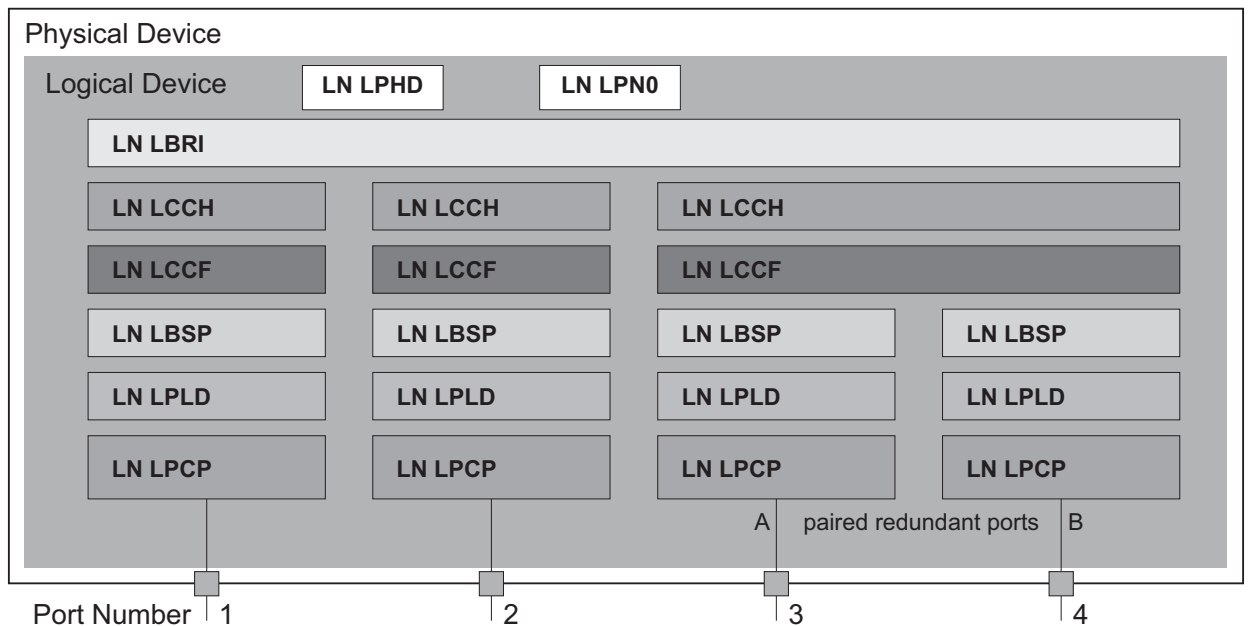


Figure 85: Bridge model based on Technical Report IEC 61850 90-4

Class	Description
LN LLNO	“Zero” logical node of the “Bridge” IED: Defines the logical properties of the device.
LN LPHD	“Physical Device” logical node of the “Bridge” IED: Defines the physical properties of the device.
LN LBRI	“Bridge” logical node: Represents general settings of the bridge functions of the device.
LN LCCH	“Communication Channel” logical node: Defines the logical “Communication Channel” that consists of one or more physical device ports.
LN LCCF	“Channel Communication Filtering” logical node: Defines the VLAN and Multicast settings for the higher-level “Communication Channel”.

Table 23: Classes of the bridge model based on TR IEC61850 90-4

Class	Description
LN LBSP	“Port Spanning Tree Protocol” logical node: Defines the Spanning Tree statuses and settings for the respective physical device port.
LN LPLD	“Port Layer Discovery” logical node: Defines the LLDP statuses and settings for the respective physical device port.
LN LPCP	“Physical Communication Port” logical node: Represents the respective physical device port.

Table 23: Classes of the bridge model based on TR IEC61850 90-4 (cont.)

9.4.2 Integration into a Control System

NOTE

RISK OF UNAUTHORIZED ACCESS TO THE DEVICE

IEC61850/MMS does not provide any authentication mechanisms. If the write access for IEC61850/MMS is activated, every client that can access the device using TCP/IP is capable of changing the settings of the device. This in turn can result in an incorrect configuration of the device and to failures in the network.

