HIRSCHMANN

A BELDEN BRAND

User Manual

Basic Configuration
Rail Switch Power Enhanced (HiOS-2S/2A/3S RSPE)

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

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

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

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

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

Rel. 4.0 - 07/2014 – 22.07.2014

Contents

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

The 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:

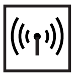
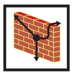
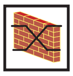
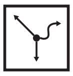
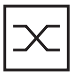
- ActiveX control for SCADA integration
- Auto-topology discovery
- Browser interface
- Client/server structure
- Event handling
- Event log
- Simultaneous configuration of multiple devices
- Graphical user interface with network layout
- SNMP/OPC gateway

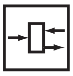
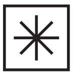
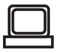
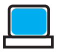
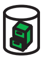
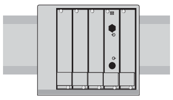
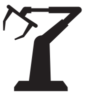
Key

The designations used in this manual have the following meanings:

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

Symbols used:

	WLAN access point
	Router with firewall
	Switch with firewall
	Router
	Switch

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

Introduction

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

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

1 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.

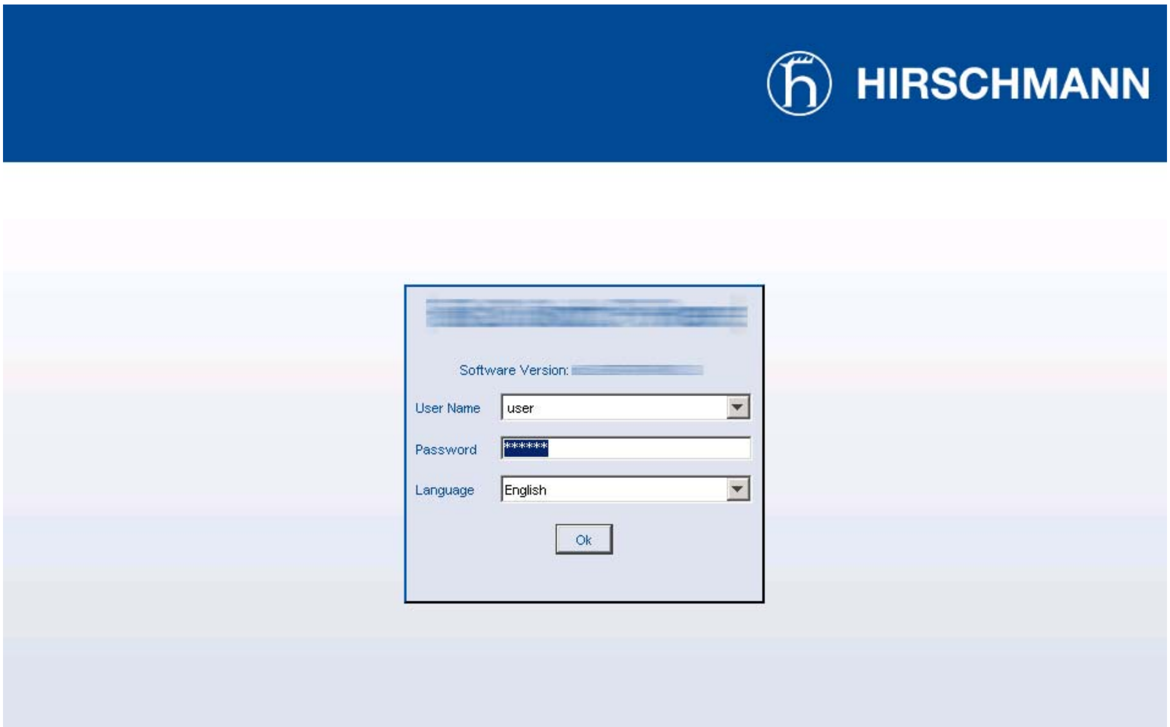
Start the graphical user interface in the Web browser:

– 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.



Software Version:

User Name: user

Password: ******

Language: English

Figure 1: Login window

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

The Web browser displays the graphical user interface.

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 Rail Switch Power Enhanced 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-2S/2A/3S RSPE device can be found in the “Installation” user manual.

You will find information for configuring your HiOS-2S/2A/3S RSPE 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.

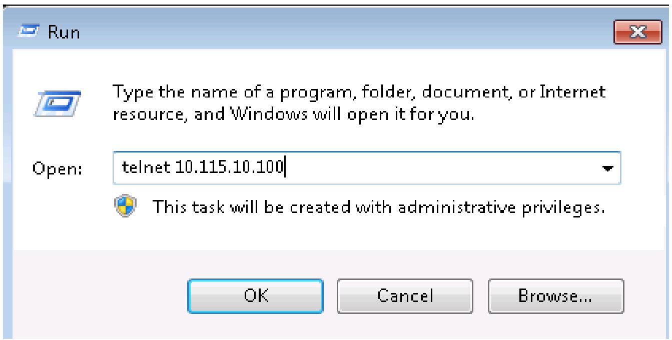
1.2.2 CLI access via telnet

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.



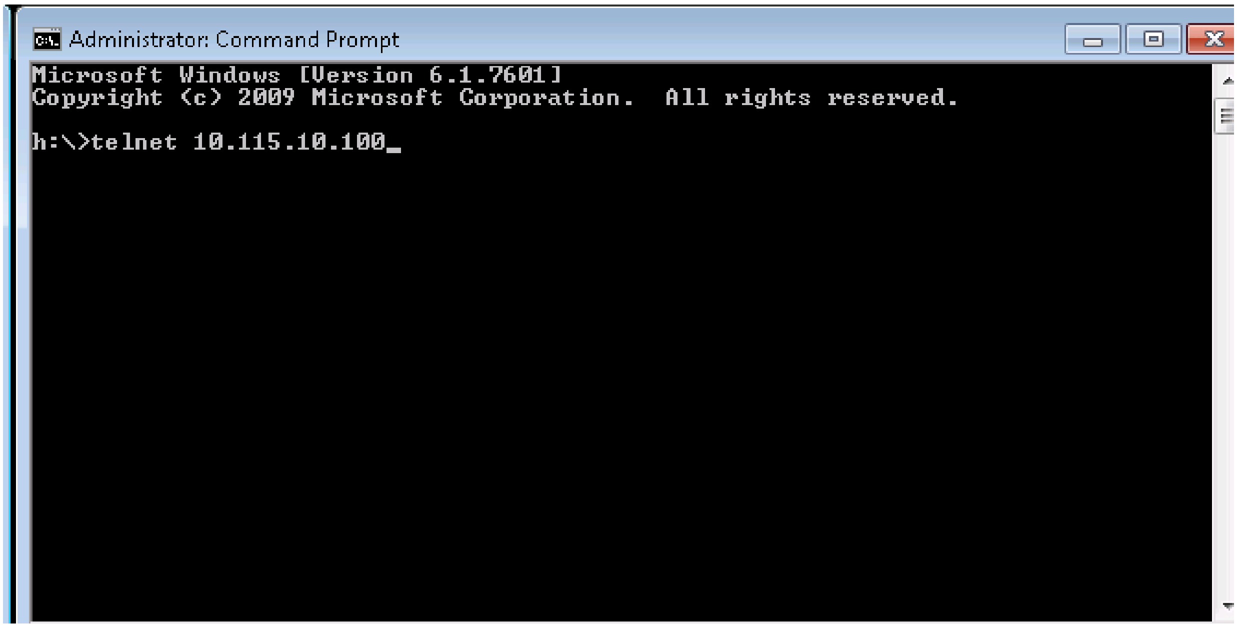
Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
This task will be created with administrative privileges.
OK
Cancel
Browse...

telnet 10.115.10.100

Figure 2: Setting up the telnet connection to the HiOS-2S/2A/3S RSPE 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>`.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

h:\>telnet 10.115.10.100_
```

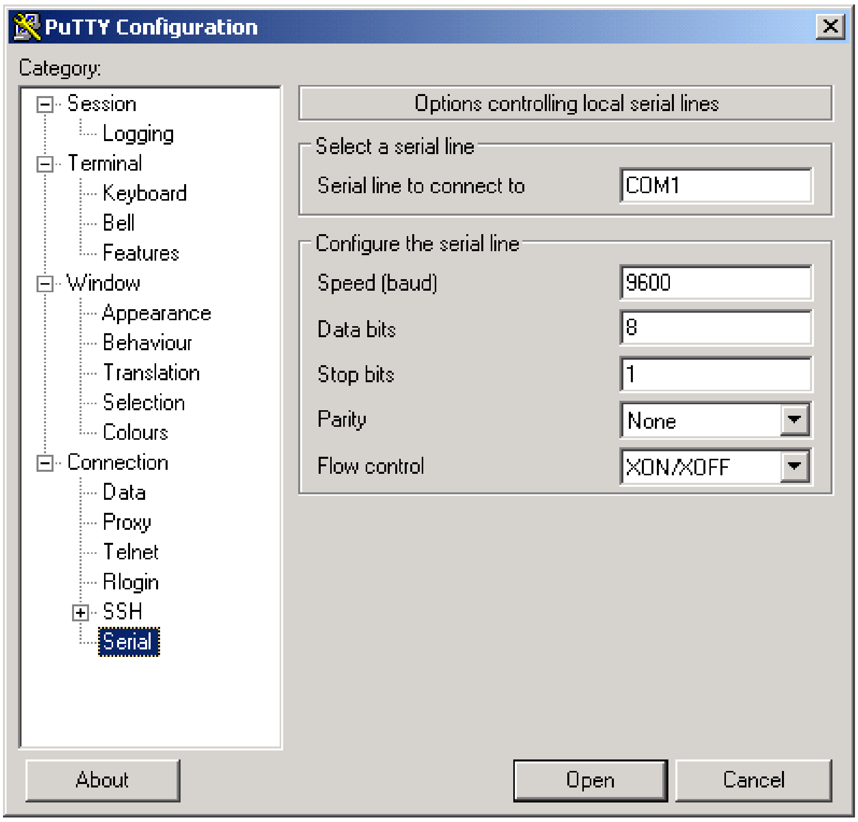
Figure 3: Setting up the telnet connection to the HiOS-2S/2A/3S RSPE via the DOS command line

■ 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:



PuTTY Configuration

Options controlling local serial lines

Select a serial line

Serial line to connect to: COM1

Configure the serial line

Speed (baud): 9600

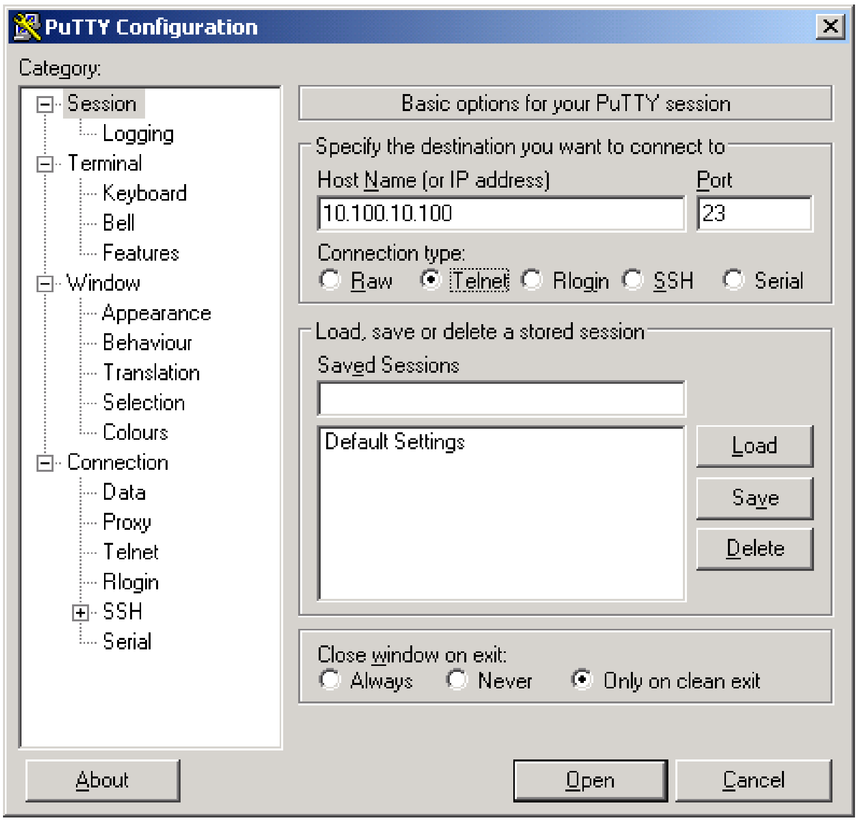
Data bits: 8

Stop bits: 1

Parity: None

Flow control: XON/XOFF

Figure 4: Configuring the serial data connection via PuTTY



Specify the destination you want to connect to

Host Name (or IP address): 10.100.10.100

Port: 23

Connection type: ○ Raw ● Telnet ○ Rlogin ○ SSH ○ Serial

Load, save or delete a stored session

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

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.

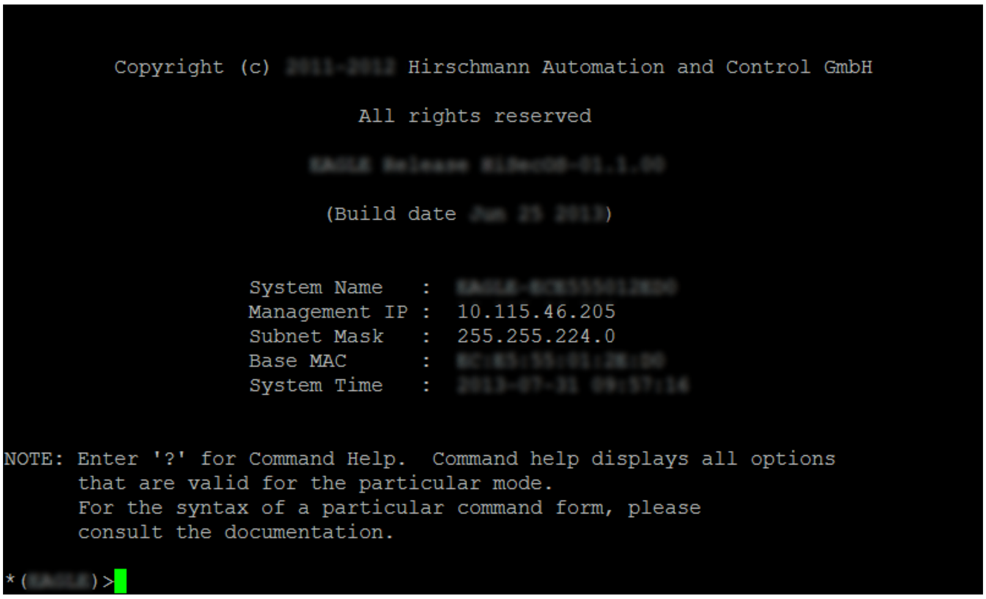
```
User: admin
Password:*******
```

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) [redacted] Hirschmann Automation and Control GmbH

                             All rights reserved

                              [redacted]

                          (Build date [redacted])


                   System Name   :  [redacted]
                   Management IP :  10.115.46.205
                   Subnet Mask   :  255.255.224.0
                   Base MAC      :  [redacted]
                   System Time   :  [redacted]

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.

*([redacted])>
```

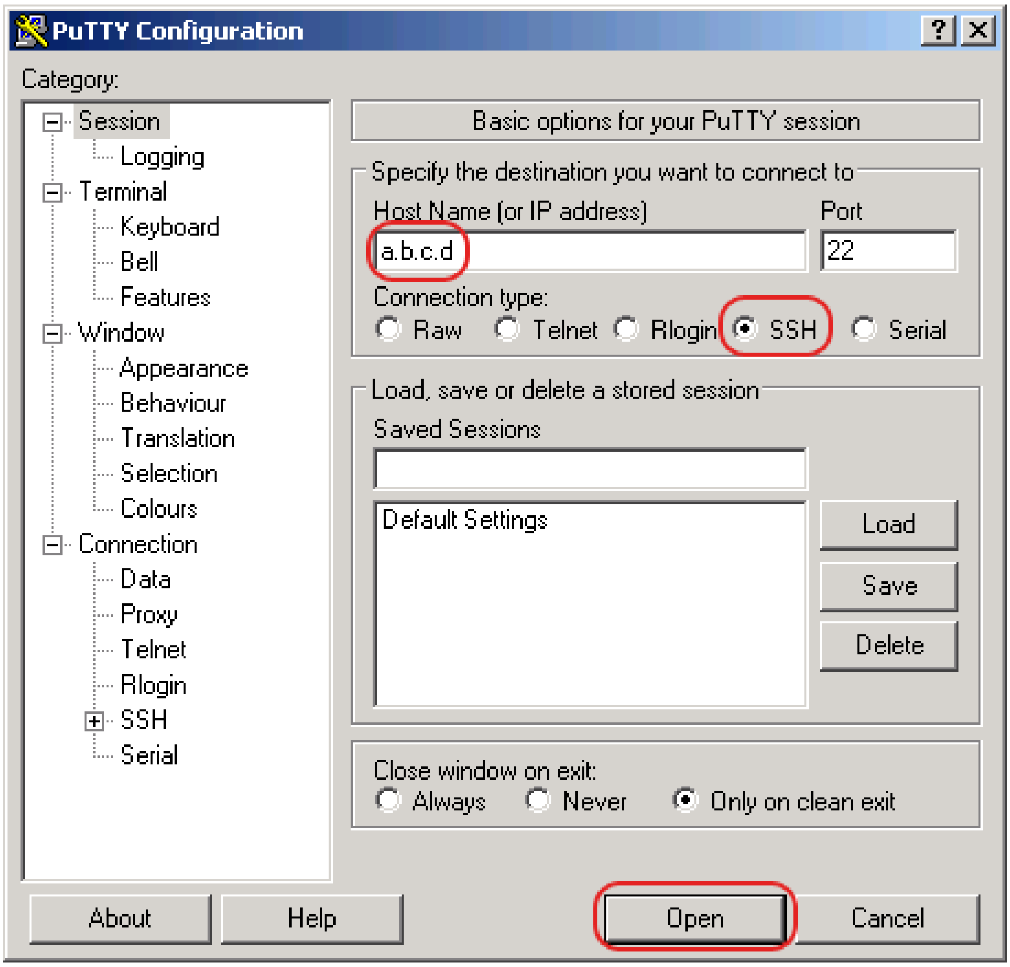
Figure 7: Start screen of CLI.

Your HiOS-2S/2A/3S RSPE appears with the command prompt
RSPE >

1.2.3 CLI via SSH (Secure Shell)

□ Start the PuTTY program on your computer.

PuTTY appears with the login screen.



Specify the destination you want to connect to

Host Name (or IP address): a.b.c.d

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 8: PuTTY input screen

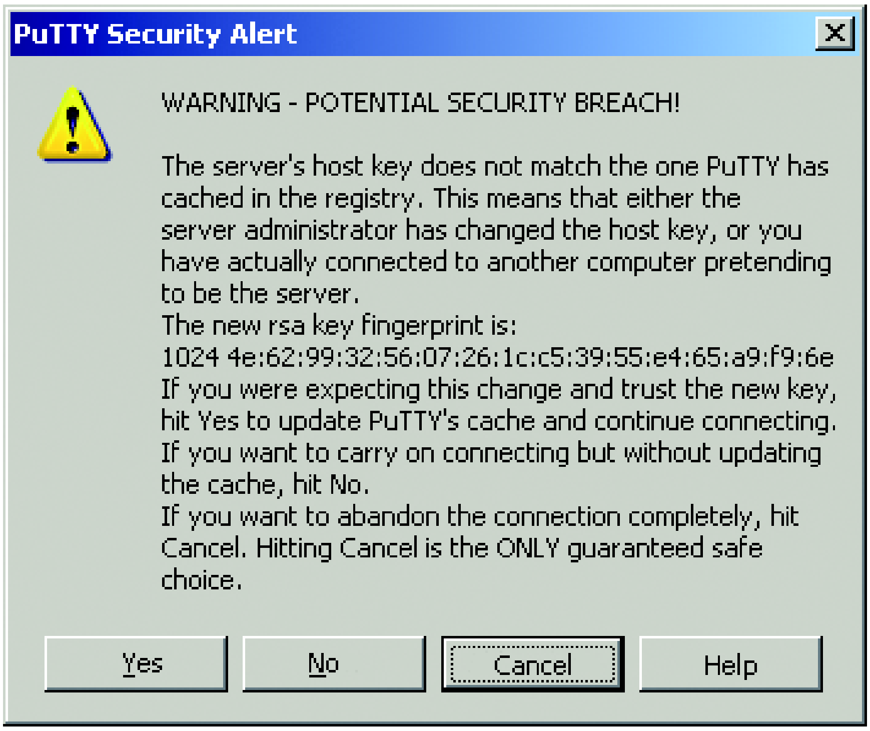
□ In the `Host Name (or IP address)` input field you enter the IP address of your device.
The IP address (a.b.c.d) consists of 4 decimal numbers with values from 0 to 255. The 4 decimal numbers are separated by points.

□ 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.



WARNING - POTENTIAL SECURITY BREACH!

The server's host key does not match the one PuTTY has cached in the registry. This means that either the server administrator has changed the host key, or you have actually connected to another computer pretending to be the server.
The new rsa key fingerprint is:
1024 4e:62:99:32:56:07:26:1c:c5:39:55:e4:65:a9:f9:6e
If you were expecting this change and trust the new key, hit Yes to update PuTTY's cache and continue connecting.
If you want to carry on connecting but without updating the cache, hit No.
If you want to abandon the connection completely, hit Cancel. Hitting Cancel is the ONLY guaranteed safe choice.

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

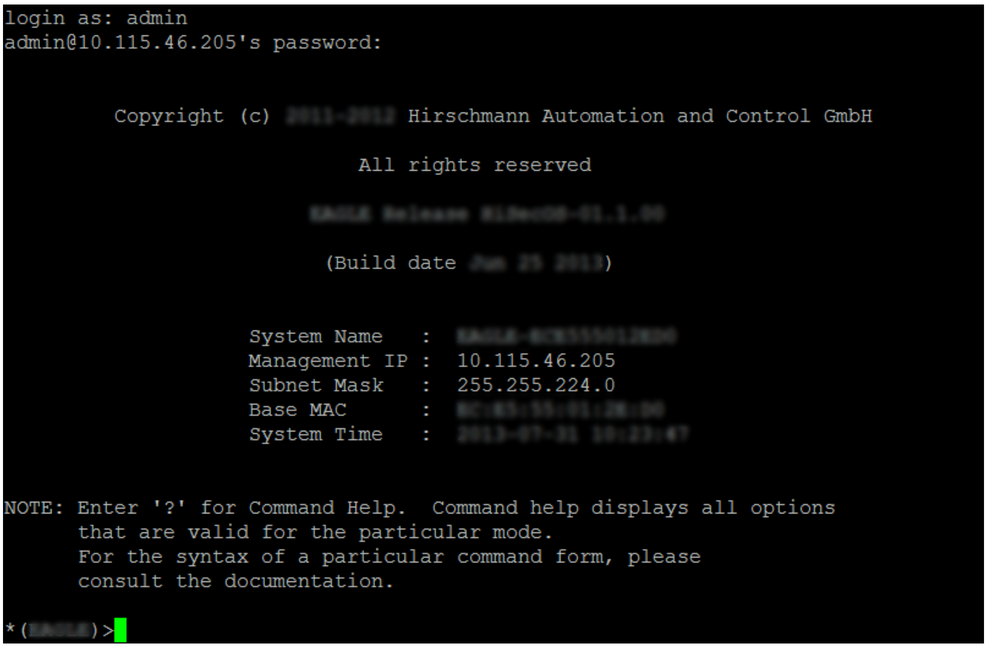
a.b.c.d is the IP address of your device.

☐ 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) [redacted] Hirschmann Automation and Control GmbH

                             All rights reserved

                          [redacted]

                          (Build date [redacted])


                    System Name    :  [redacted]
                    Management IP  :  10.115.46.205
                    Subnet Mask    :  255.255.224.0
                    Base MAC       :  [redacted]
                    System Time    :  [redacted]


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.

*([redacted])>
```

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.

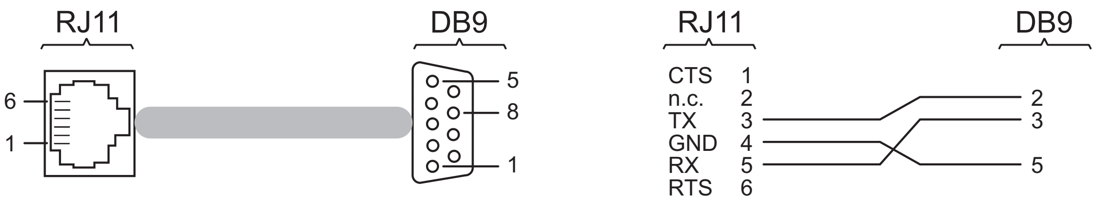
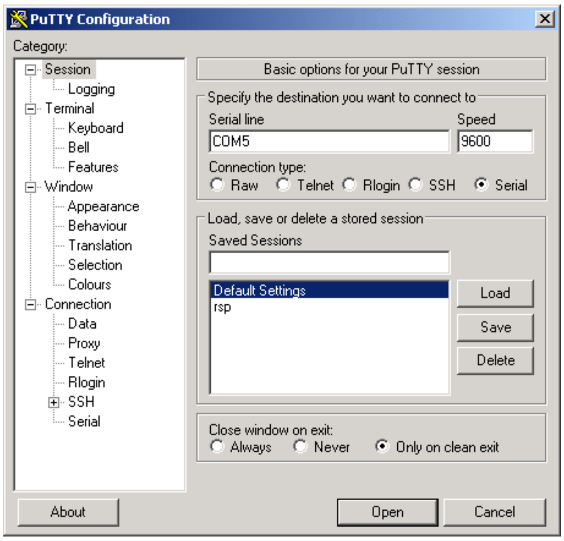


Figure 12: Pin assignment of the V.24 interface and the DB9 connector

- □ 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 13). Press the Enter key.



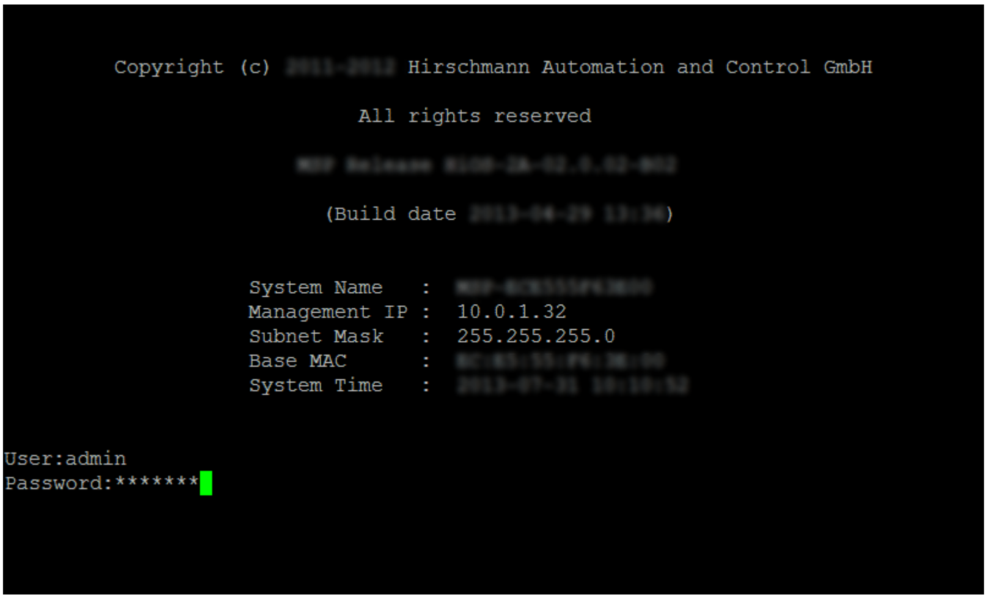
Specify the destination you want to connect to
Serial line: COM5
Speed: 9600
Connection type: ○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial

Load, save or delete a stored session
Saved Sessions
Default Settings
rsp

Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 13: 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.



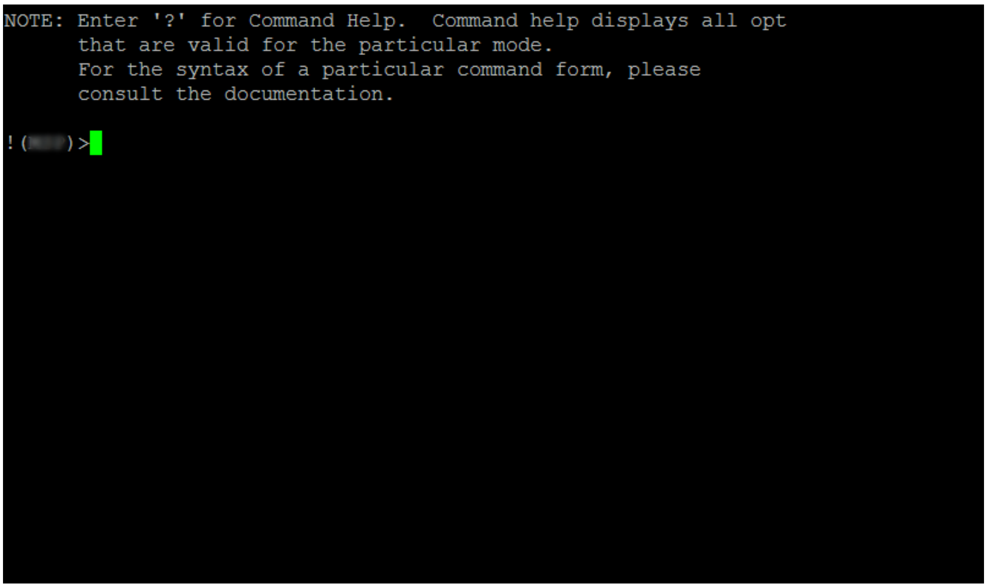
```
        Copyright (c) [redacted] Hirschmann Automation and Control GmbH

                          All rights reserved

                        [redacted]

                       (Build date [redacted])


                   System Name   :  [redacted]
                   Management IP :  10.0.1.32
                   Subnet Mask   :  255.255.255.0
                   Base MAC      :  [redacted]
                   System Time   :  [redacted]


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

Figure 14: 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.

!([redacted])>
```

Figure 15: 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:

- ▶ Managing the operating system and verifying the software image
- ▶ 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:

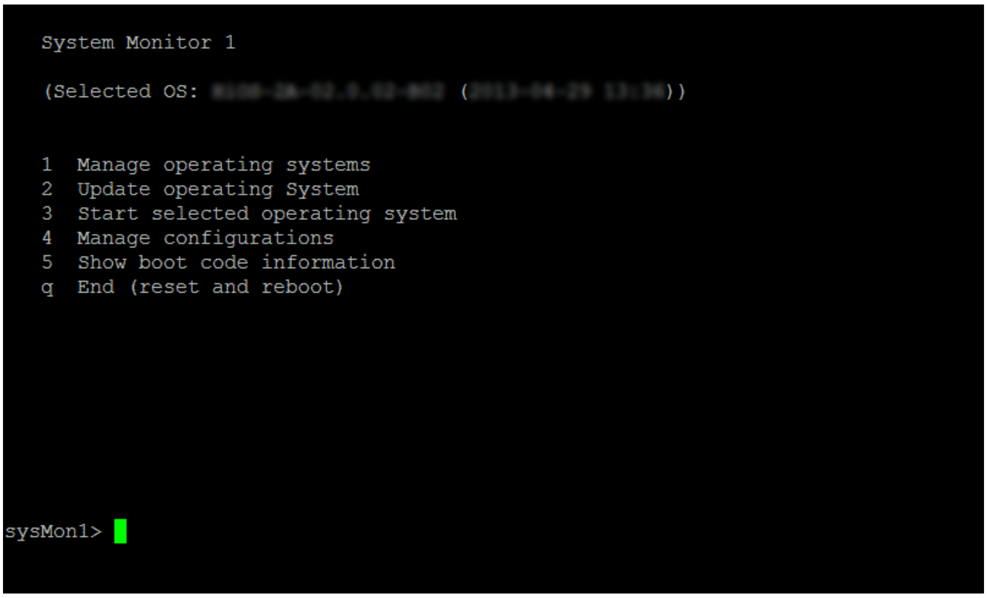
□ Use the terminal cable to connect the V.24 interface of the device with the “COM” port of the PC.
□ Start the VT100 terminal emulation on the PC.
□ Specify the following transmission parameters:
  - Speed: 9,600 baud
  - Stopbit: 8 bit

- 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: [redacted] ([redacted]))


  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 16: 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
- Configuration using the external memory.
  You choose this method if you are replacing a device with a device of the same type and have already saved the configuration in the external memory.
- 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-Sahara Africa
- LACNIC (Regional Latin-American and Caribbean IP Address Registry) – Latin America and some Caribbean Islands
- RIPE NCC (Réseaux IP Européens) - Europe and Surrounding Regions

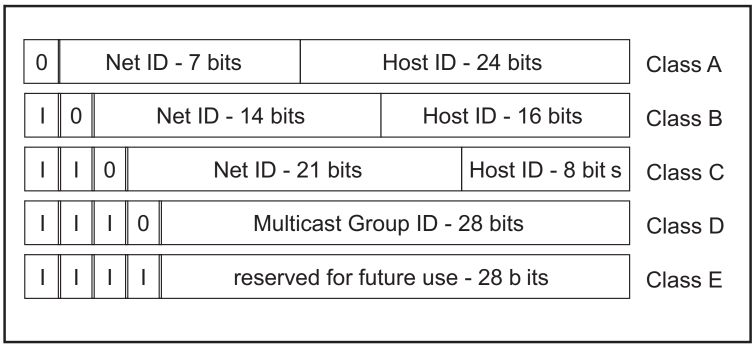

0 | Net ID - 7 bits | Host ID - 24 bits | Class A
I | 0 | Net ID - 14 bits | Host ID - 16 bits | Class B
I | I | 0 | Net ID - 21 bits | Host ID - 8 bit s | Class C
I | I | I | 0 | Multicast Group ID - 28 bits | Class D
I | I | I | I | reserved for future use - 28 b its | Class E

Figure 17: 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.

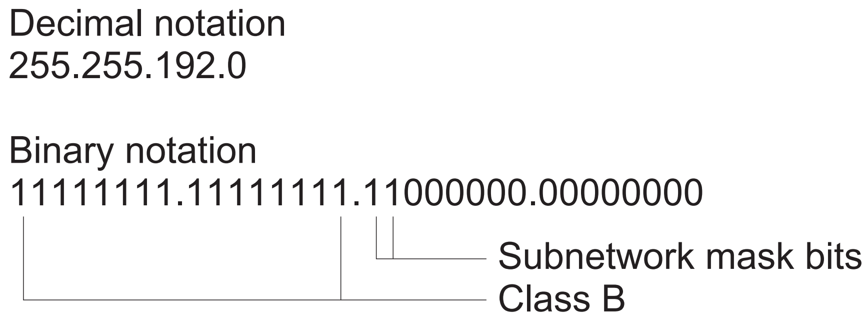
2.1.2 Netmask

Routers and gateways subdivide large networks into subnetworks. The netmask asssigns 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:

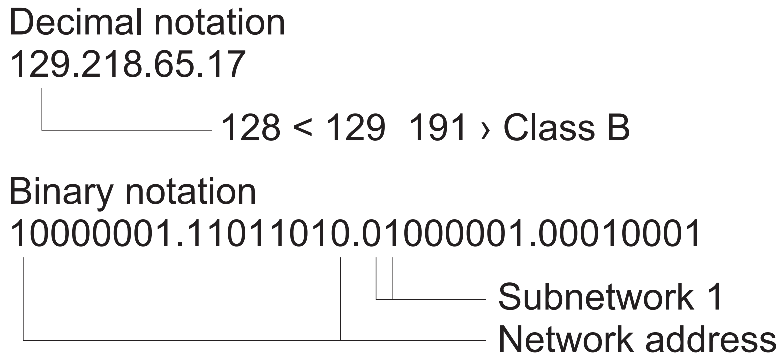


Decimal notation
255.255.192.0

Binary notation
11111111.11111111.11000000.00000000

Subnetwork mask bits
Class B

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

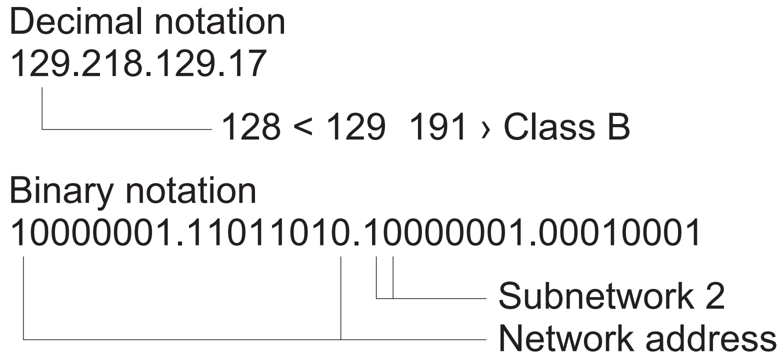


Decimal notation
129.218.65.17

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?

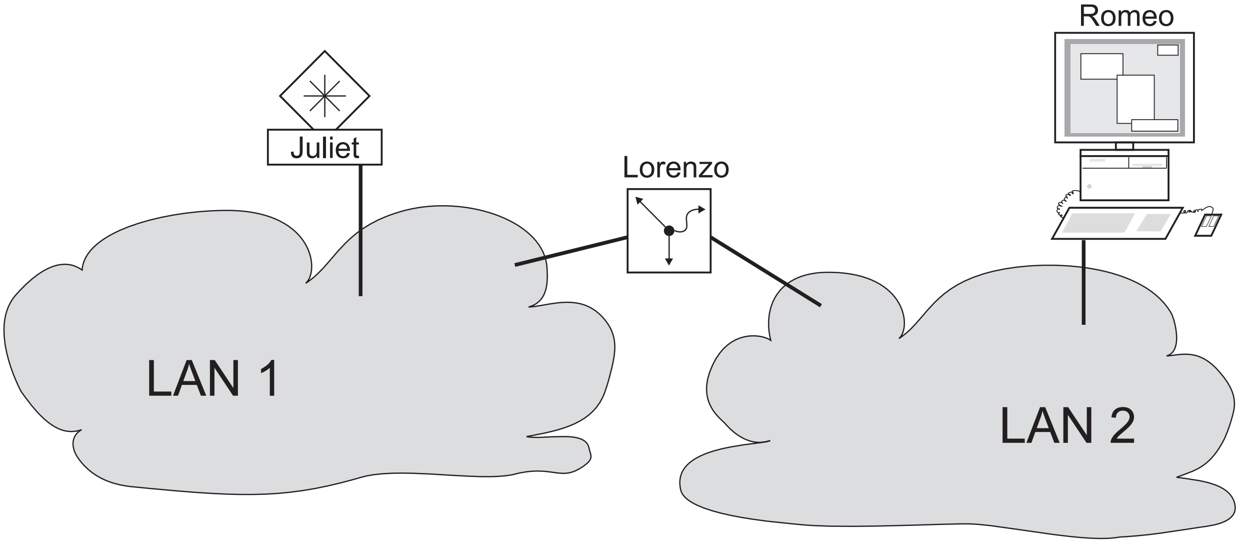


Figure 18: Management agent that is separated from its management station by a router

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 hmNetGateway-IPAddr 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
		25 mask bits

CIDR notation: 149.218.112.0/25

Mask bits

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, the HiDiscovery protocol, the external memory. You have the option of performing the configuration via the V.24 interface using the CLI.

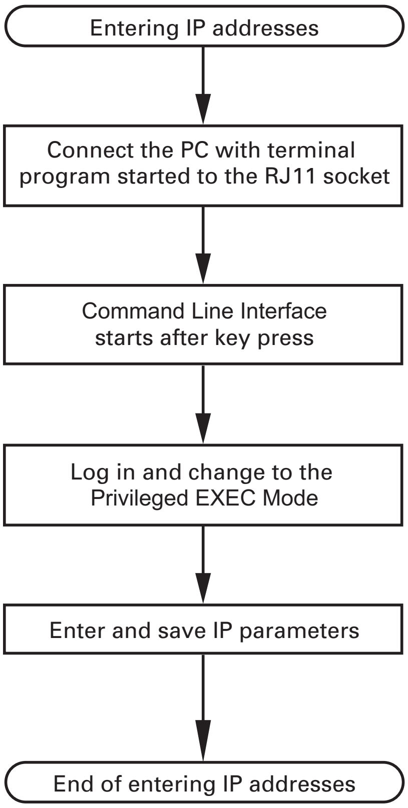
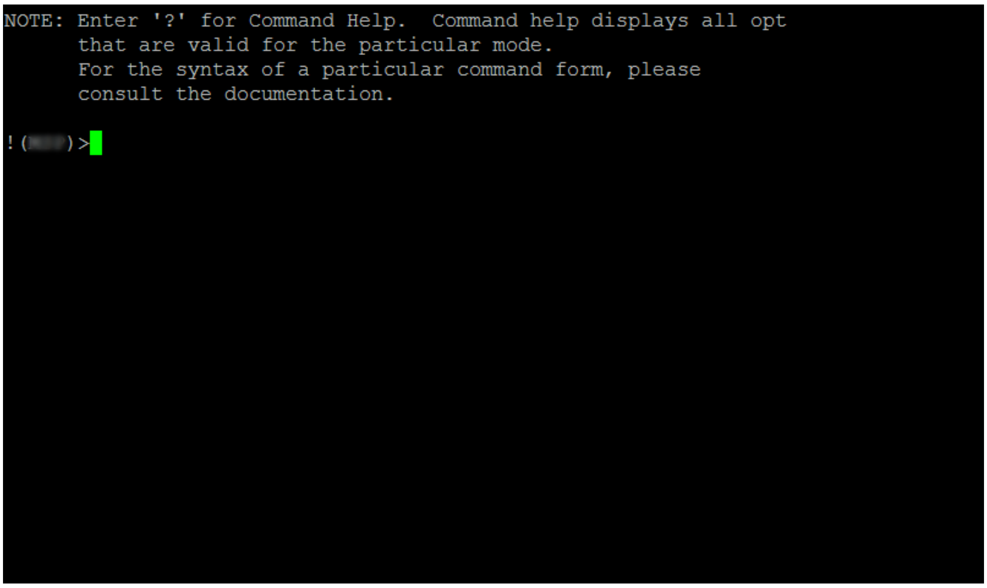

Entering IP addresses
Connect the PC with terminal program started to the RJ11 socket
Command Line Interface starts after key press
Log in and change to the Privileged EXEC Mode
Enter and save IP parameters
End of entering IP addresses

Figure 19: 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.

!([redacted])>
```

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

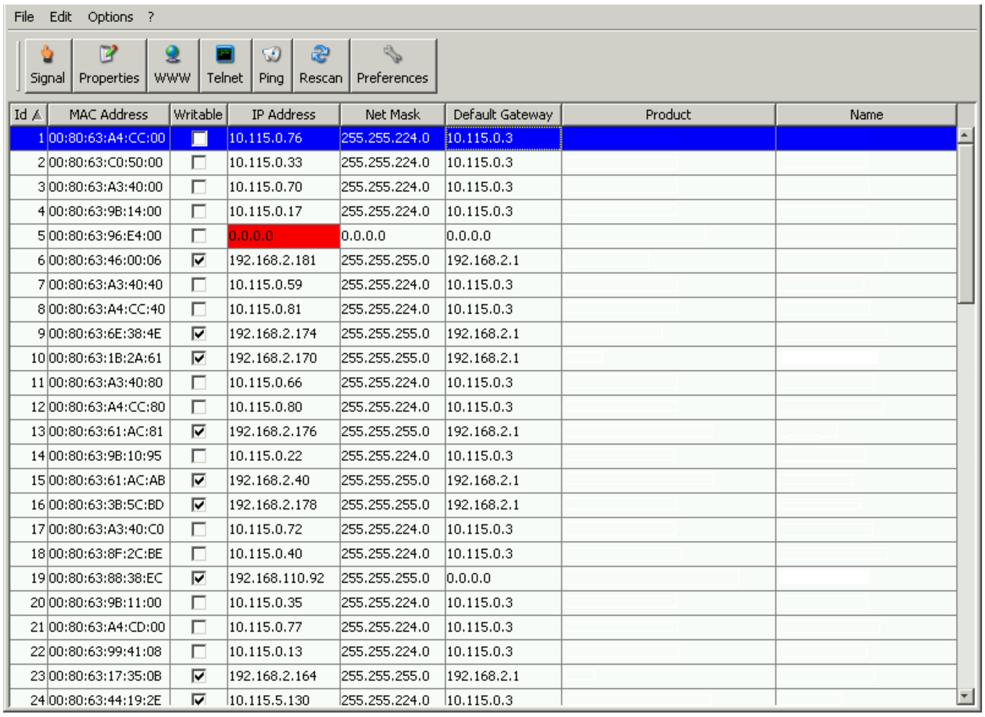
After entering the IP parameters, you easily configure the device via the graphical user interface (see the “GUI” reference manual).

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.



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

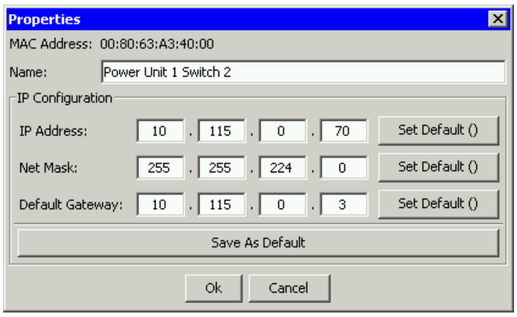
Figure 20: HiDiscovery

When HiDiscovery is started, HiDiscovery 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 can 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 in the tool bar to set the LEDs for the selected device flashing. To switch off the flashing, click on the symbol again.
☐ By double-clicking a line, you open a window in which you can enter the device name and the IP parameter.