Only activate the write access if you have taken additional measures (e.g. Firewall, VPN, etc.) to eliminate the risk of unauthorized access.

Failure to follow these instructions can result in equipment damage.

Use the following steps after installation, connecting and configuring the Switch:

- Check that the device has an IP address assigned.
- To start the MMS server, activate the function in the graphical user interface, in the `Advanced > Industrial Protocols > IEC61850-MMS` dialog.

When you finish these steps, an MMS client is able to connect to the device and to read and monitor the objects defined in the switch.

- To configure the objects specified in the switch, mark the "Write Access" checkbox enabling the MMS client.

9.4.3 Offline configuration

The device allows you to download the ICD file using the graphical user interface. This file contains the properties of the device described with SCL and enables you to configure the substation without directly connecting to the device.

- You download the ICD file by clicking the "Download ICD File" button in the `Advanced > Industrial Protocols > IEC61850-MMS` dialog.

9.4.4 Monitoring the device

The IEC61850/MMS server integrated into the device allows you to monitor multiple statuses of the device with the Report Control Block (RCB). The device allows up to 5 MMS clients to register for an RCB at the same time.

The device allows you to monitor the following statuses:

Class	RCB object	Description
LN LPHD	PwrSupAlm	Changes when 1 of the redundant power supplies fails or starts operating again.
	TmpAlm	Changes when the temperature measured in the device exceeds or falls below the set temperature thresholds.
	PhyHealth	Changes when the status of the "LPHD.PwrSupAlm" or "LPHD.TmpAlm" RCB object changes.
LN LBRI	Health	Changes when the status of the "LPHD.PwrSupAlm" or "LPHD.TmpAlm" RCB object changes.
	RstpRoot	Changes when the device takes over or relinquishes the role of the root bridge.
	RstpTopoCnt	Changes when the topology changes due to a root bridge change.
LN LCCH	ChLiv	Changes when the link status of the physical port changes.
LN LPCP	PhyHealth	Changes when the link status of the physical port changes.

Table 24: Statuses of the device that can be monitored with IEC 61850/MMS

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.

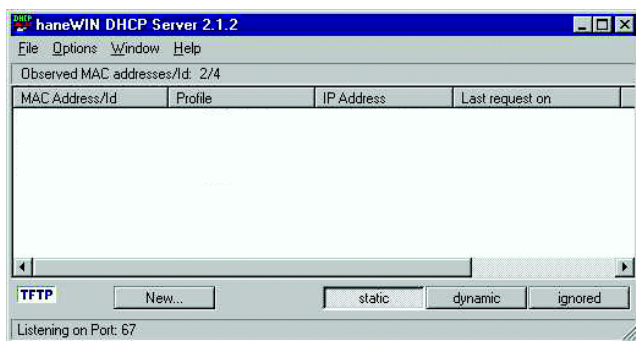


Figure 86: Start window of the DHCP server

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`.

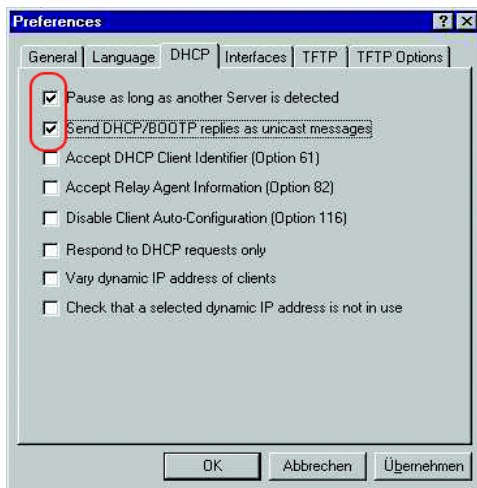


Figure 87: DHCP setting

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

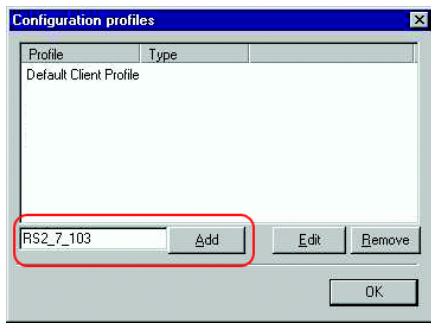


Figure 88: Adding configuration profiles

- Enter the netmask and click `Apply`.