Properties

MAC Address: 00:80:63:A3:40:00

Name: Power Unit 1 Switch 2

IP Configuration

IP Address: 10 . 115 . 0 . 70

Net Mask: 255 . 255 . 224 . 0

Default Gateway: 10 . 115 . 0 . 3

Figure 21: HiDiscovery—IP parameter assignment

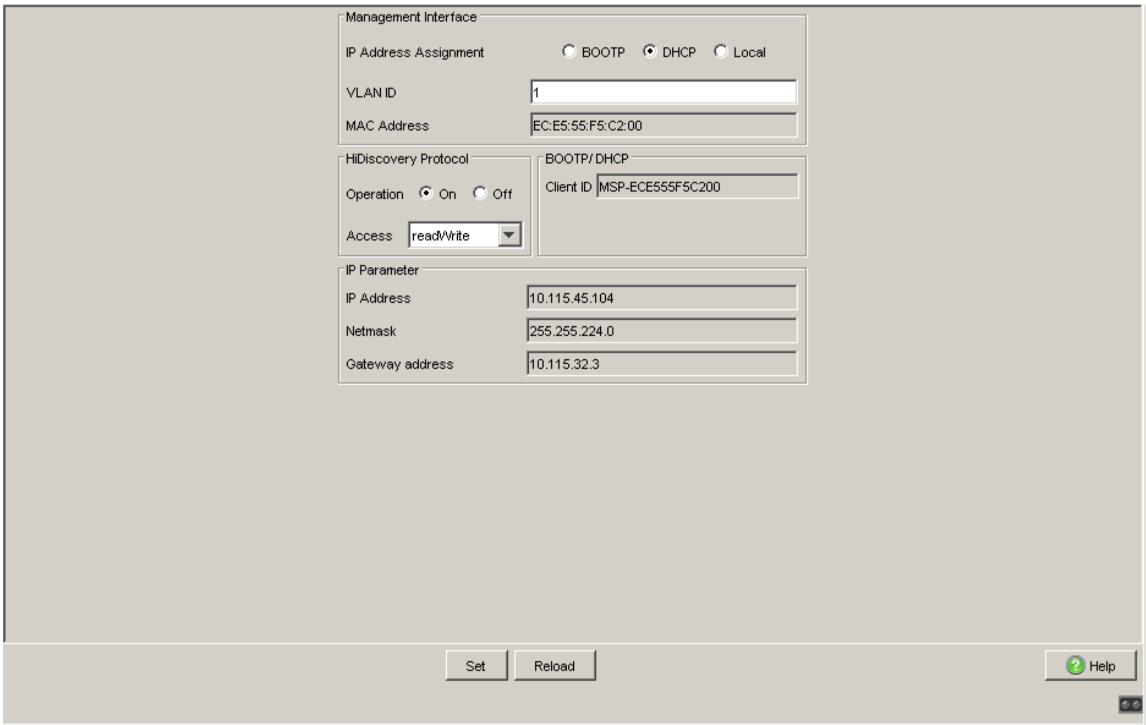
Note: For security reasons, switch off the HiDiscovery function for the device in the graphical user interface, after you have assigned the IP parameters to the device.

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.



Management Interface

IP Address Assignment ○ BOOTP ● DHCP ○ Local

VLAN ID 1

MAC Address EC:E5:55:F5:C2:00

HiDiscovery Protocol

Operation ● On ○ Off

Access readWrite

BOOTP/ DHCP

Client ID MSP-ECE555F5C200

IP Parameter

IP Address 10.115.45.104

Netmask 255.255.224.0

Gateway address 10.115.32.3

Figure 22: `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 Sever 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 47.

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:

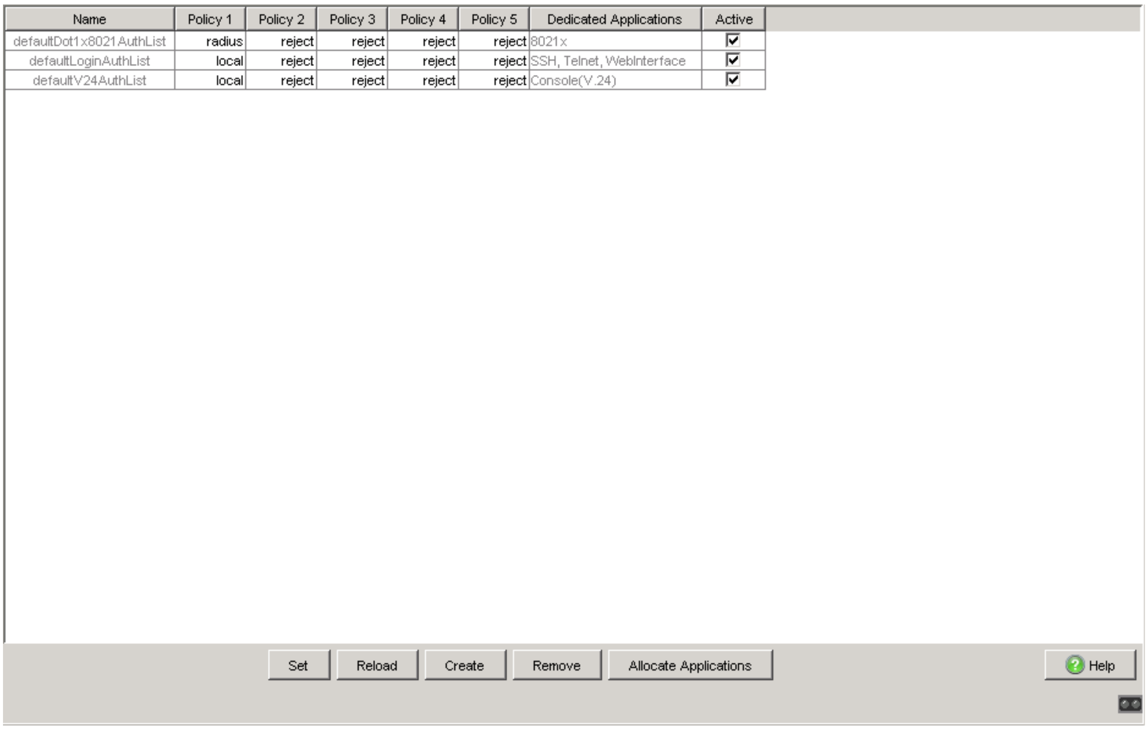
- `defaultDot1x8021AuthList`
  This list specifies the methods for the authentication of connected terminal devices using IEEE 802.1X. The `8021x` application is allocated to the list.
- `defaultLoginAuthList`
  This list specifies the methods for the authentication for users that log in using the graphical 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	☑
defaultLoginAuthList	local	reject	reject	reject	reject	SSH, Telnet, WebInterface	☑
defaultV24AuthList	local	reject	reject	reject	reject	Console(V.24)	☑

Figure 23: `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.

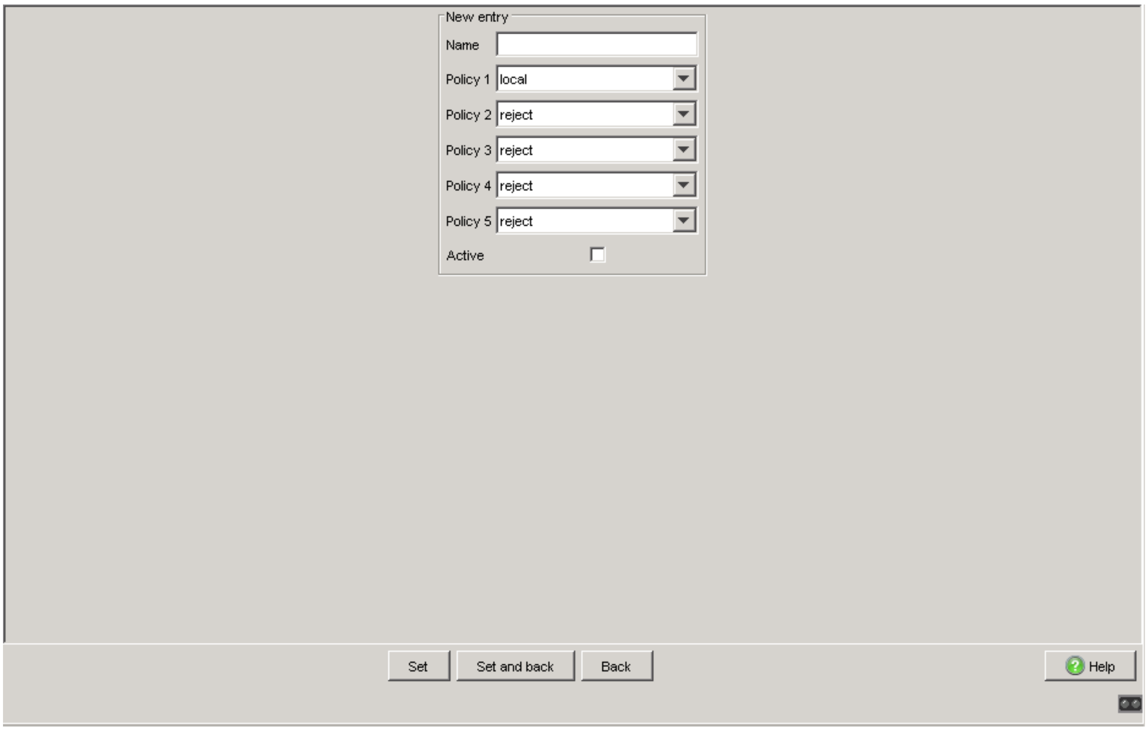
In the following example, we will set up a separate list for each of the applications included in the default list `defaultLoginAuthList`.

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.



New entry

Name:

Policy 1: local

Policy 2: reject

Policy 3: reject

Policy 4: reject

Policy 5: reject

Active: □

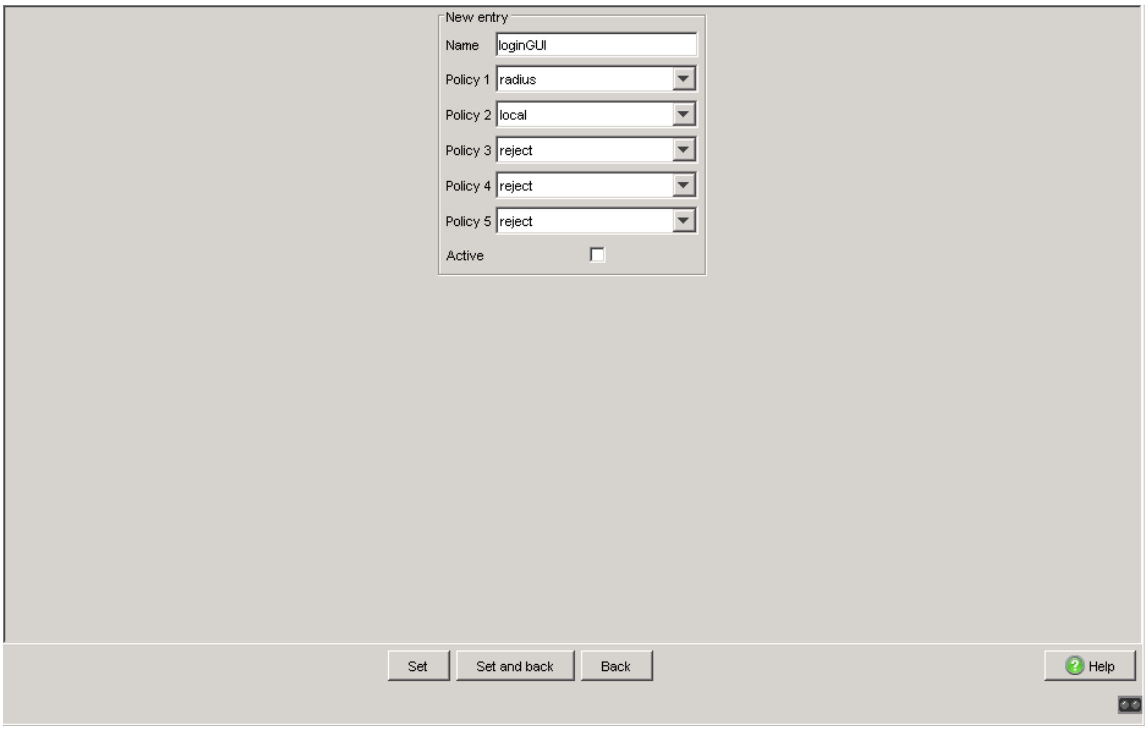
Figure 24: New entry frame in the `Device Security > Authentication List` dialog

□ 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 "Policy 1" field.
- □ 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 unsuccessful, 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"


New entry

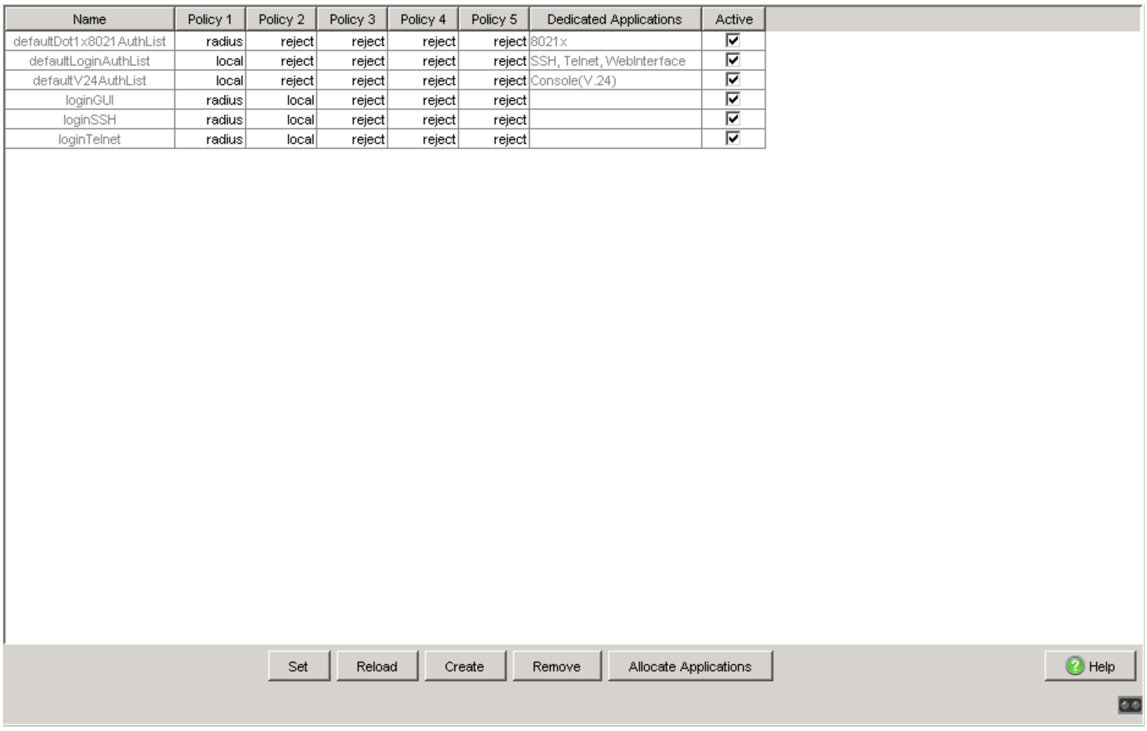
Name	loginGUI
Policy 1	radius
Policy 2	local
Policy 3	reject
Policy 4	reject
Policy 5	reject
Active	□

Figure 25: 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	☑
defaultLoginAuthList	local	reject	reject	reject	reject	SSH, Telnet, WebInterface	☑
defaultV24AuthList	local	reject	reject	reject	reject	Console(V.24)	☑
loginGUI	radius	local	reject	reject	reject		☑
loginSSH	radius	local	reject	reject	reject		☑
loginTelnet	radius	local	reject	reject	reject		☑

Figure 26: `Device Security > Authentication List` *dialog*

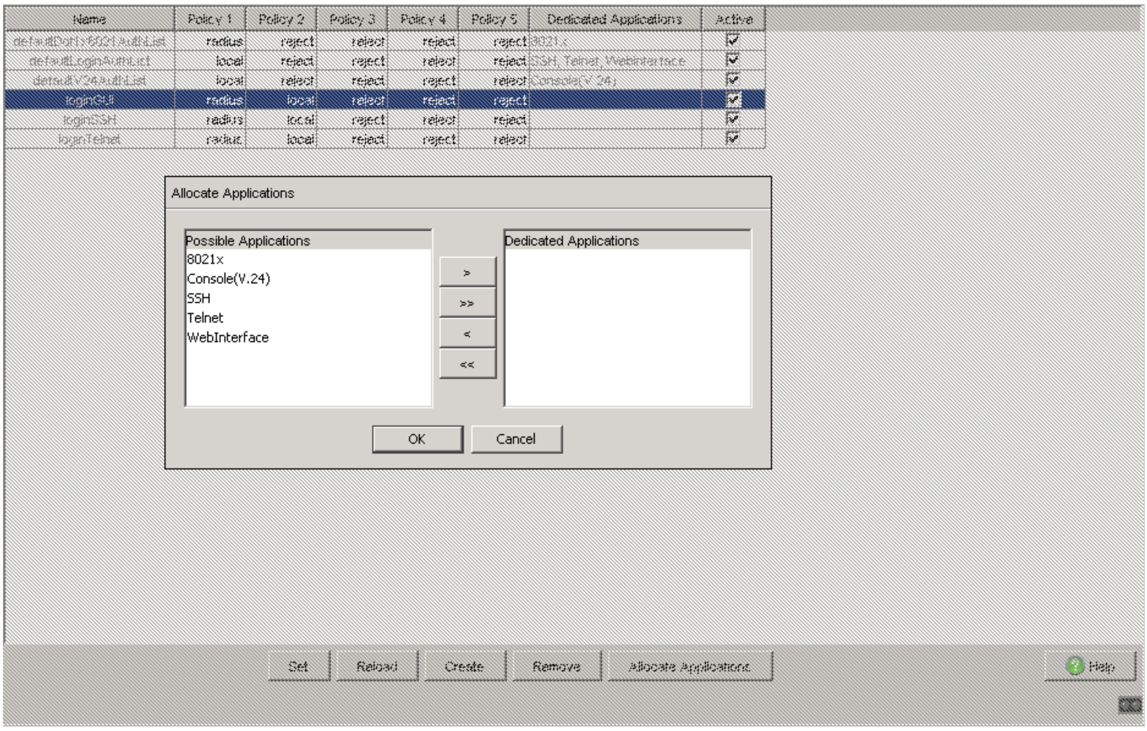
`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`authlists add loginGUI`	Creates the `loginGUI` list.
`authlists enable loginGUI`	Activates the `loginGUI` list.
`authlists set-policy loginGUI radius local reject reject reject`	Allocates the methods to the `loginGUI` list according to the example.
`show authlists`	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.



Name	Policy 1	Policy 2	Policy 3	Policy 4	Policy 5	Dedicated Applications	Active
defaultDot1x8021AuthList	radius	reject	reject	reject	reject	8021x	☑
defaultLoginAuthList	local	reject	reject	reject	reject	SSH, Telnet, WebInterface	☑
defaultV24AuthList	local	reject	reject	reject	reject	Console(V.24)	☑
loginGUI	radius	local	reject	reject	reject		☑
loginSSH	radius	local	reject	reject	reject		☑
loginTelnet	radius	local	reject	reject	reject		☑

Allocate Applications

Possible Applications	Dedicated Applications
8021x	
Console(V.24)	
SSH	
Telnet	
WebInterface	

Figure 27: 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.

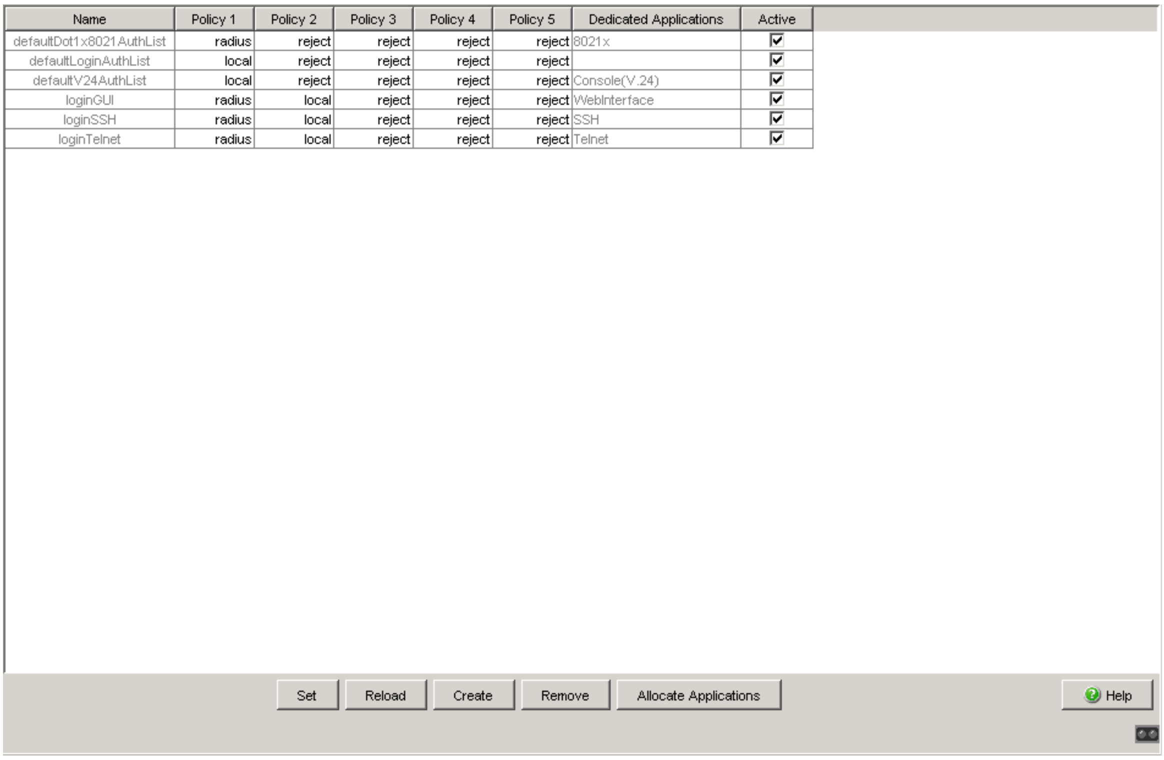
- For access using the graphical user interface (GUI), select `Web Interface`.
- For access using the CLI via SSH, select `SSH`.
- For access using the CLI via Telnet, select `Telnet`.

□ 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	☑
defaultLoginAuthList	local	reject	reject	reject	reject		☑
defaultV24AuthList	local	reject	reject	reject	reject	Console(V.24)	☑
loginGUI	radius	local	reject	reject	reject	WebInterface	☑
loginSSH	radius	local	reject	reject	reject	SSH	☑
loginTelnet	radius	local	reject	reject	reject	Telnet	☑

Figure 28: `Device Security > Authentication List` *dialog*

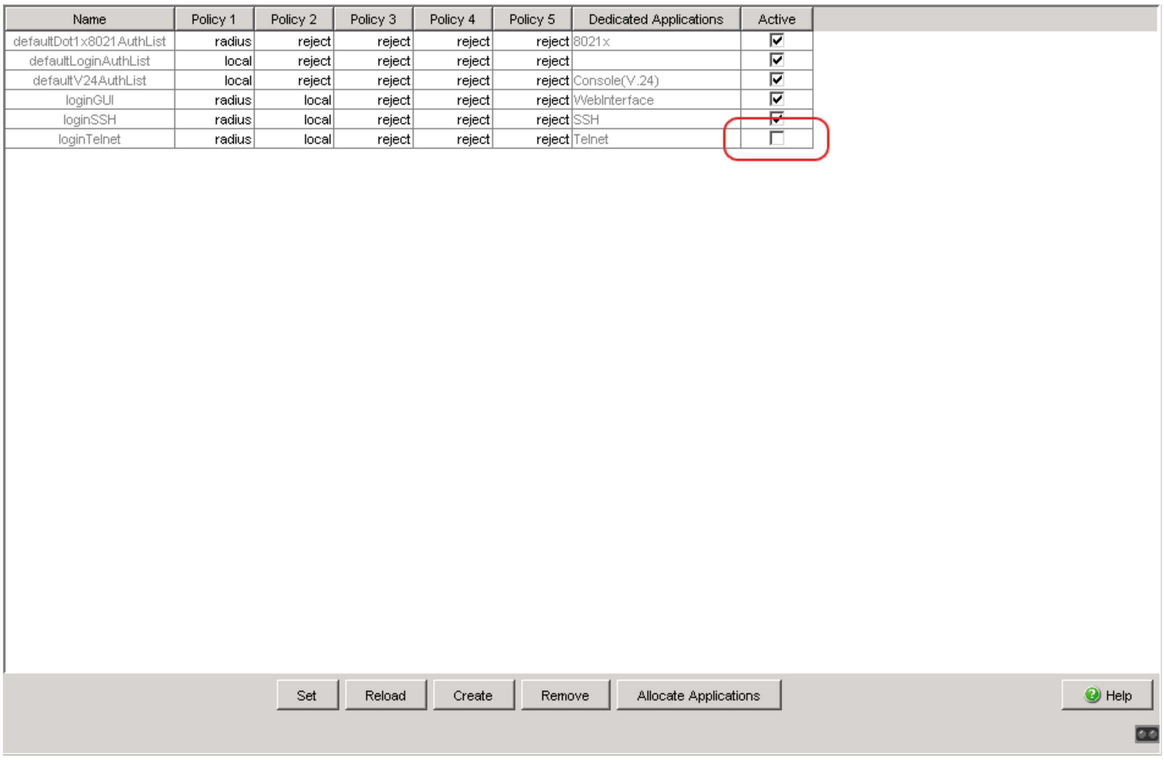
- □ Repeat these work steps to allocate an application to the other lists.
- □ To temporarily save the changes, click "Set".

`show applists`	Shows the applications and the allocated lists.
`appllists set-authlist WebInterface loginGUI`	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	☑
defaultLoginAuthList	local	reject	reject	reject	reject		☑
defaultV24AuthList	local	reject	reject	reject	reject	Console(V.24)	☑
loginGUI	radius	local	reject	reject	reject	WebInterface	☑
loginSSH	radius	local	reject	reject	reject	SSH	☑
loginTelnet	radius	local	reject	reject	reject	Telnet	□

Figure 29: `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`	Deactivates the `loginTelnet` list.
`save`	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: ▶ 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 ▶ External memory activation and deactivation ▶ 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 activtities 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 activtities with read access.
Unauthorized	No access to the device possible. ▶ 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.)

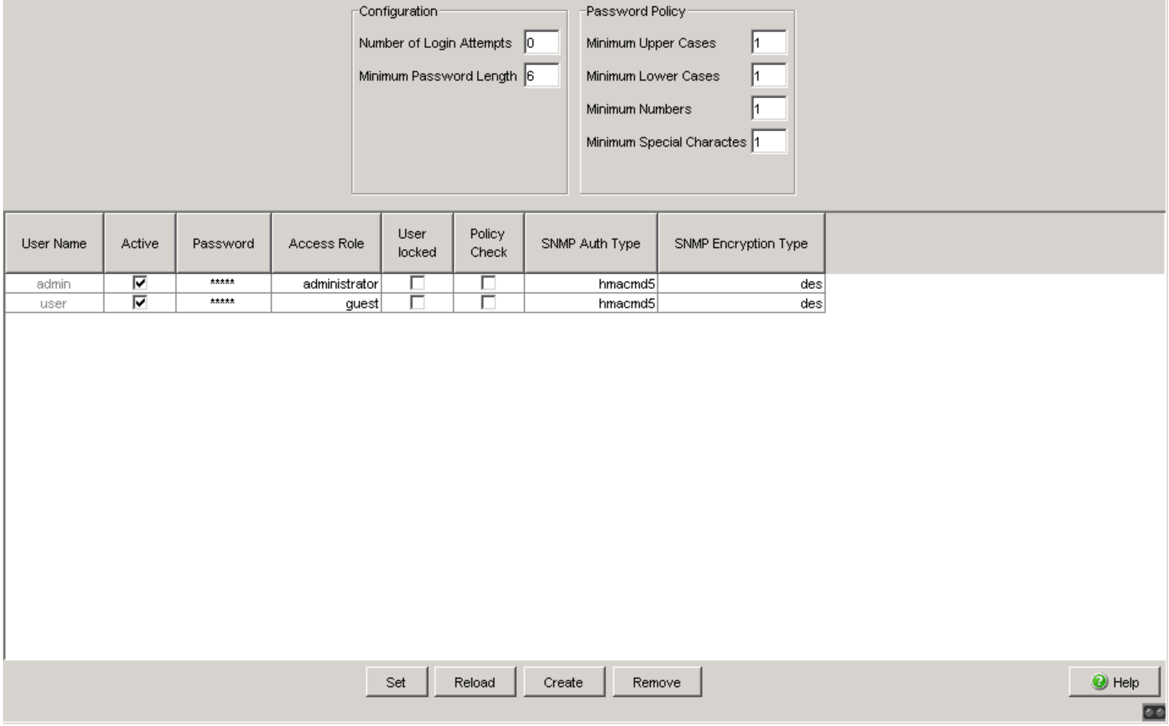
3.2.2 Managing user accounts

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.



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 Charactes: 1

User Name	Active	Password	Access Role	User locked	Policy Check	SNMP Auth Type	SNMP Encryption Type
admin	☑	*****	administrator	□	□	hmacmd5	des
user	☑	*****	guest	□	□	hmacmd5	des

Figure 30: `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	`admin`	`user`
Password	`private`	`public`
Authorization	`administrator`	`guest`
User locked	`off`	`off`
Policy Check	`off`	`off`
SNMP Auth Type	`hmacmd5`	`hmacmd5`
SNMP Encryption Type	`des`	`des`

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.

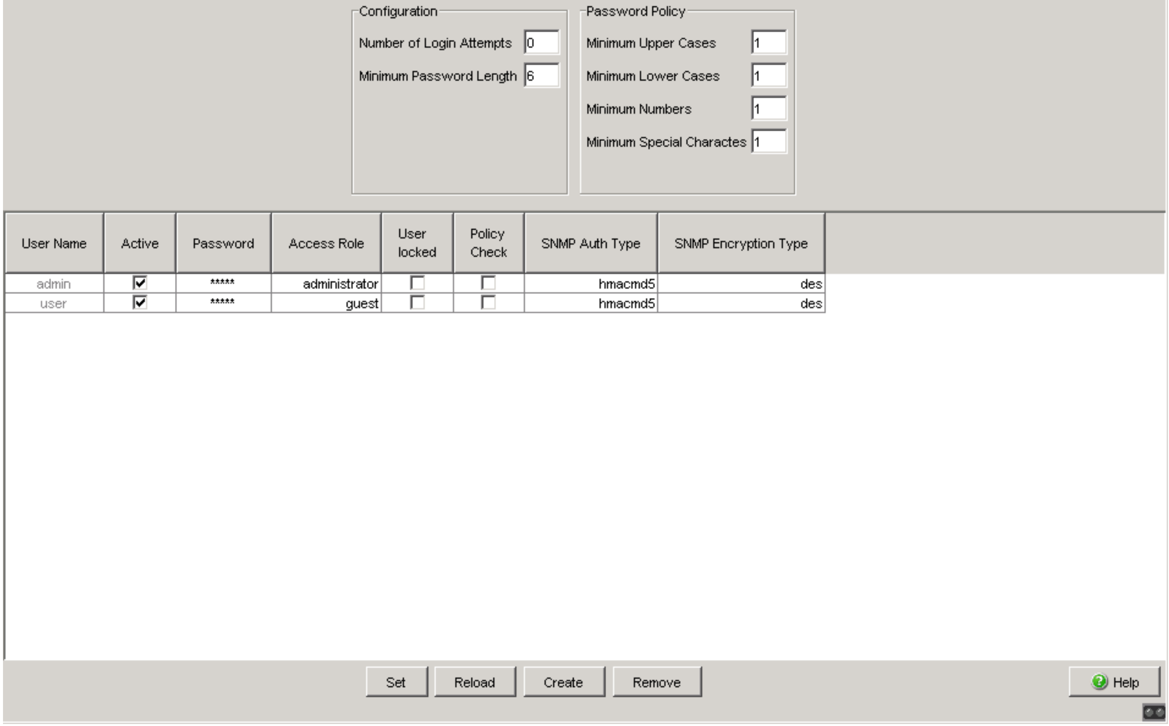
Prerequisite: User account with authorization profile `administrator`.

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.



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 Charactes 1

User Name	Active	Password	Access Role	User locked	Policy Check	SNMP Auth Type	SNMP Encryption Type
admin	☑	*****	administrator	☐	☐	hmacmd5	des
user	☑	*****	guest	☐	☐	hmacmd5	des

Figure 31: `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".

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`users password-policy-check <user> enable`	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 (`show security-status all`). You specify the settings that cause this message with the command `security-status monitor pwd-policy-inactive`.

`users password <user> SECRET`	Specifies the password “SECRET” for the `<user>` user account. Enter at least 6 characters.
`save`	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.

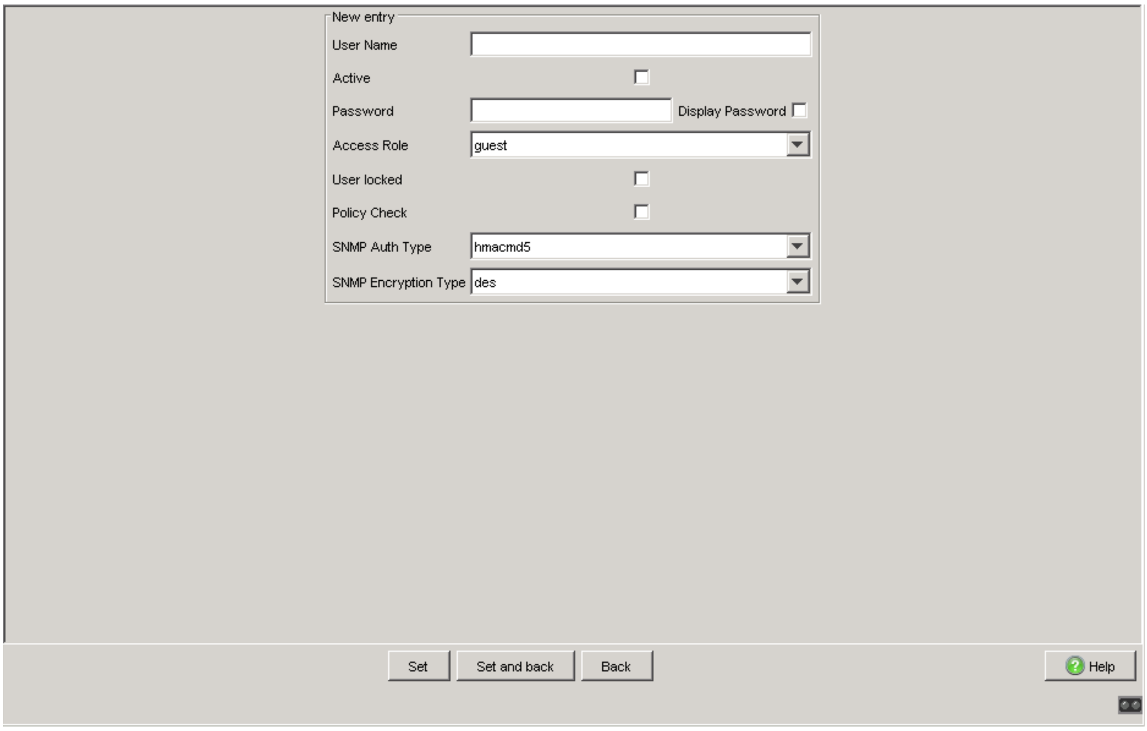
Prerequisite: User account with authorization profile `administrator`.

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.



New entry

User Name		
Active	□	
Password		Display Password □
Access Role	guest	
User locked	□	
Policy Check	□	
SNMP Auth Type	hmacmd5	
SNMP Encryption Type	des	

Figure 32: 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.

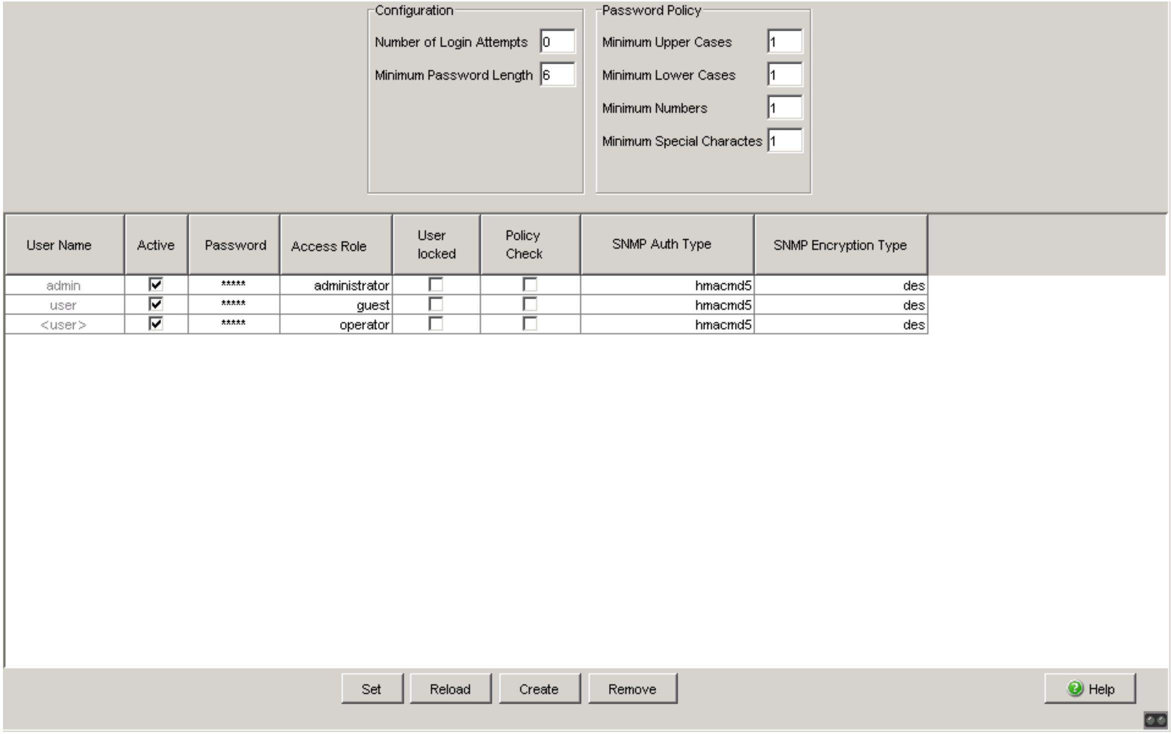
- □ To make the password visible when it is being input, select the "Display Password" checkbox.
- ▶ The device differentiates between upper and lower case.
- ▶ The minimum length of the password is defined in the "Configuration" frame. The device always checks the minimum length of the password.

□ 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.



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 Charactes: 1

User Name	Active	Password	Access Role	User locked	Policy Check	SNMP Auth Type	SNMP Encryption Type
admin	☑	*****	administrator	□	□	hmacmd5	des
user	☑	*****	guest	□	□	hmacmd5	des
<user>	☑	*****	operator	□	□	hmacmd5	des

Figure 33: `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.

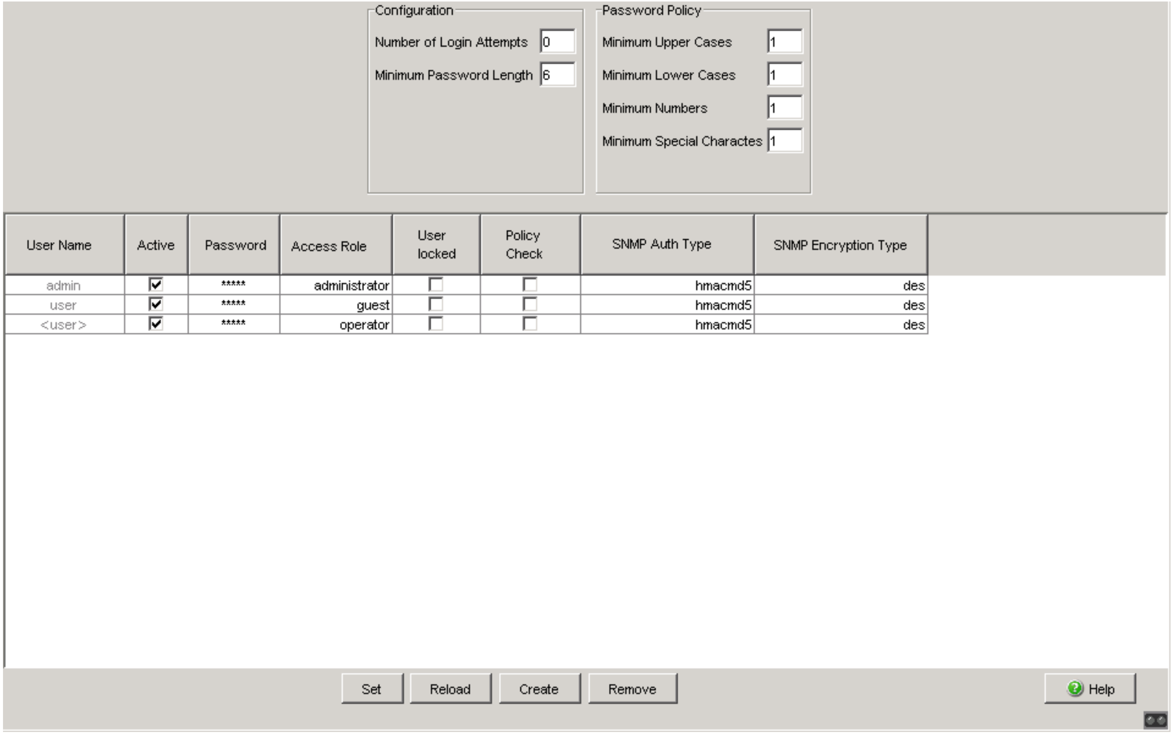
Prerequisite: User account with authorization profile `administrator`.

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.



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 Charactes: 1

User Name	Active	Password	Access Role	User locked	Policy Check	SNMP Auth Type	SNMP Encryption Type
admin	☑	*****	administrator	□	□	hmacmd5	des
user	☑	*****	guest	□	□	hmacmd5	des
<user>	☑	*****	operator	□	□	hmacmd5	des

Figure 34: `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`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`users disable <user>`	To disable 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.

- □ 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>`	Deletes the `<user>` 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.

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.

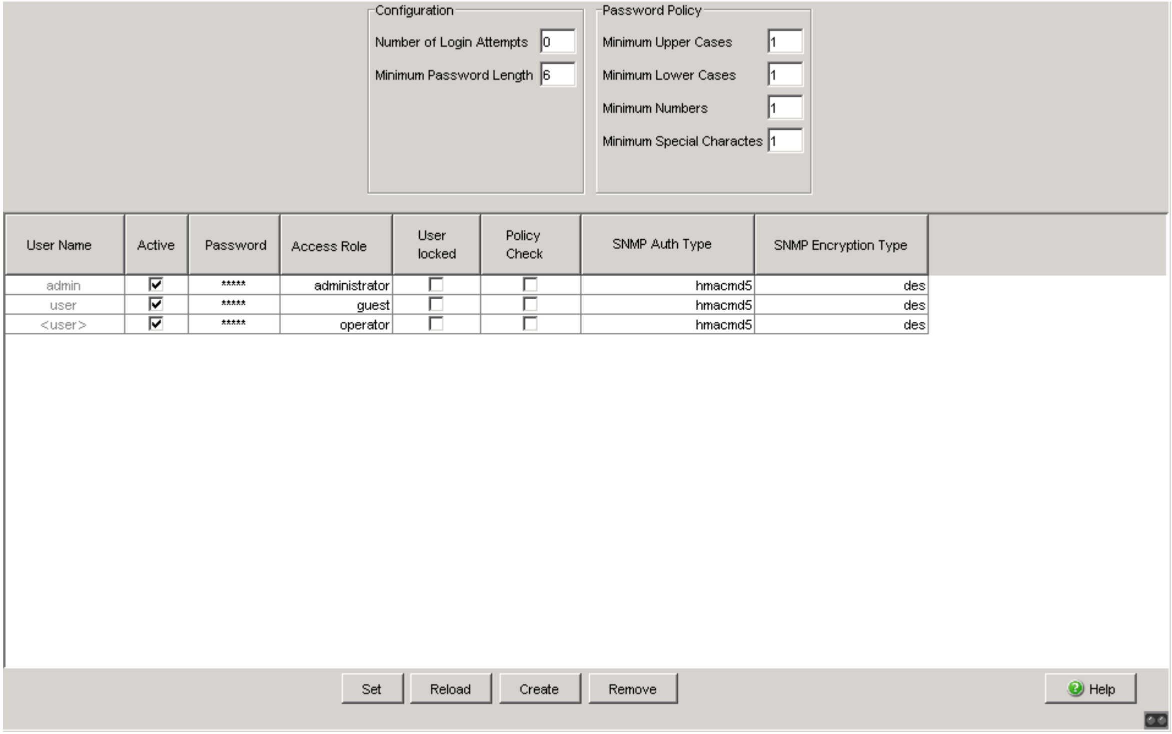
In the default settings, practical values for the policy are set up on the device. You have the option of adjusting the policy to meet your requirements.

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.



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 Charactes	1

User Name	Active	Password	Access Role	User locked	Policy Check	SNMP Auth Type	SNMP Encryption Type
admin	☑	*****	administrator	□	□	hmacmd5	des
user	☑	*****	guest	□	□	hmacmd5	des
<user>	☑	*****	operator	□	□	hmacmd5	des

Figure 35: `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".

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`passwords min-lenght 6`	Specifies the policy for the minimum length of the password.
`passwords min-lowercase-chars 1`	Specifies the policy for the minimum number of lower-case letters in the password.
`passwords min-numeric-chars 1`	Specifies the policy for the minimum number of digits in the password.
`passwords min-special-chars 1`	Specifies the policy for the minimum number of special characters in the password.
`passwords min-uppercase-chars 1`	Specifies the policy for the minimum number of upper-case letters in the password.
`show passwords`	Shows the policies that are set up.
`save`	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.

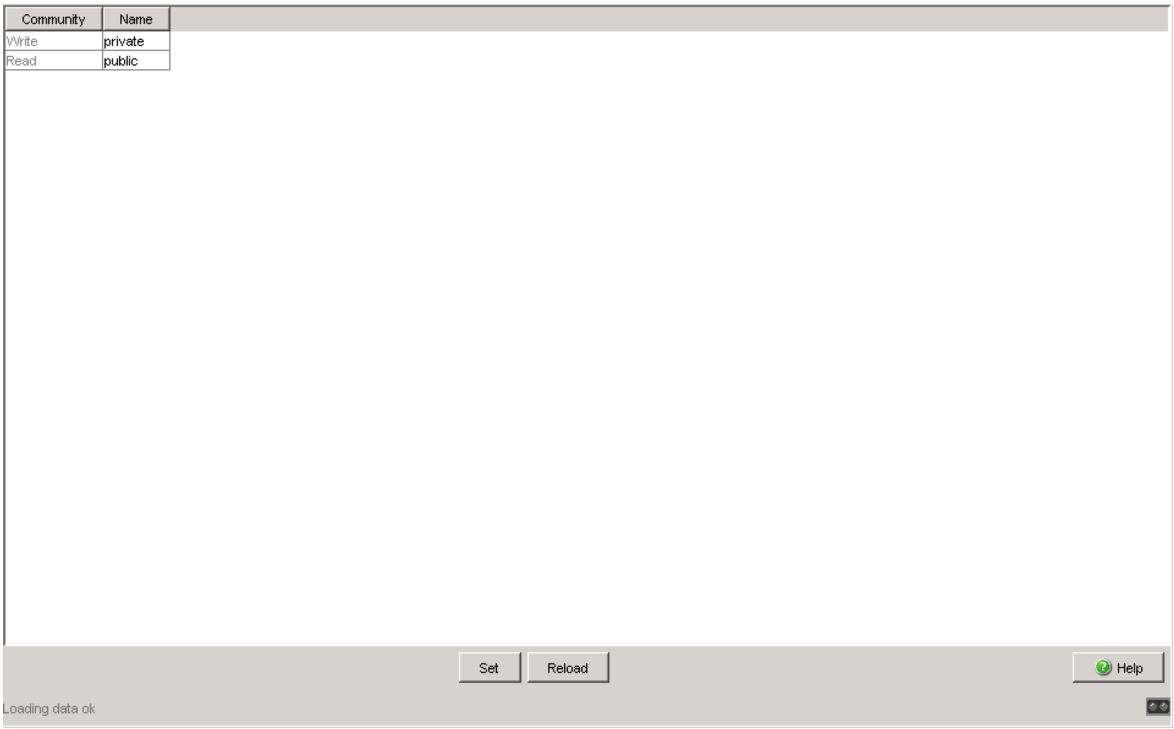
Prerequisite: User account with authorization profile `administrator`.