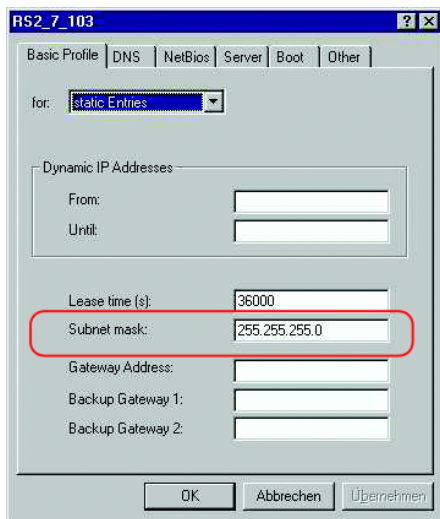


Figure 89: Netmask in the configuration profile

- 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`.

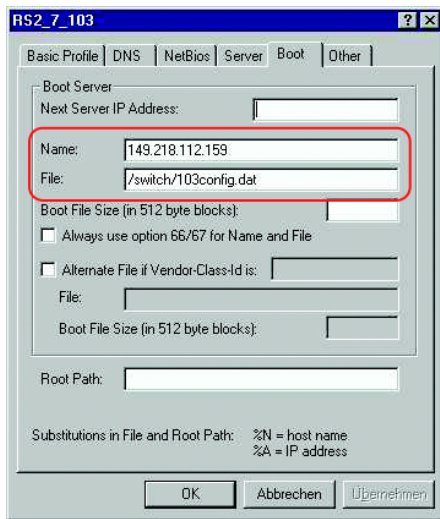


Figure 90: Configuration file on the tftp server

- 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`.

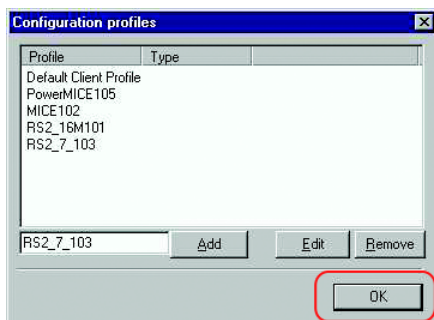


Figure 91: Managing configuration profiles

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

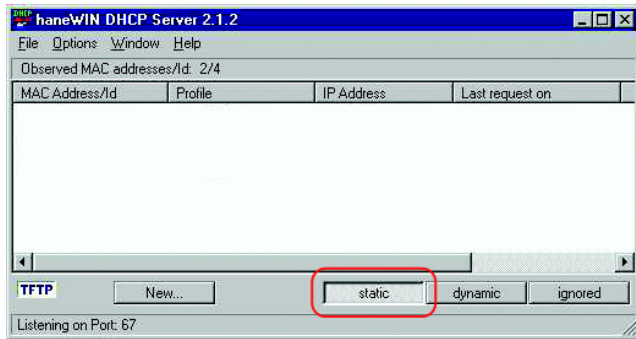


Figure 92: Static address input

- Click New.

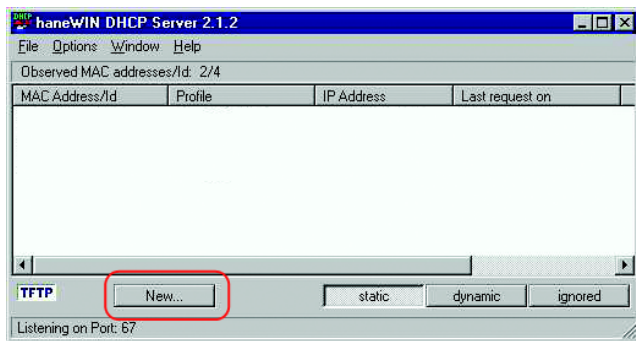


Figure 93: Adding static addresses

- 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.