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 36: `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".

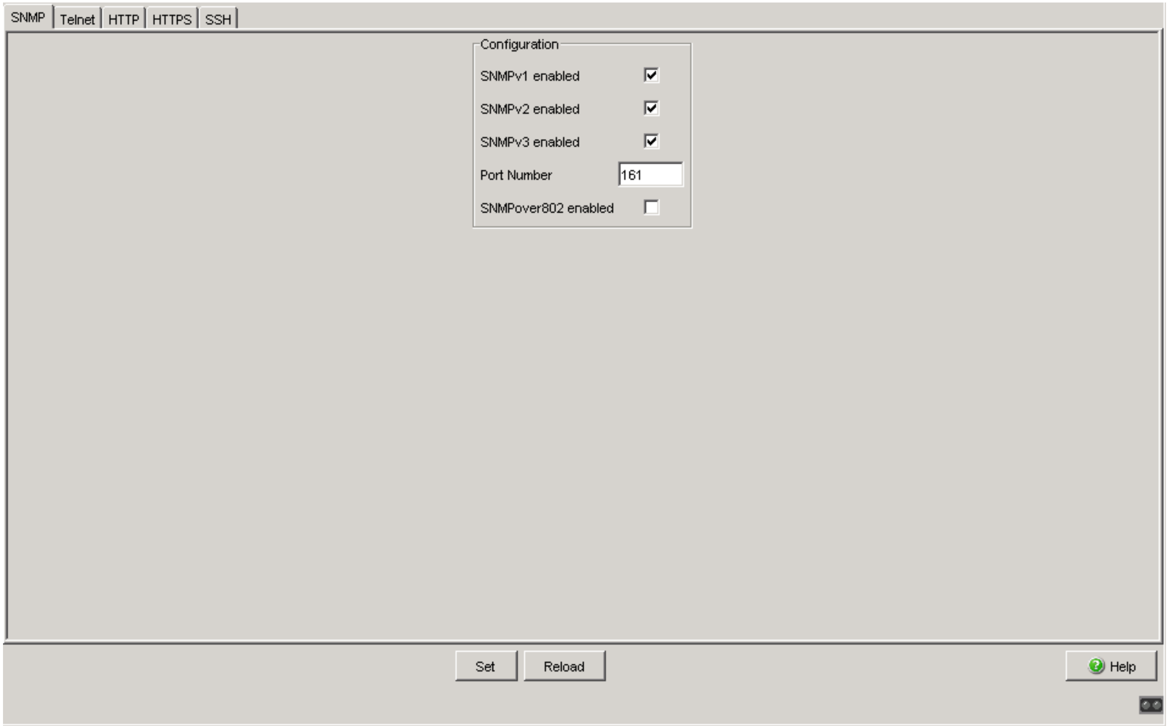
☐ To permanently save the changes, you open the `Basic Settings >` Load/Save dialog and click "Save".

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`snmp community rw <community name>`	Specifies the community for read/write access.
`show snmp community`	Shows the communities that are set up.
`save`	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.



Configuration

SNMPv1 enabled ☑

SNMPv2 enabled ☑

SNMPv3 enabled ☑

Port Number 161

SNMPover802 enabled ☐

Figure 37: 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`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`no snmp access version v1`	Deactivates the SNMPv1 protocol.
`no snmp access version v2`	Deactivates the SNMPv2 protocol.
`show snmp access`	Shows the settings of the SNMP server.
`save`	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.

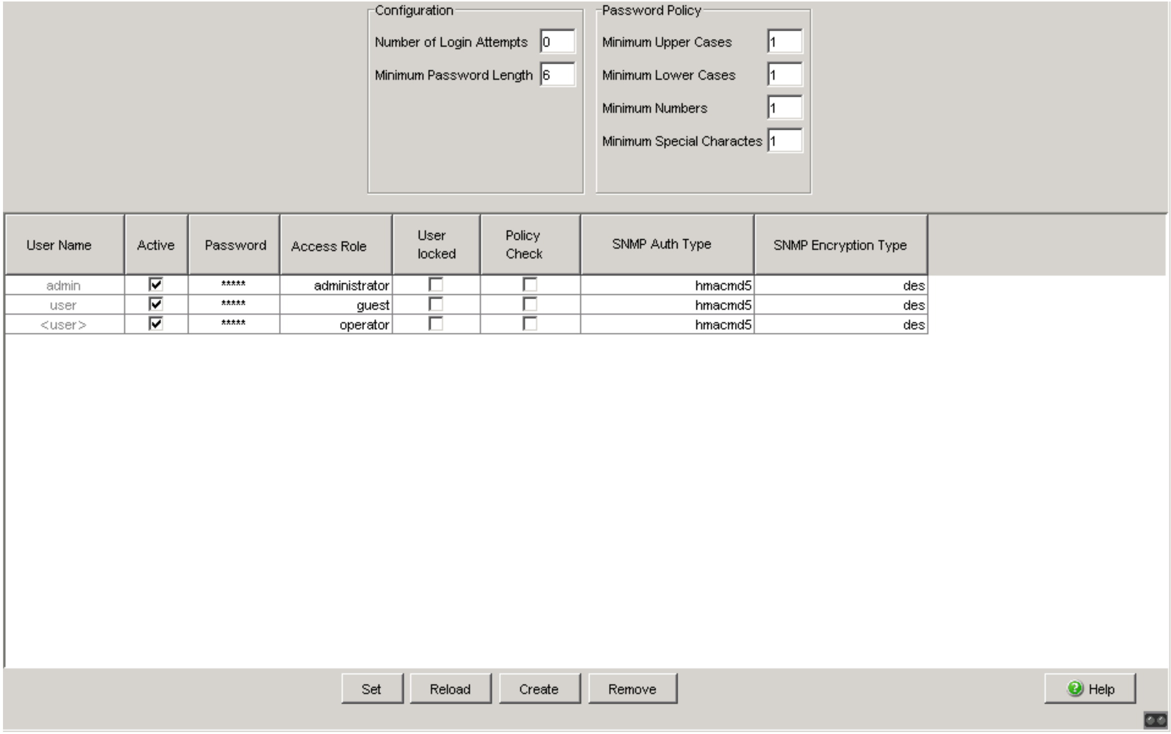
The device allows you to specify the "SNMP Auth Type" and "SNMP Encryption Type" parameters individually in each user account.

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.



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 Charactes: 1

User Name	Active	Password	Access Role	User locked	Policy Check	SNMP Auth Type	SNMP Encryption Type
admin	☑	*****	administrator	□	□	hmacmd5	des
user	☑	*****	guest	□	□	hmacmd5	des
<user>	☑	*****	operator	□	□	hmacmd5	des

Figure 38: `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`	Switch to the privileged EXEC mode.
`configure`	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.

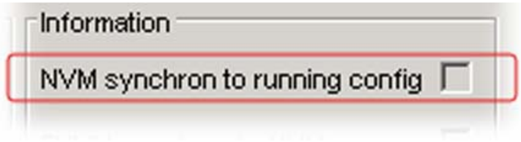
If an external memory is connected, the device generates a copy of the configuration profile on the external memory automatically. The device allows you to deactivate this function.

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`.



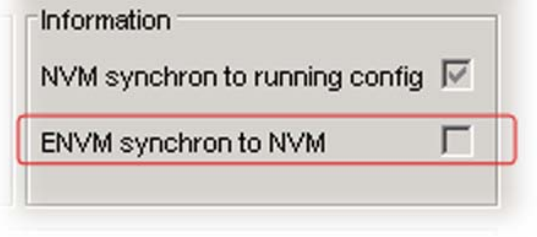
Information

NVM synchron to running config □

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

If the copy in the external memory differs from the configuration profile in the non-volatile memory, you see the difference based on the following criteria:

The checkbox in the `Basic Settings > Load/Save` dialog, "Information" frame is `unmarked`. If the configuration profiles match, the checkbox is `marked`.


Information

NVM synchron to running config ☑

ENVM synchron to NVM □

```
show config status
Configuration Storage sync State
--------------------------------
...
NV to ACA31..................................out of sync
...
```

4.2 Saving settings

Prerequisite: User account with authorization profile `administrator`.

4.2.1 Saving the configuration profile in the device

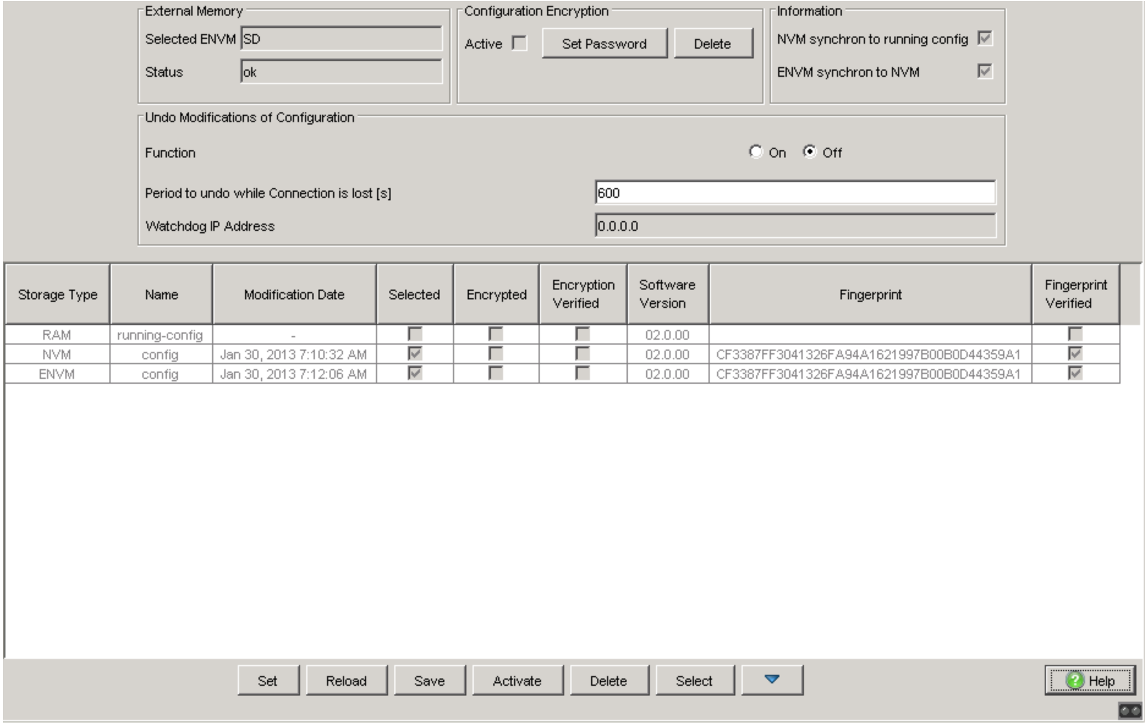
If you change the settings of the device during operation, the device stores the changes in its memory (`RAM`). In order to keep the changes after a reboot, save the configuration profile in non-volatile memory (`NVM`).

■ 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.



External Memory

Selected ENVM: SD

Status: ok

Configuration Encryption

Active □

Information

NVM synchron to running config ☑

ENVM synchron to NVM ☑

Undo Modifications of Configuration

Function: ○ On ● Off

Period to undo while Connection is lost [s]: 600

Watchdog IP Address: 0.0.0.0

Storage Type	Name	Modification Date	Selected	Encrypted	Encryption Verified	Software Version	Fingerprint	Fingerprint Verified
RAM	running-config	-	□	□	□	02.0.00		□
NVM	config	Jan 30, 2013 7:10:32 AM	☑	□	□	02.0.00	CF3387FF3041326FA94A1621997B00B0D44359A1	☑
ENVM	config	Jan 30, 2013 7:12:06 AM	☑	□	□	02.0.00	CF3387FF3041326FA94A1621997B00B0D44359A1	☑

Figure 39: `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.

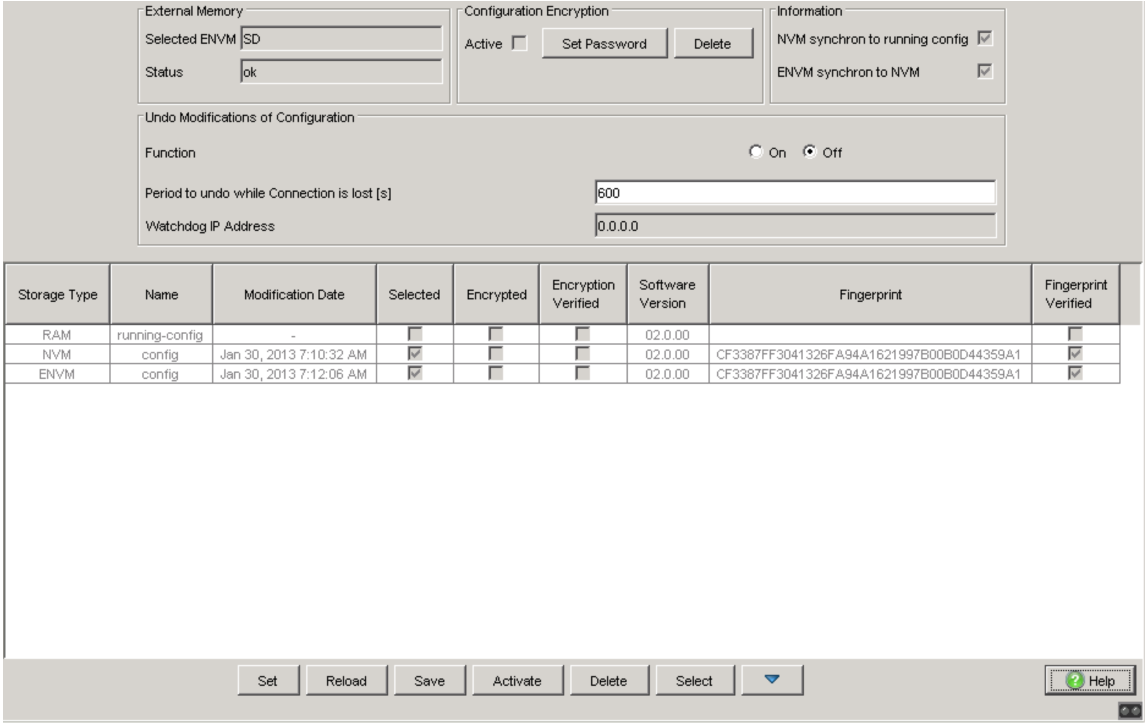
`show config profiles nvm`	Displays the configuration profiles contained in non-volatile memory (`NVM`).
`enable`	Switch to the privileged EXEC mode.
`save`	Saves the settings in the non-volatile memory of the device (`NVM`) in the “selected” configuration profile.

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.



External Memory
Selected ENVM: SD
Status: ok

Configuration Encryption
Active ☐

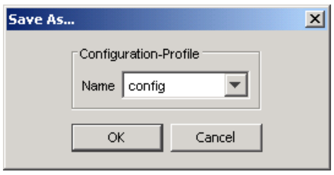
Information
NVM synchron to running config ☑
ENVM synchron to NVM ☑

Undo Modifications of Configuration
Function: ○ On ● Off
Period to undo while Connection is lost [s]: 600
Watchdog IP Address: 0.0.0.0

Storage Type	Name	Modification Date	Selected	Encrypted	Encryption Verified	Software Version	Fingerprint	Fingerprint Verified
RAM	running-config	-	☐	☐	☐	02.0.00		☐
NVM	config	Jan 30, 2013 7:10:32 AM	☑	☐	☐	02.0.00	CF3387FF3041326FA94A1621997B00B0D44359A1	☑
ENVM	config	Jan 30, 2013 7:12:06 AM	☑	☐	☐	02.0.00	CF3387FF3041326FA94A1621997B00B0D44359A1	☑

Figure 40: `Basic Settings > Load/Save` *dialog*

□ Click the ▾ button, then "Save As...".
The dialog shows the "Save As…" window.



Save As...
Configuration-Profile
Name: config

Figure 41: 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".

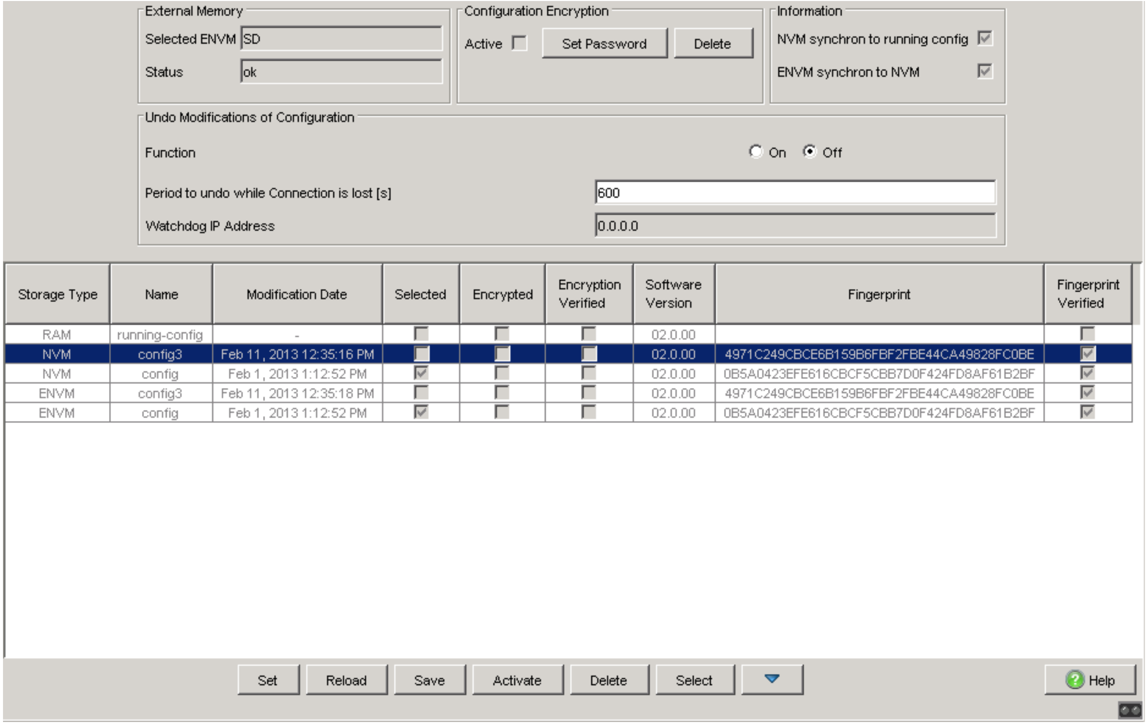
`show config profiles nvm`	Displays the configuration profiles contained in non-volatile memory (`NVM`).
`enable`	Switch to the privileged EXEC mode.
`copy config running-config nvm profile <string>`	Save the current settings in the configuration profile named <string> in non-volatile memory (`NVM`). 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.



External Memory
Selected ENVM: SD
Status: ok

Configuration Encryption
Active □

Information
NVM synchron to running config ☑
ENVM synchron to NVM ☑

Undo Modifications of Configuration
Function: ○ On ● Off
Period to undo while Connection is lost [s]: 600
Watchdog IP Address: 0.0.0.0

Storage Type	Name	Modification Date	Selected	Encrypted	Encryption Verified	Software Version	Fingerprint	Fingerprint Verified
RAM	running-config	-	□	□	□	02.0.00		□
NVM	config3	Feb 11, 2013 12:35:16 PM	□	□	□	02.0.00	4971C249CBCE6B159B6FBF2FBE44CA49828FC0BE	☑
NVM	config	Feb 1, 2013 1:12:52 PM	☑	□	□	02.0.00	0B5A0423EFE616CBCF5CBB7D0F424FD8AF61B2BF	☑
ENVM	config3	Feb 11, 2013 12:35:18 PM	□	□	□	02.0.00	4971C249CBCE6B159B6FBF2FBE44CA49828FC0BE	☑
ENVM	config	Feb 1, 2013 1:12:52 PM	☑	□	□	02.0.00	0B5A0423EFE616CBCF5CBB7D0F424FD8AF61B2BF	☑

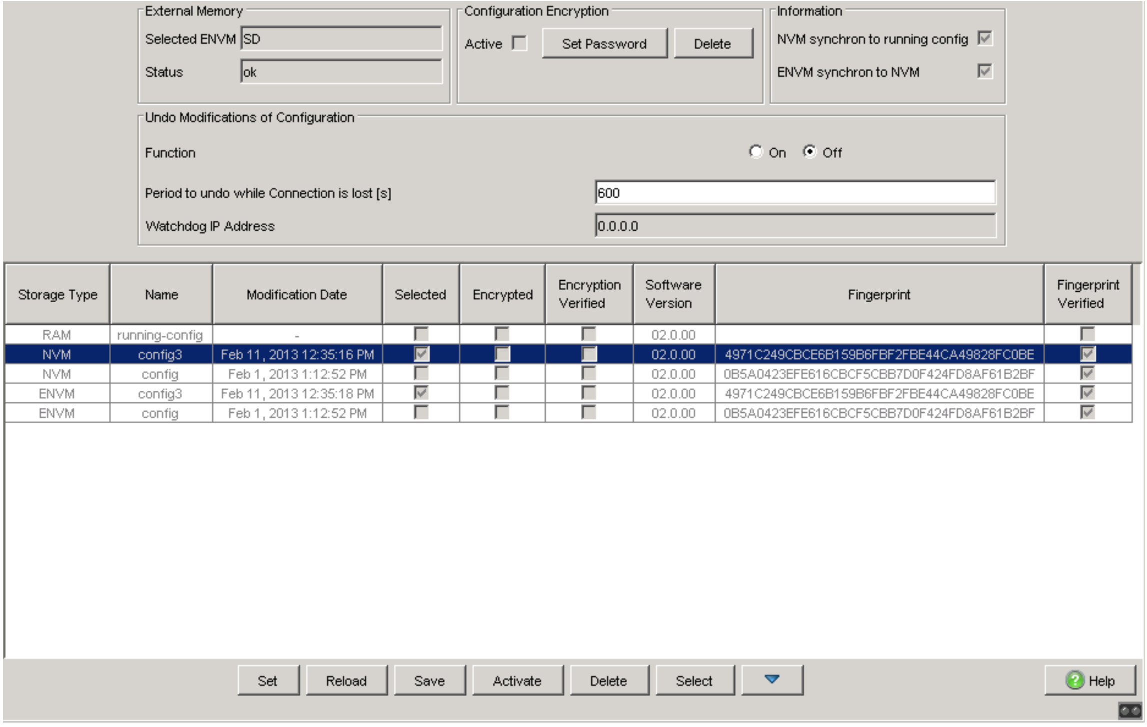
Figure 42: `Basic Settings > Load/Save` *dialog*

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`.



External Memory

Selected ENVM: SD

Status: ok

Configuration Encryption

Active □ | Set Password | Delete

Information

NVM synchron to running config ☑

ENVM synchron to NVM ☑

Undo Modifications of Configuration

Function ○ On ● Off

Period to undo while Connection is lost [s]: 600

Watchdog IP Address: 0.0.0.0

Storage Type	Name	Modification Date	Selected	Encrypted	Encryption Verified	Software Version	Fingerprint	Fingerprint Verified
RAM	running-config	-	□	□	□	02.0.00		□
NVM	config3	Feb 11, 2013 12:35:16 PM	☑	□	□	02.0.00	4971C249CBCE6B159B6FBF2FBE44CA49828FC0BE	☑
NVM	config	Feb 1, 2013 1:12:52 PM	□	□	□	02.0.00	0B5A0423EFE616CBCF5CBB7D0F424FD8AF61B2BF	☑
ENVM	config3	Feb 11, 2013 12:35:18 PM	☑	□	□	02.0.00	4971C249CBCE6B159B6FBF2FBE44CA49828FC0BE	☑
ENVM	config	Feb 1, 2013 1:12:52 PM	□	□	□	02.0.00	0B5A0423EFE616CBCF5CBB7D0F424FD8AF61B2BF	☑

Figure 43: `Basic Settings > Load/Save` *dialog*

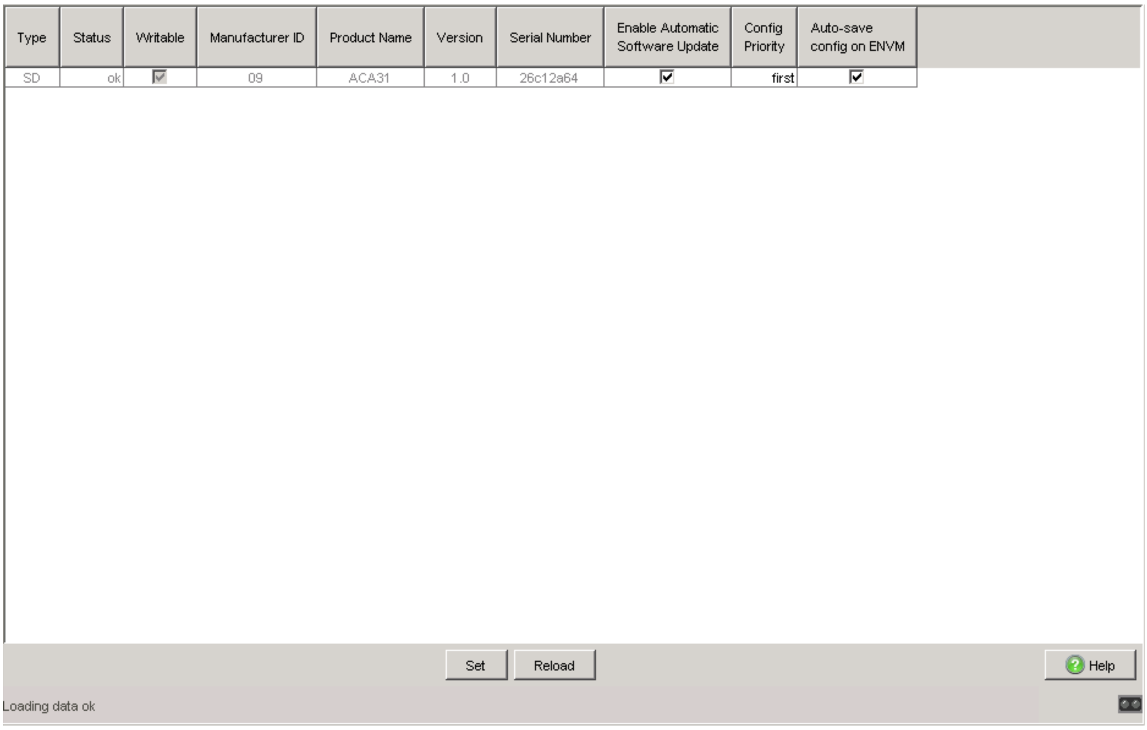
`enable`	Switch to the privileged EXEC mode.
`show config profiles nvm`	Displays the configuration profiles contained in non-volatile memory (`NVM`).
`configure`	Switch to the Configuration mode.
`config profile select nvm 1`	Identifier of the configuration profile. Take note of the adjacent name of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

4.2.2 Saving the configuration profile in external memory

When you save a configuration profile, the device automatically creates a copy in external memory when the external memory is connected. In the delivery state of the device, this function is enabled. You have the following option of enabling or disabling this function.

Perform the following work steps:

□ Open the `Basic Settings > External Memory` dialog.



Type	Status	Writable	Manufacturer ID	Product Name	Version	Serial Number	Enable Automatic Software Update	Config Priority	Auto-save config on ENVM
SD	ok	☑	09	ACA31	1.0	26c12a64	☑	first	☑

Loading data ok

Figure 44: `Basic Settings > External Memory` *dialog*

□ In order to cause the device to automatically generate a copy in external memory during the saving process, select the checkbox in the "Auto-save config on ENVM" column.

□ To turn off the function, remove the checkmark from the checkbox in the "Auto-save config on ENVM" column.

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

□ 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.
`config envm config-save sd|usb`	Enable the function. When you save a configuration profile, the device creates a copy in the external memory. `sd` = External SD memory `usb` = External USB memory
`no config envm config-save sd|usb`	Disable the function. The device does not create a copy in the external memory. `sd` = External SD memory `usb` = External USB memory
`save`	Saves the settings in the non-volatile memory of the device (`NVM`) in the “selected” configuration profile.

4.2.3 Exporting a configuration profile

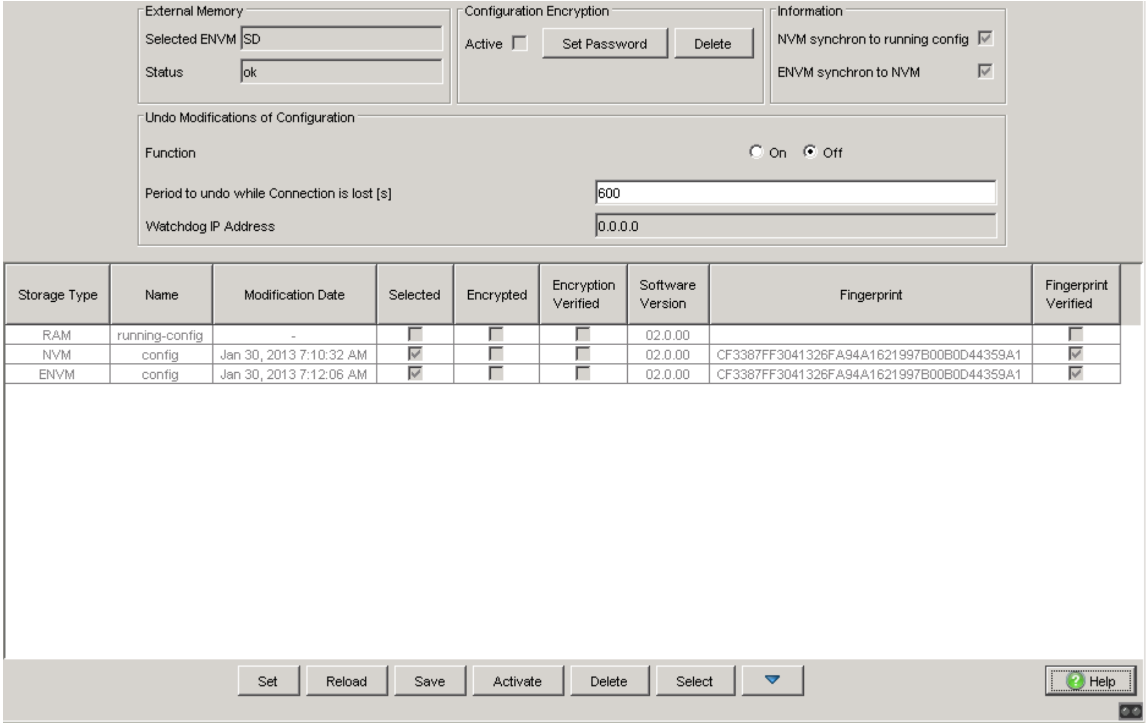
The device offers you the option of saving a configuration profile to a server as an XML file. If you use the graphical user interface, you have the option to save the XML file directly to your PC.

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.



External Memory
Selected ENVM: SD
Status: ok

Configuration Encryption
Active ☐

Information
NVM synchron to running config ☑
ENVM synchron to NVM ☑

Undo Modifications of Configuration
Function: ○ On ● Off
Period to undo while Connection is lost [s]: 600
Watchdog IP Address: 0.0.0.0

Storage Type	Name	Modification Date	Selected	Encrypted	Encryption Verified	Software Version	Fingerprint	Fingerprint Verified
RAM	running-config	-	☐	☐	☐	02.0.00		☐
NVM	config	Jan 30, 2013 7:10:32 AM	☑	☐	☐	02.0.00	CF3387FF3041326FA94A1621997B00B0D44359A1	☑
ENVM	config	Jan 30, 2013 7:12:06 AM	☑	☐	☐	02.0.00	CF3387FF3041326FA94A1621997B00B0D44359A1	☑

Figure 45: `Basic Settings > Load/Save` dialog

□ Select the line of the desired configuration profile.

□ Click the ▼ button, then "Export...".
The dialog displays the "Export..." window.

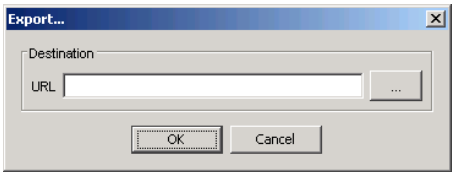


Figure 46: Export... window in the `Basic Settings > Load/Save` dialog

□ 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.

`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 remote tftp://<IP-Adresse>/<Pfad>/<Dateiname>`	Save the configuration profile in memory (`RAM`) on a TFTP server.
`copy config nvm remote tftp://<IP-Adresse>/<Pfad>/<Dateiname>`	Save the selected configuration profile in non-volatile memory (`NVM`) on a TFTP server.
`copy config nvm profile config3 remote tftp://<IP-Adresse>/<Pfad>/<Dateiname>`	Save the configuration profile `config3` 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.

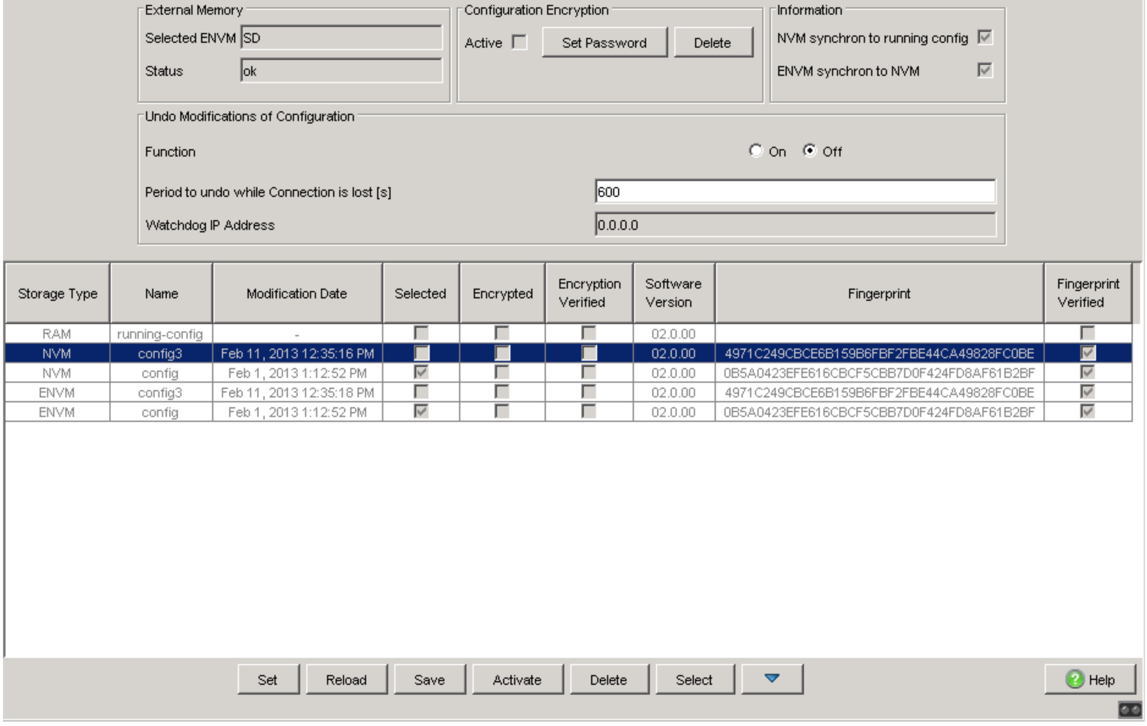
Prerequisite: User account with authorization profile `administrator`.

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.



External Memory
Selected ENVM: SD
Status: ok

Configuration Encryption
Active ☐

Information
NVM synchron to running config ☑
ENVM synchron to NVM ☑

Undo Modifications of Configuration
Function: ○ On ● Off
Period to undo while Connection is lost [s]: 600
Watchdog IP Address: 0.0.0.0

Storage Type	Name	Modification Date	Selected	Encrypted	Encryption Verified	Software Version	Fingerprint	Fingerprint Verified
RAM	running-config	-	☐	☐	☐	02.0.00		☐
NVM	config3	Feb 11, 2013 12:35:16 PM	☐	☐	☐	02.0.00	4971C249CBCE6B159B6FBF2FBE44CA49828FC0BE	☑
NVM	config	Feb 1, 2013 1:12:52 PM	☑	☐	☐	02.0.00	0B5A0423EFE616CBCF5CBB7D0F424FD8AF61B2BF	☑
ENVM	config3	Feb 11, 2013 12:35:18 PM	☐	☐	☐	02.0.00	4971C249CBCE6B159B6FBF2FBE44CA49828FC0BE	☑
ENVM	config	Feb 1, 2013 1:12:52 PM	☑	☐	☐	02.0.00	0B5A0423EFE616CBCF5CBB7D0F424FD8AF61B2BF	☑

Figure 47: `Basic Settings > Load/Save` *dialog*

☐ Select the line of the desired configuration profile.

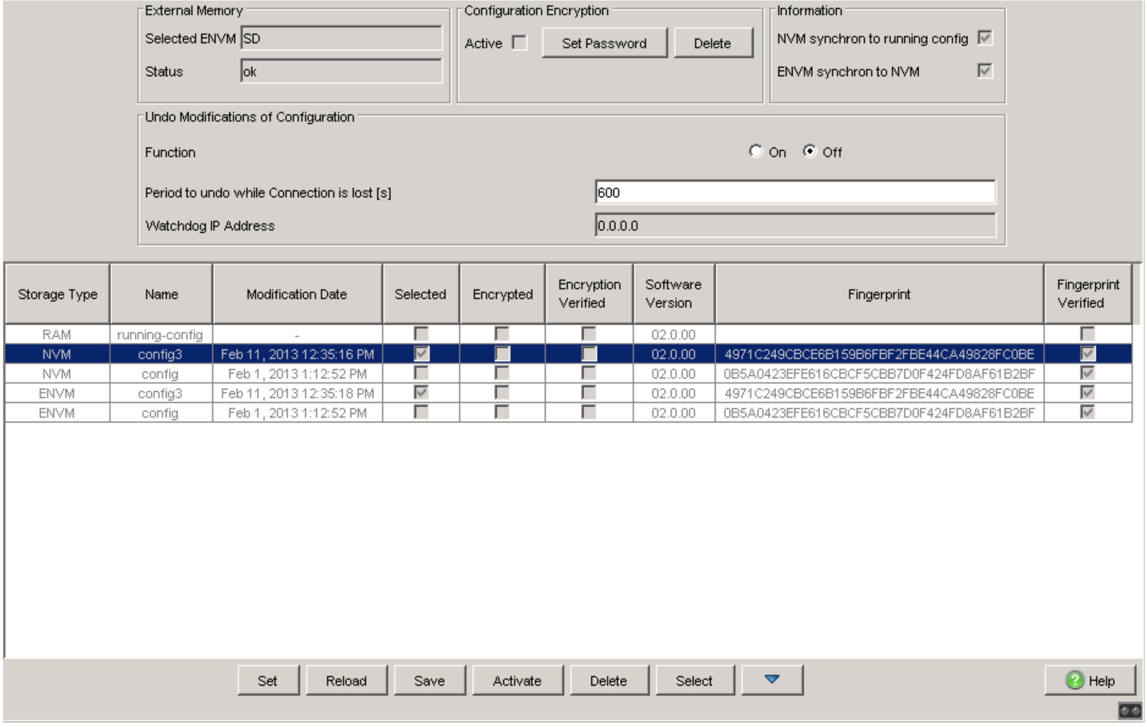
☐ Click the "Activate" button.

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`.



External Memory

Selected ENVM: SD

Status: ok

Configuration Encryption

Active □ Set Password Delete

Information

NVM synchron to running config ☑

ENVM synchron to NVM ☑

Undo Modifications of Configuration

Function ○ On ● Off

Period to undo while Connection is lost [s]: 600

Watchdog IP Address: 0.0.0.0

Storage Type	Name	Modification Date	Selected	Encrypted	Encryption Verified	Software Version	Fingerprint	Fingerprint Verified
RAM	running-config	-	□	□	□	02.0.00		□
NVM	config3	Feb 11, 2013 12:35:16 PM	☑	□	□	02.0.00	4971C249CBCE6B159B6FBF2FBE44CA49828FC0BE	☑
NVM	config	Feb 1, 2013 1:12:52 PM	□	□	□	02.0.00	0B5A0423EFE616CBCF5CBB7D0F424FD8AF61B2BF	☑
ENVM	config3	Feb 11, 2013 12:35:18 PM	☑	□	□	02.0.00	4971C249CBCE6B159B6FBF2FBE44CA49828FC0BE	☑
ENVM	config	Feb 1, 2013 1:12:52 PM	□	□	□	02.0.00	0B5A0423EFE616CBCF5CBB7D0F424FD8AF61B2BF	☑

Figure 48: `Basic Settings > Load/Save` *dialog*

`show config profiles nvm`	Displays the configuration profiles contained in non-volatile memory (`NVM`).
`enable`	Switch to the privileged EXEC mode.
`copy config nvm profile config3 running-config`	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 Loading the configuration profile from the external memory

If an external memory is connected, the device loads a configuration profile from the external memory upon restart automatically. The device allows you to save these settings in a configuration profile in non-volatile memory.

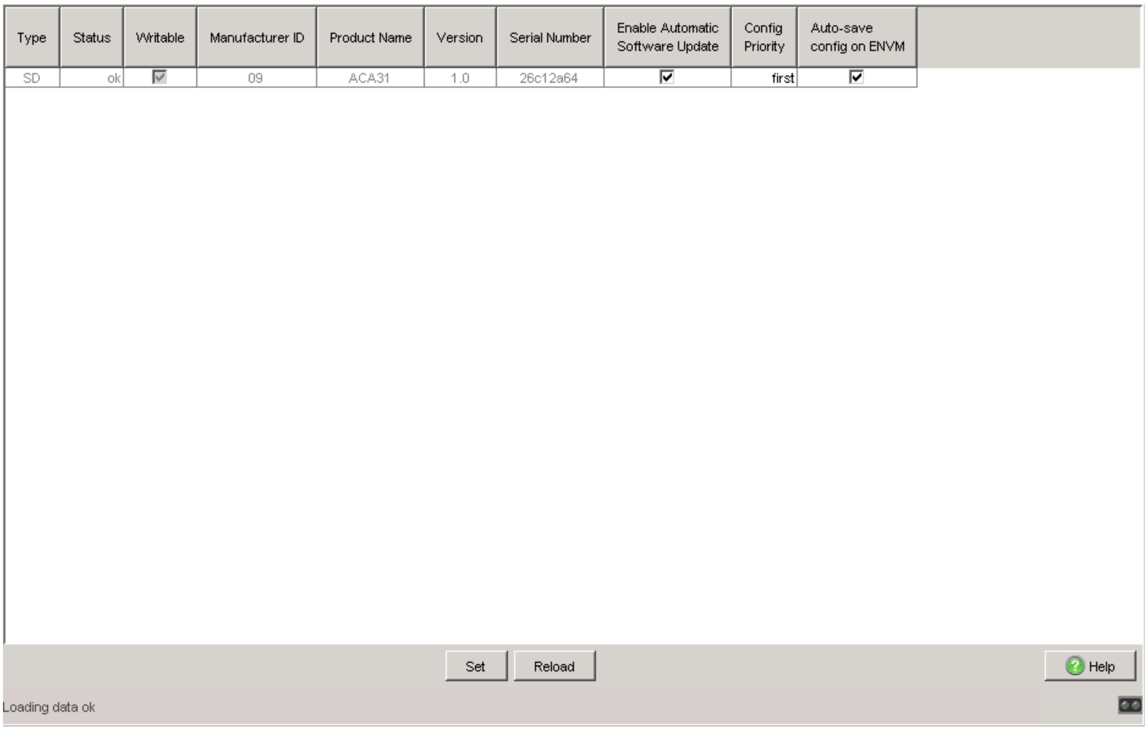
If the external memory contains the configuration profile of an identical device, this allows you to transfer the settings from one device to another.

Perform the following work steps:

□ Verify that the device loads a configuration profile from the external memory upon restart.

In the state on delivery of the device, this function is turned on. If the function is turned off, turn it on again as follows:

□ Open the `Basic Settings > External Memory` dialog.



Type	Status	Writable	Manufacturer ID	Product Name	Version	Serial Number	Enable Automatic Software Update	Config Priority	Auto-save config on ENVM
SD	ok	☑	09	ACA31	1.0	26c12a64	☑	first	☑

Loading data ok

Figure 49: `Basic Settings > External Memory` dialog

□ In the "Config Priority" column, select the value `first`.

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

☐ 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.
`config envm load-priority sd|usb first`	Enable the function. Upon reboot, the device loads a configuration profile from the external memory. `sd` = External SD memory `usb` = External USB memory
`show config envm settings`	Displays the settings of the external memory (`ENVM`).

```
Type   Status      Auto Update Save Config Config Load Prio
------ ----------- ----------- ----------- ----------------
sd     ok          [x]         [x]         first
usb    ok          [x]         [x]         second
```

☐ Save the settings of the device in a configuration profile in non-volatile memory.
See “Saving the configuration profile in the device” on page 90.

The device allows you via CLI to copy the settings from the external memory directly into non-volatile memory.

`show config profiles nvm`	Displays the configuration profiles contained in non-volatile memory (`NVM`).
`enable`	Switch to the privileged EXEC mode.
`copy config envm profile config3 nvm`	Copy the configuration profile `config3` from the external memory (`ENVM`) to the non-volatile memory (`NVM`).