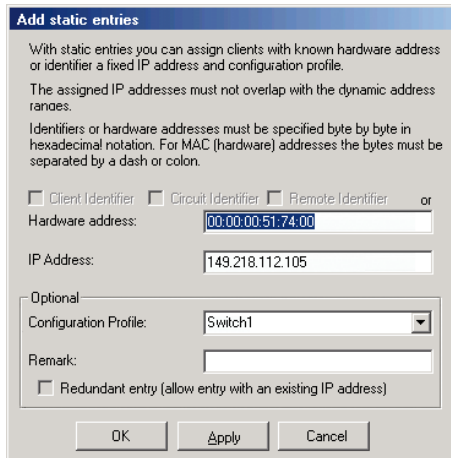


Figure 94: Entries for static addresses

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

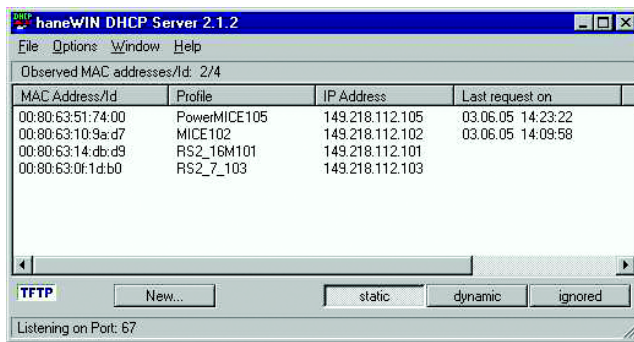


Figure 95: DHCP server with entries

A.2 Changing the MAC Address

The device allows you to change the burned in MAC Address to a user defined MAC Address. The user defined MAC address is:

- ▶ Configurable by CLI and GUI.
- ▶ Stored in the internal boot parameter block.
- ▶ Retrieved during the boot phase.

The user defined MAC Address is configured using either the Web Interface or the CLI.

- Open the `Basic Settings > Network` dialog, "MAC configuration" tab.
- Enter in the "Configuration" frame, "Local Admin MAC Address" field the user-defined MAC address.
- The device applies the change upon restart.

<code>enable</code>	Switch to the privileged EXEC mode.
<code>configure</code>	Switch to the Configuration mode.
<code>network management mac</code>	Configure the locally administered MAC address.
<code><local-addr></code>	
<code>show network management mac</code>	Display the MAC address settings of the device.

Note: Changes to the MAC address require you to reboot the device before the new address is assigned.

A.3 Define the Management port

You can configure the device to restrict management access to one port or allow management access on every port. The user defined Management port is configured using either the Web Interface or the CLI.

- Open the `Basic Settings > Network` dialog, "MAC configuration" tab.
- To restrict the access to certain users, enter the port used for the management in the "Configuration" frame, "Management Port" field.

`network management port`

`<1/1...1/6>`

`show network management port`

Configuring the port for the management access.

The value zero allows the access from any port.

Show the network management port.

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

`hm2PSSstate` (OID = 1.3.6.1.4.1.248.11.11.1.1.1.1.2)

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 1.3.6.1.4.1.248.11.11.1.1.1.1.2.1`" returns the response "1", which means that the power supply is ready for operation.

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. 1.3.6.1.4.1.248...)
Octet string	ASCII character string
PSID	Power supply identifier (number of the power supply unit)

Definition of the syntax terms used:

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.