4.3.3 Importing a configuration profile

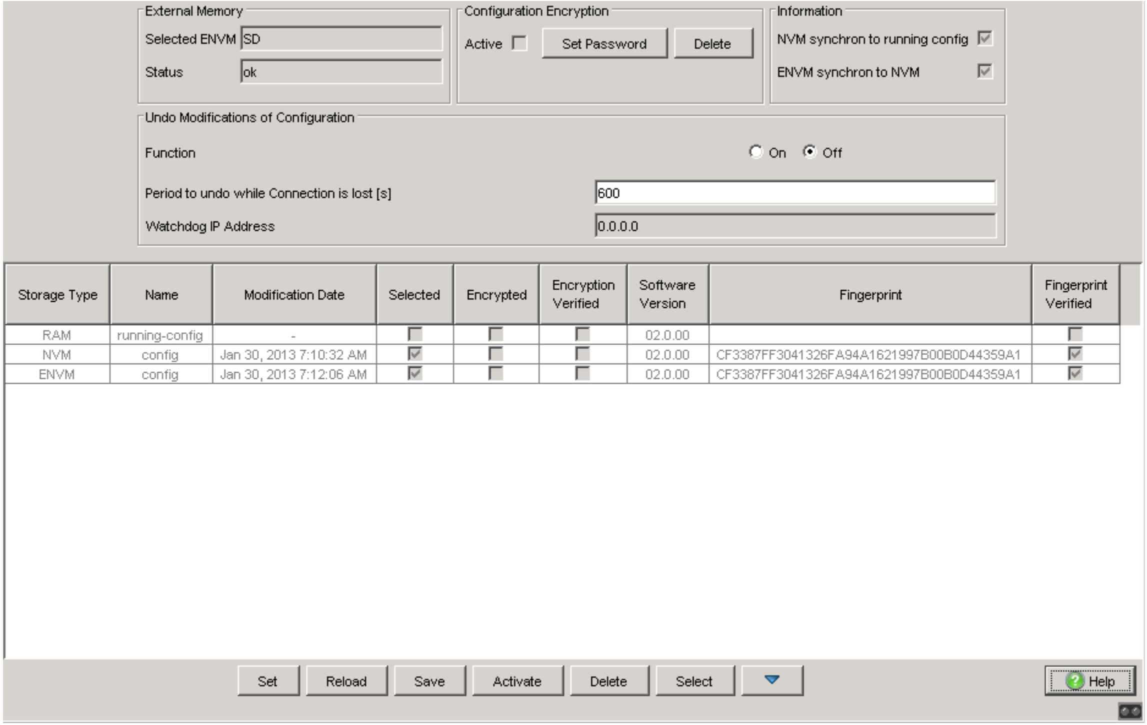
The device allows you to import from a server a configuration profile saved as an XML file. If you use the graphical user interface, you have the option to import the XML file directly from your PC.

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.



External Memory
Selected ENVM: SD
Status: ok

Configuration Encryption
Active □

Information
NVM synchron to running config ☑
ENVM synchron to NVM ☑

Undo Modifications of Configuration
Function: ○ On ● Off
Period to undo while Connection is lost [s]: 600
Watchdog IP Address: 0.0.0.0

Storage Type	Name	Modification Date	Selected	Encrypted	Encryption Verified	Software Version	Fingerprint	Fingerprint Verified
RAM	running-config	-	□	□	□	02.0.00		□
NVM	config	Jan 30, 2013 7:10:32 AM	☑	□	□	02.0.00	CF3387FF3041326FA94A1621997B00B0D44359A1	☑
ENVM	config	Jan 30, 2013 7:12:06 AM	☑	□	□	02.0.00	CF3387FF3041326FA94A1621997B00B0D44359A1	☑

Figure 50: `Basic Settings > Load/Save` *dialog*

□ Click the ▼ button, then "Import…".
The dialog shows the "Import…" window.

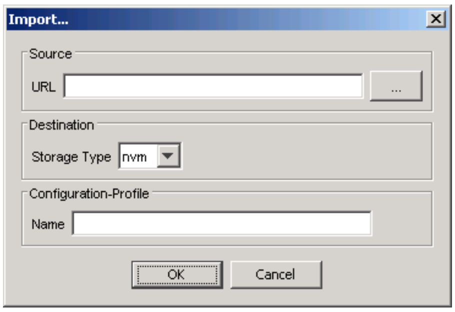


Figure 51: Import... window in the `Basic Settings > Load/Save` dialog

□ 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`	Switch to the privileged EXEC mode.
`copy config remote tftp://<IP-Adresse>/<Pfad>/<Dateiname> running-config`	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.

If an external memory is connected, the device also deletes the configuration profiles saved on the external memory.

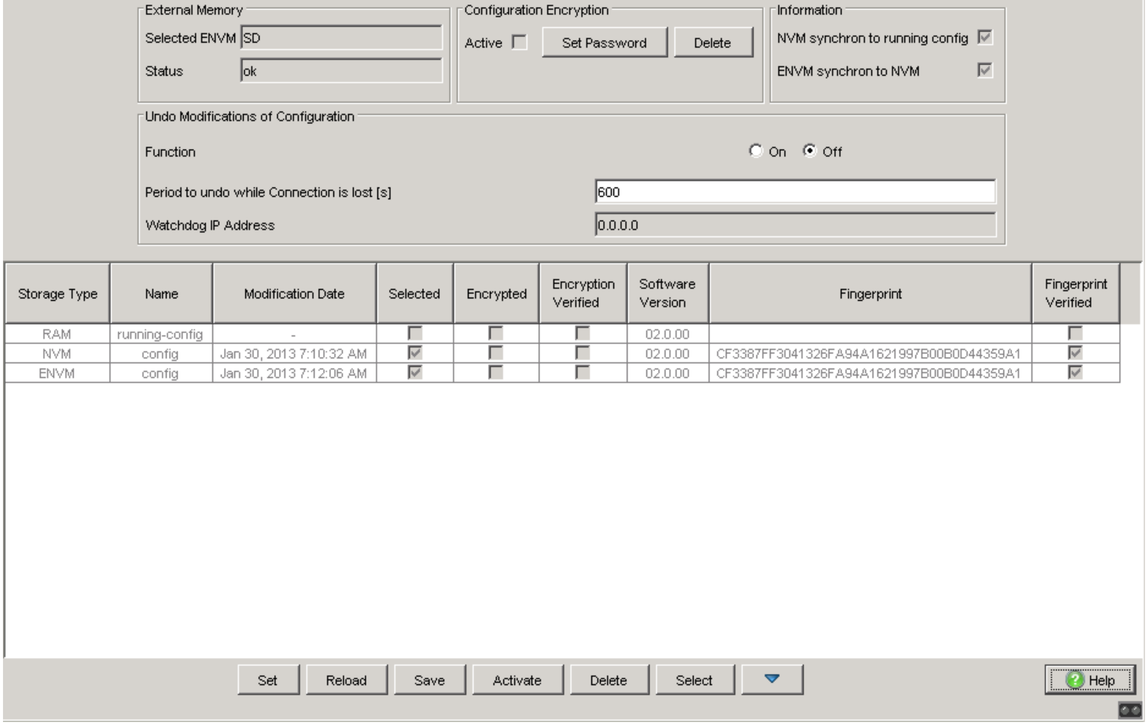
The device then reboots and loads the factory settings.

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.


External Memory
Selected ENVM: SD
Status: ok

Configuration Encryption
Active ☐

Information
NVM synchron to running config ☑
ENVM synchron to NVM ☑

Undo Modifications of Configuration
Function: ○ On ● Off
Period to undo while Connection is lost [s]: 600
Watchdog IP Address: 0.0.0.0

Storage Type	Name	Modification Date	Selected	Encrypted	Encryption Verified	Software Version	Fingerprint	Fingerprint Verified
RAM	running-config	-	☐	☐	☐	02.0.00		☐
NVM	config	Jan 30, 2013 7:10:32 AM	☑	☐	☐	02.0.00	CF3387FF3041326FA94A1621997B00B0D44359A1	☑
ENVM	config	Jan 30, 2013 7:12:06 AM	☑	☐	☐	02.0.00	CF3387FF3041326FA94A1621997B00B0D44359A1	☑

Figure 52: `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.
If an external memory is connected, the device also deletes the configuration profiles saved on the external memory.
After a brief period, the device restarts and loads the delivery settings.

`enable`	Switch to the privileged EXEC mode.
`clear factory`	Deleting the configuration profiles in the volatile memory (`RAM`) and in non-volatile memory (`NVM`). If an external memory is connected, the device also deletes the configuration profiles saved on the external memory. 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 Loading Software Updates

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

The device gives you the following options for updating the device software:

- Software update from the PC
- Software update from a server
- Software update from the external memory
- Loading an older software

Note: The device settings are kept after updating the device software.

You see the version of the installed device software in the login window of the graphical user interface. If you are already logged in, perform the following work steps to display the version of the installed software.

□ Open the `Basic Settings > Software` dialog.

The field "Running Version" displays the version number and creation date of the device software that the device loaded during the last restart and is currently running.

`enable`	Change to the Privileged EXEC mode.
`show system info`	Displays the system information such as the version number and creation date of the device software that the device loaded during the last restart and is currently running.

5.1 Software update from the PC

The prerequisite is that the image file of the device software is saved on a data carrier which is accessible from your PC.

Perform the following work steps:

☐ Navigate to the folder where the image file of the device software is saved.

☐ Open the `Basic Settings > Software` dialog.

☐ Drag the image file of the device software into the field "File" in the "Software Update" frame.
Alternatively, click in the "Software Update" frame the " …" button and select the image file.

☐ To start the update procedure, click the "Update" button.
The device copies the currently running device software into the backup memory.
As soon as the update procedure is completed successfully, the device displays the message "Firmware successfully loaded onto the device".
Upon restart, the device loads the installed device software.

5.2 Software update from a server

To update the software using TFTP, SFTP or SCP you need a server on which the image file of the device software is saved.

Perform the following work steps:

- □ Open the `Basic Settings > Software` dialog.
- □ Enter in the "File" field in the "Software Update" frame the URL for the image file in the following form:
  - ▶ When the image file is saved on a TFTP server:
    `sftp://<IP address>/<path>/<image_file_name>.bin`
  - ▶ When the image file is saved on a SCP or SFTP server:
    `scp://` or `sftp://<IP address>/<path>/<image_file_name>.bin`
    `scp://` or
    `sftp://<user>:<password>@<IP address>/<path>/<image file name>.bin`
    If you enter the URL without the user and password, the device displays the window "Authentication". There you enter "Username" and "Password" to login to the server.
- □ To start the update procedure, click the "Update" button.
  The device copies the currently running device software into the backup memory.
  As soon as the update procedure is completed successfully, the device displays the message "Firmware successfully loaded onto the device".
  Upon restart, the device loads the installed device software.

`enable`	Change to the Privileged EXEC mode.
`copy firmware remote tftp://10.0.1.159/product.bin system`	Transfer the “product.bin” file to the device from the TFTP server with the IP address 10.0.1.159.

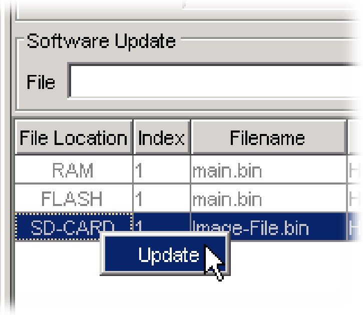
5.3 Software update from the external memory

5.3.1 Manually—initiated by the administrator

The device allows you to update the device software with just a few mouse clicks. The prerequisite is that the image file of the device software is located in the external memory.

Perform the following work steps:

- □ Open the `Basic Settings > Software` dialog.
- □ In the table, mark the row which displays the name of the desired image file on the external memory.
- □ Right-click to display the context menu.
- □ To start the update procedure, click in the context menu the "Update" entry.



File Location	Index	Filename
RAM	1	main.bin
FLASH	1	main.bin
SD-CARD	1	Image-File.bin

The device copies the currently running device software into the backup memory.
As soon as the update procedure is completed successfully, the device displays the message "Firmware successfully loaded onto the device".
Upon restart, the device loads the installed device software.

5.3.2 Automatically—initiated by the device

During a restart the device updates the device software automatically when the following files are located in the external memory:

▶ the image file of the device software
▶ a text file “startup.txt” with the content
`autoUpdate=<image_file_name>.bin`

Prerequisite is that in the `Basic Settings > External Memory` dialog, row "Enable Automatic Software Update" you mark the checkbox. This is the default setting on the device.

Perform the following work steps:

☐ Copy the image file of the new device software into the main directory of the external memory. Use an image file suitable for the device exclusively.
☐ Create a text file “startup.txt” in the main directory of the external memory.
☐ Open the “startup.txt” file in the text editor and add the following line:
`autoUpdate=<image_file_name>.bin`
☐ Install the external memory on the device.
☐ Restart the device.
During the booting process, the device checks automatically the following criteria:
– Is an external memory connected?
– Is a “startup.txt” file in the main directory of the external memory?
– Does the image file exist which is specified in the “startup.txt” file?
– Is the software version of the image file more recent than the software currently running on the device?
If the criteria are fulfilled, the device starts the update procedure.
The device copies the currently running device software into the backup memory.
As soon as the update procedure is completed successfully, the device reboots automatically and loads the new software version.

Check the result of the update procedure. The log file in the `Diagnostics >` Report `> System Log` dialog contains one of the following messages:

▶ `S_watson_AUTOMATIC_SWUPDATE_SUCCESS`
Software update completed successfully
▶ `S_watson_AUTOMATIC_SWUPDATE_ABORTED`
Software update aborted

- `S_watson_AUTOMATIC_SWUPDATE_ABORTED_WRONG_FILE`
  Software update aborted due to wrong image file
- `S_watson_AUTOMATIC_SWUPDATE_ABORTED_SAVING_FILE`
  Software update aborted due to failed saving of the image file to the device

5.4 Loading an older software

The device allows you to replace the device software with an older version. The basic settings on the device are kept after replacing the device software.

Note: The settings for functions which are available in the newer device software version exclusively are lost.

If you intend to downgrade to the software version HiOS 2.x.xx, note the the following information:

Using an up-to-date software version, the device saves the settings in a compressed configuration profile. When booting with the above mentioned software version, the device is able to read uncompressed configuration profiles exclusively. If upon booting solely a compressed configuration profile is available, the device boots applying the delivery settings. The settings in the compressed configuration profile are then lost.

To save the configuration profile which is compatible with the software version mentioned above, you proceed as follows:

▶ Before downgrading

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

□ Click the ▾ and "Export..."buttons to export the configuration profile as an unencrypted XML file.

▶ After downgrading

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

□ Click the ▾ and "Import..."buttons to import the configuration profile.

6 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.

6.1 Basic settings

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

6.1.1 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`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`clock set <YYYY-MM-DD> <HH:MM:SS>`	Set the system time of the device.
`clock timezone offset <-780..840>`	Enter the time difference between the local time and the received UTC time in minutes.
`save`	Saves the settings in the non-volatile memory of the device (`NVM`) in the “selected” configuration profile.

6.1.2 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`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`clock summer-time mode <disable|recurring|eu|usa>`	Configure the automatic daylight saving time changeover: turn on or off or activate with a profile.
`clock summer-time recurring start`	Enter the start time for the changeover.
`clock summer-time recurring end`	Enter the end time for the changeover.
`save`	Saves the settings in the non-volatile memory of the device (`NVM`) in the “selected” configuration profile.

6.2 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.

6.2.1 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.

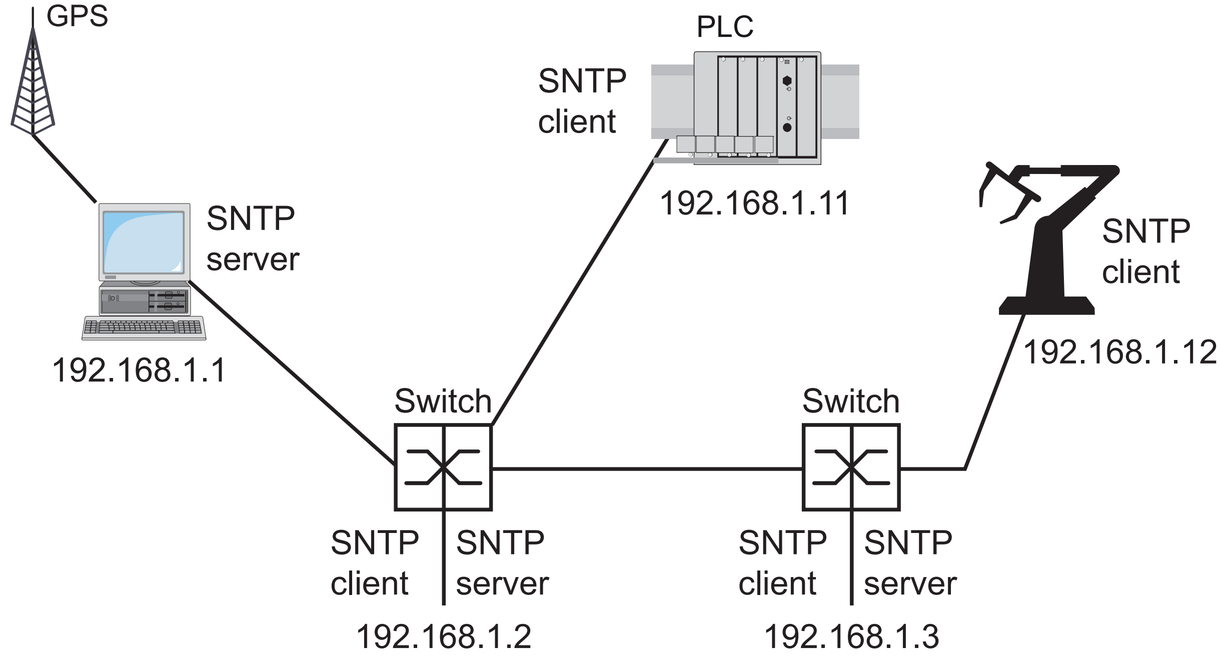


Figure 53: Example of SNTP cascade

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.

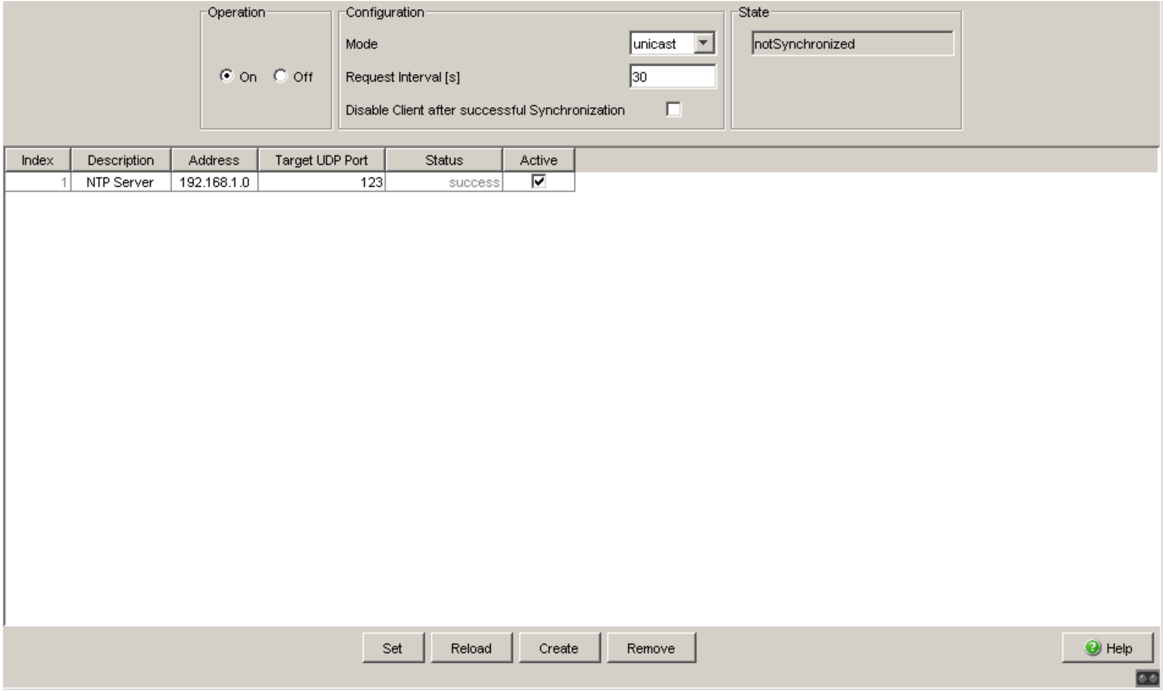
□ If no reference time source is available to you, determine a device with an SNTP server as a reference time source. Adjust its system time at regular intervals.

6.2.2 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.



Operation

● On ○ Off

Configuration

Mode: unicast

Request Interval [s]: 30

Disable Client after successful Synchronization □

State

notSynchronized

Index	Description	Address	Target UDP Port	Status	Active
1	NTP Server	192.168.1.0	123	success	☑

Figure 54: `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

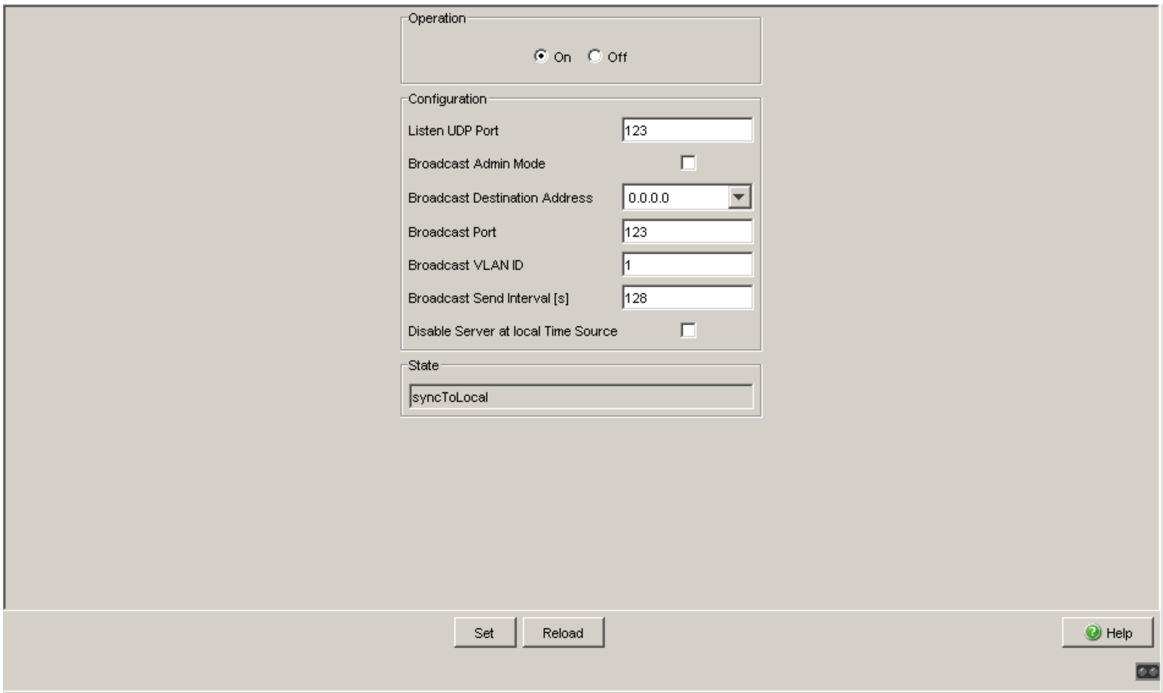
Table 7: SNTP client settings for the example

6.2.3 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.



Operation

● On ○ Off

Configuration

Listen UDP Port	123
Broadcast Admin Mode	□
Broadcast Destination Address	0.0.0.0
Broadcast Port	123
Broadcast VLAN ID	1
Broadcast Send Interval [s]	128
Disable Server at local Time Source	□

State

syncToLocal

Figure 55: `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

6.3 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.

6.3.1 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).