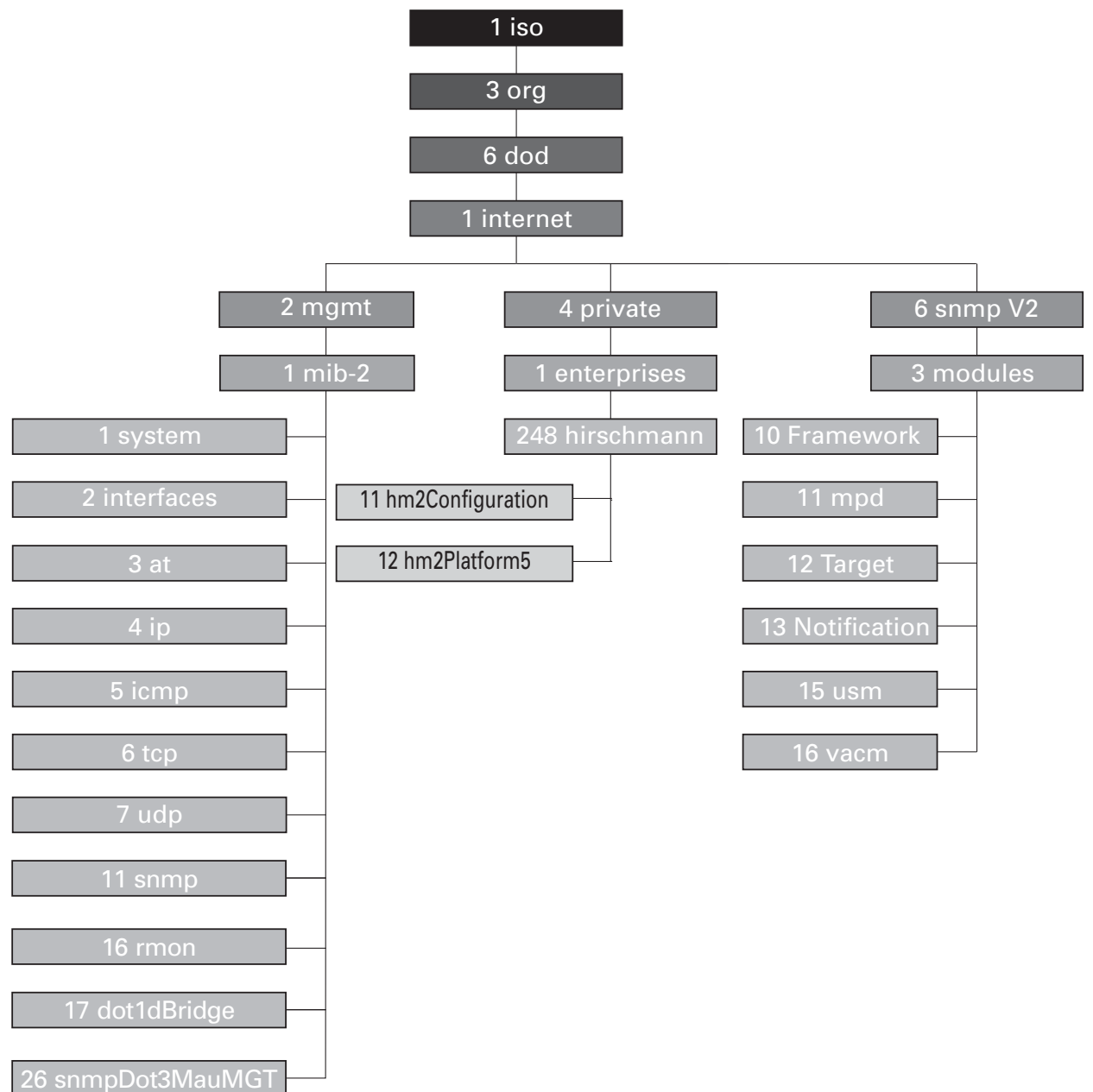


Figure 96: Tree structure of the Hirschmann MIB

A description of the MIB can be found on the product CD provided with the device.

B.2 Abbreviations used

ACA31	AutoConfiguration Adapter
ACL	Access Control List
BOOTP	Bootstrap Protocol
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
FDB	Forwarding Database
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
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
MIB	Management Information Base
MRP	Media Redundancy Protocol
MSTP	Multiple Spanning Tree Protocol
NMS	Network Management System
NTP	Network Time Protocol
PC	Personal Computer
PTP	Precision Time Protocol
QoS	Quality of Service
RFC	Request For Comment
RM	Redundancy Manager
RSTP	Rapid Spanning Tree Protocol
SCP	Secure Copy
SFP	Small Form-factor Pluggable
SFTP	SSH File Transfer Protocol
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 Maintenance

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

B.5 Readers' Comments

What is your opinion of this manual? We are constantly striving to provide as comprehensive a description of our product as possible, as well as important information to assist you in the operation of this product. Your comments and suggestions help us to further improve the quality of our documentation.

Your assessment of this manual:

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

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

Suggestions for improvement and additional information:

General comments:

Sender:

Company / Department:

Name / Telephone number:

Street:

Zip code / City:

E-mail:

Date / Signature:

Dear User,

Please fill out and return this page

- ▶ as a fax to the number +49 (0)7127/14-1600 or
- ▶ per mail to

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

C Index

A			
Access roles	75	HiDiscovery	51
Aging time	154	HiView	11, 18
Alarm	209	Host address	42
Alarm messages	206	I	
APNIC	41	IANA	41
ARIN	41	IEC 61850	258
ARP	46	IEEE MAC Address	227
B		IGMP snooping	153, 154
Bandwidth	181	Industrial HiVision	12, 57
Best Master Clock algorithm	134	Instantiation	276
BOOTP	39	IP Address	41, 49, 56
Boundary clock (PTP)	132	IP header	165, 170
C		IRIG-B	138
CD-ROM	266	ISO/OSI layer model	46
CIDR	47	L	
Classless Inter-Domain Routing	47	LACNIC	41
Command Line Interface	20	Leave message	154
Configuration changes	206	Link monitoring	212
Configuration file	56	Login window	19
D		M	
Daylight saving time	122	MAC address filter	144
Delay measurement (PTP)	135	MAC destination address	46
Delay (PTP)	135	Memory (RAM)	97
Device Status	212	Message	206
DHCP	39	MMS	258
DHCP server	121, 126, 266	Multicast	154
DiffServ	165	N	
DSCP	165, 178	Netmask	43, 50
E		Network Management	57
Event log file	235	Non-volatile memory (NVM)	97
F		NVM (non-volatile memory)	97
FAQ	287	O	
First installation	39	Object classes	276
Flow control	181	Object description	276
G		Object ID	276
Gateway	43, 50	OpenSSH Suite	30
Generic object classes	276	Ordinary clock (PTP)	133
Grandmaster (PTP)	134	P	
H		Password	26, 30, 33
HaneWin	266	Polling	206
Hardware reset	206	Port Mirroring	238
		Port Priority	177
		PPS	138

Index

PPS (Pulse per Second)	138	Trap target table	206
Priority	169	Type of Service	170
Priority tagged frames	169		
PTP	117	U	
PTP domain	136	Update	36
PuTTY	21	User name	26, 30, 33
Q		V	
QoS	167	Video	171
Query	154	VLAN	185
Queue	171	VLAN priority	176
R		VLAN tag	169, 185
RAM (memory)	97	VoIP	171
Real time	164	VT100	32
Redundancy	11	V.24	20, 32
Reference time source	120, 126, 134	W	
Report	230	Weighted Fair Queuing	171
Report message	154	Weighted Round Robin	171
RIPE NCC	41		
RMON probe	238		
Router	43		
S			
Secure Shell	22, 27		
Secure Shell	20		
Segmentation	206		
Service	230		
Service Shell Reactivation	116		
Setting the time	120		
SFP module	225		
SNMP	18, 206		
SNMPv1/v2	90		
SNTP	117		
SSH	20, 22, 27		
Starting the graphical user interface (GUI)	18		
Store-and-forward	144		
Strict Priority	171		
Subidentifier	276		
Subnet	50		
Symbol	13		
System requirements (GUI)	18		
T			
Target table	206		
Technical Questions	287		
Time signal (IRIG-B/PPS)	138		
ToS	165, 170		
Traffic class	171, 177		
Traffic Shaping	178		
Training Courses	287		
Transmission reliability	206		
Transparent clock (PTP)	133		
Trap	206, 209		

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