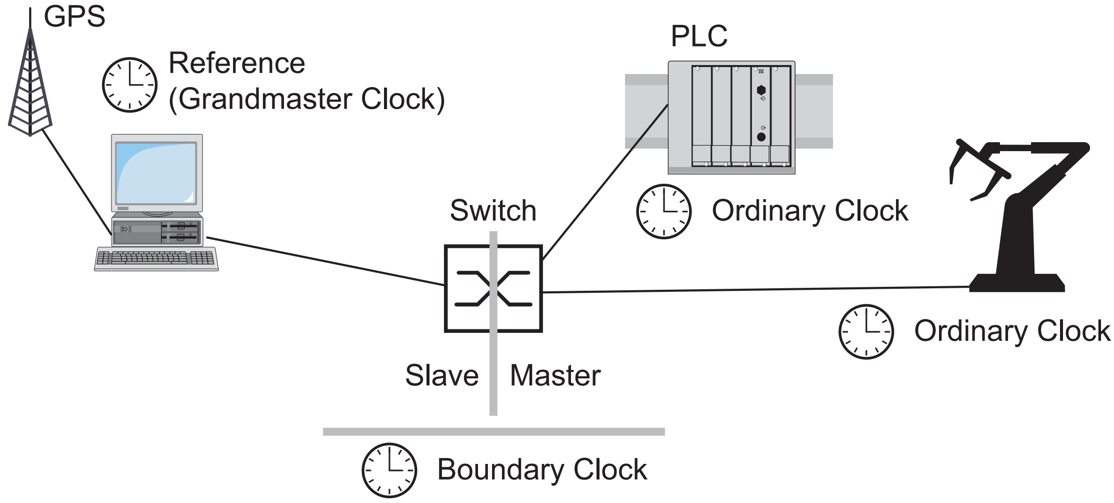


Figure 56: Position of the boundary clock in a network

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.

6.3.2 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.

6.3.3 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.

6.3.4 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.

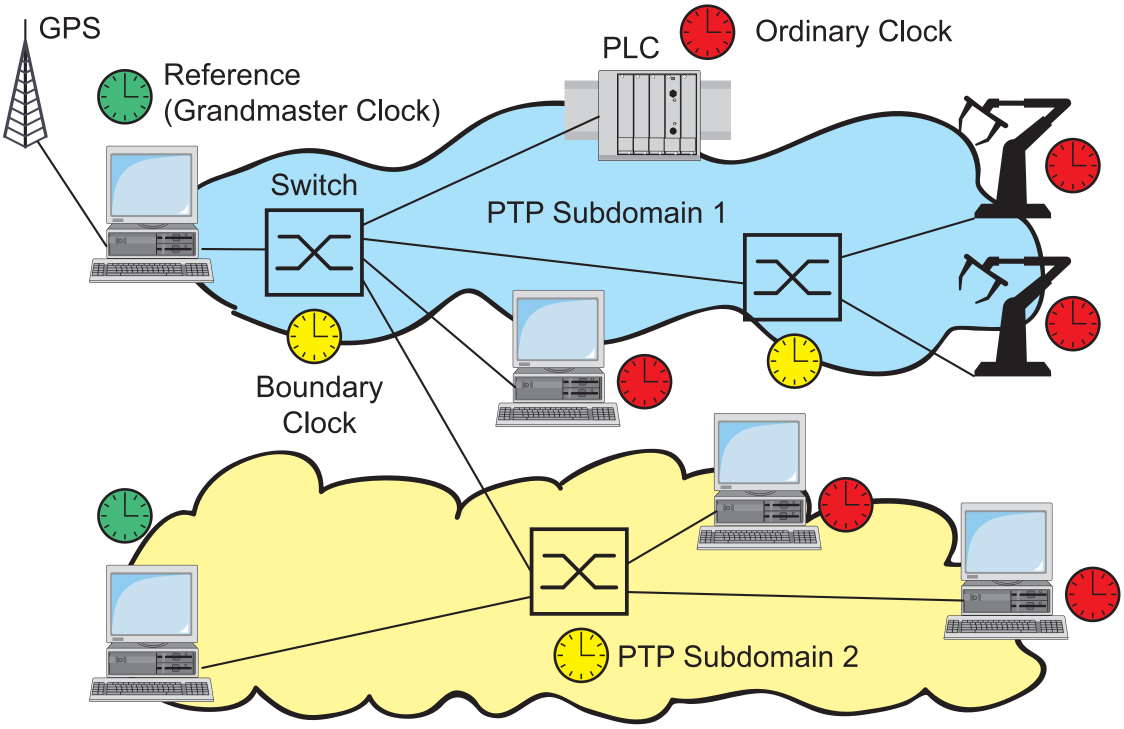


Figure 57: Example of PTP domains

6.3.5 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.

7 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

7.1 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.

7.1.1 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.

7.1.2 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).

7.1.3 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.

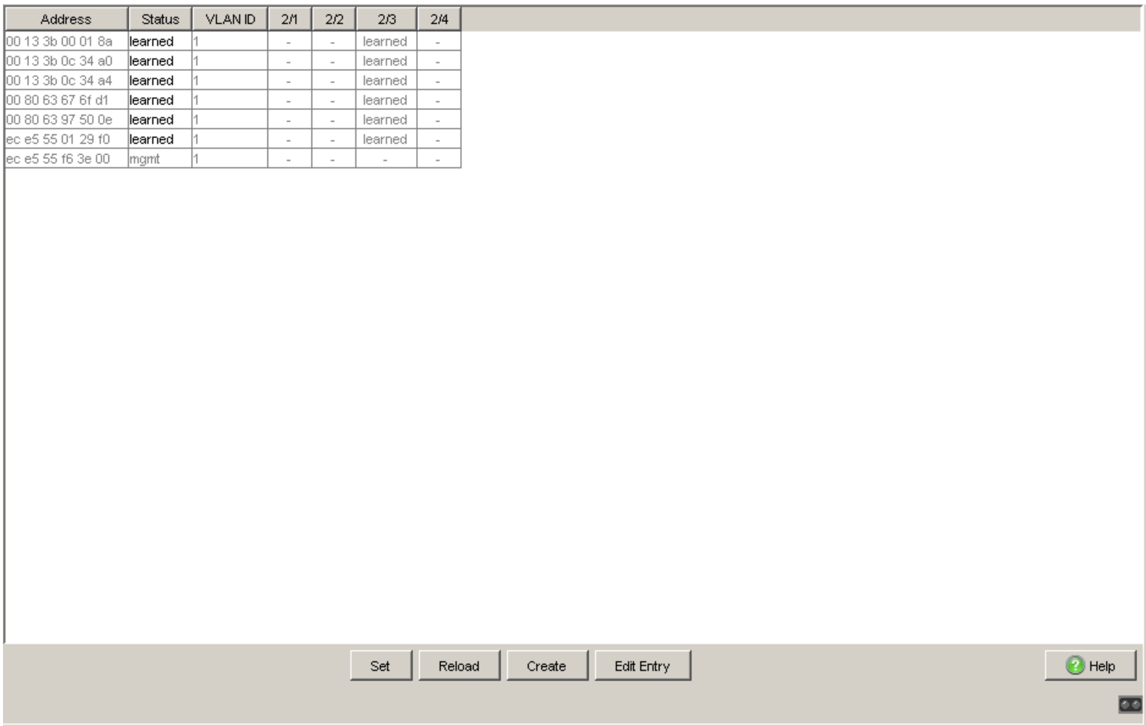
You manage the static address entries in the graphical user interface (GUI) or in the CLI.

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 f0	learned	1	-	-	learned	-
ec e5 55 f6 3e 00	mgmt	1	-	-	-	-

Figure 58: `Switching > Filter for MAC Addresses` *dialog*

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

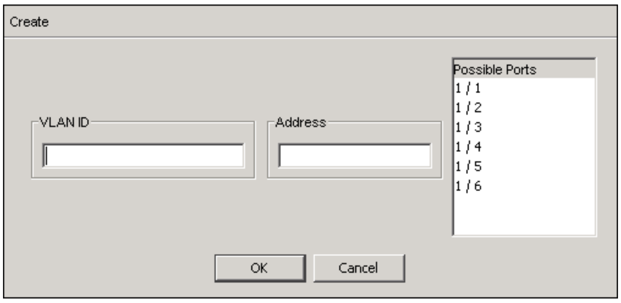


Figure 59: Create window in the `Switching > Filter for MAC Addresses` *dialog*

□ 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.

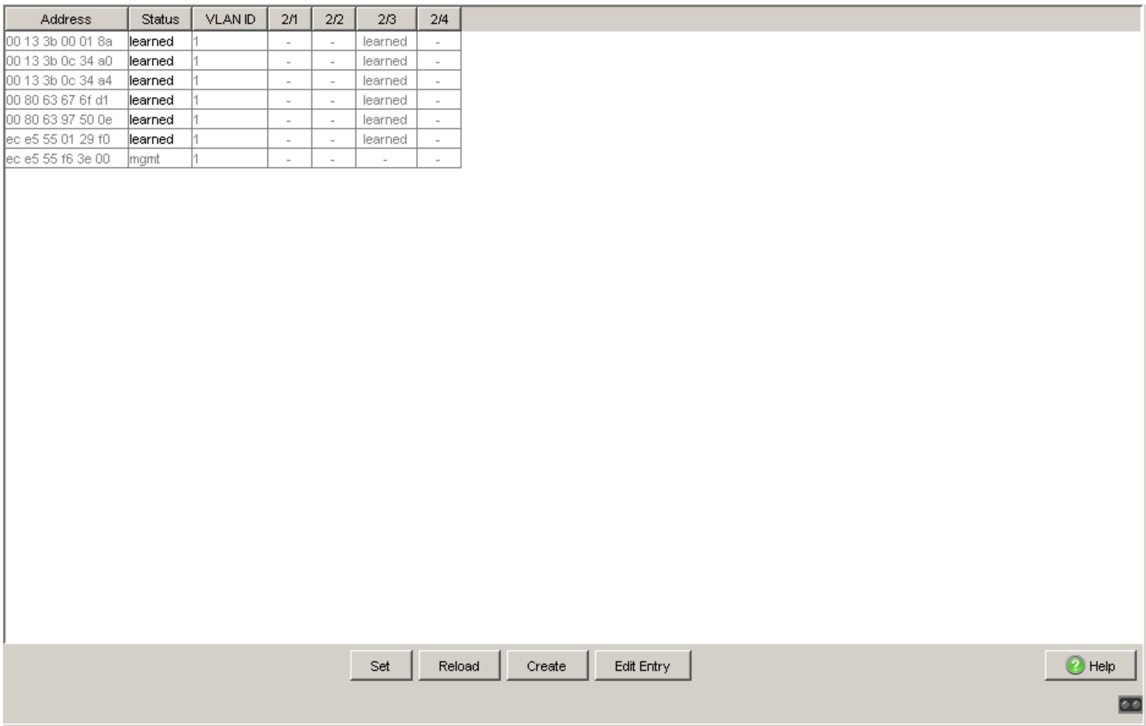
□ To temporarily save the changes, click "Set".

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

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`mac-filter <MAC address> <VLAN ID>`	Create the MAC address filter, consisting of a MAC address and VLAN ID.
`interface 1/1`	Select interface 1 port 1.
`mac-filter <MAC address> <VLAN ID>`	Assign the port to a previously created MAC address filter.
`save`	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	-	-	-	-

Figure 60: `Switching > Filter for MAC Addresses` *dialog*

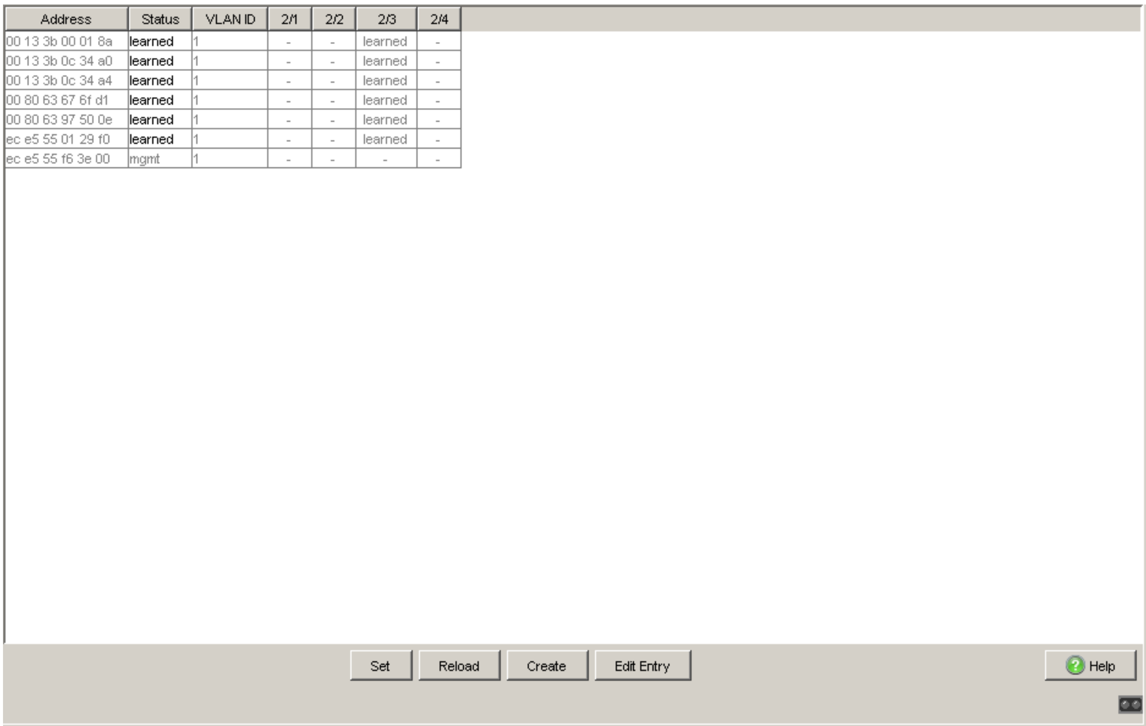
□ To convert a learned MAC address into a static address entry, select the value `permanent` in the "Status" column.

□ 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 f6 3e 00	mgmt	1	-	-	-	-

Figure 61: `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`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`interface 1/1`	Select interface 1 port 1.
`no mac-filter <MAC address> <VLAN ID>`	Cancel the assignment of the MAC address filter on the port.
`exit`	Switch to the Configuration mode.
`no mac-filter <MAC address> <VLAN ID>`	Delete the MAC address filter, consisting of a MAC address and VLAN ID.

`exit`	Switch to the privileged EXEC mode.
`save`	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).

7.2 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.

7.2.1 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.

7.2.2 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

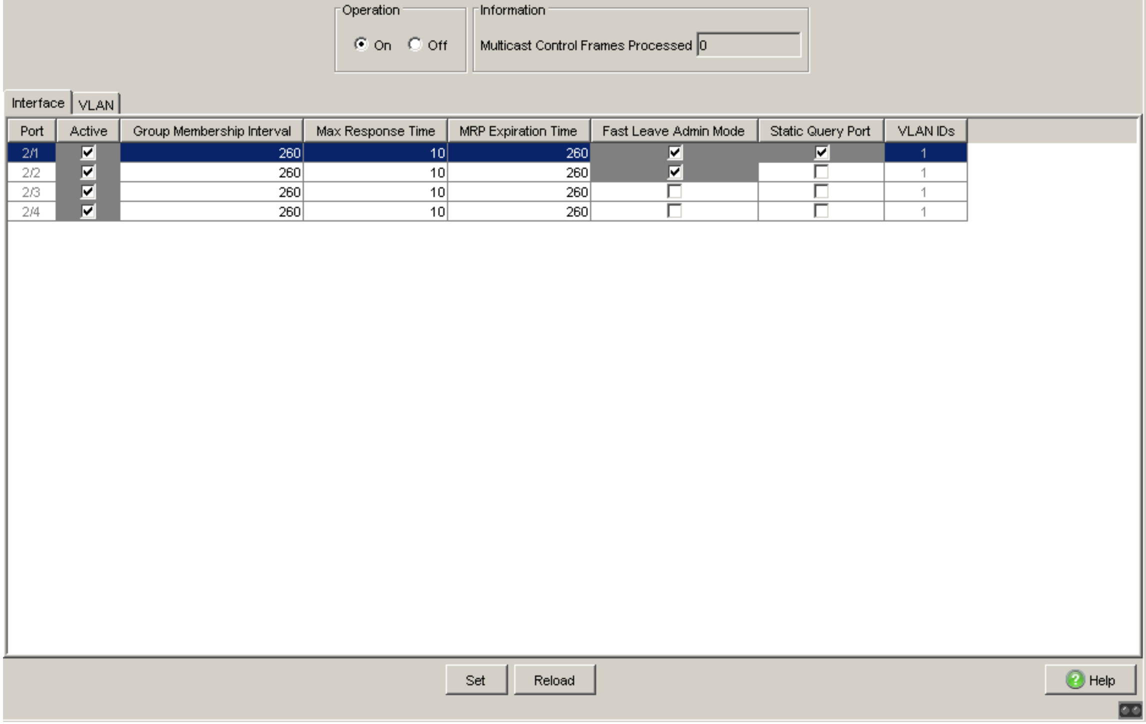
Perform the following work steps:

- □ 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.



Operation: ● On ○ Off

Information: Multicast Control Frames Processed: 0

Interface | VLAN

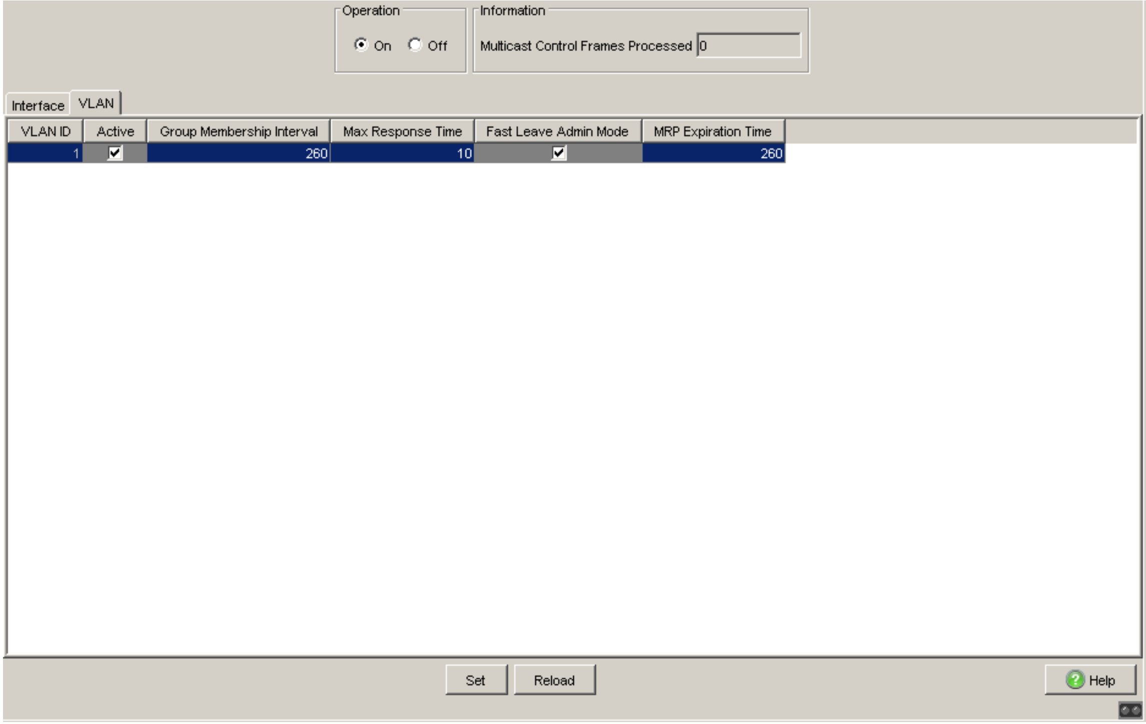
Port	Active	Group Membership Interval	Max Response Time	MRP Expiration Time	Fast Leave Admin Mode	Static Query Port	VLAN IDs
2/1	☑	260	10	260	☑	☑	1
2/2	☑	260	10	260	☑	□	1
2/3	☑	260	10	260	□	□	1
2/4	☑	260	10	260	□	□	1

Figure 62: 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.



Operation
● On ○ Off

Information
Multicast Control Frames Processed 0

Interface | VLAN

VLAN ID	Active	Group Membership Interval	Max Response Time	Fast Leave Admin Mode	MRP Expiration Time
1	☑	260	10	☑	260

Figure 63: 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

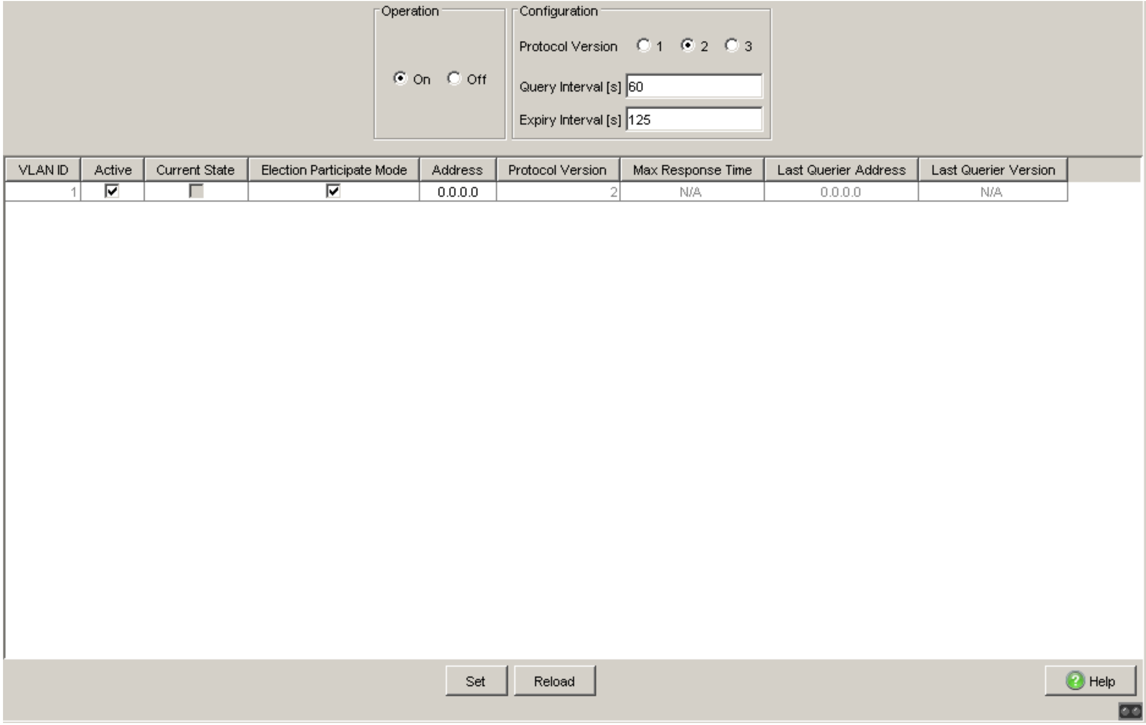
The device itself optionally sends active query messages; alternatively, it responds to query messages or detects other multicast queriers in the network (IGMP querier function).

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.



Operation

● On ○ Off

Configuration

Protocol Version ○ 1 ● 2 ○ 3

Query Interval [s] 60

Expiry Interval [s] 125

VLAN ID	Active	Current State	Election Participate Mode	Address	Protocol Version	Max Response Time	Last Querier Address	Last Querier Version
1	☑	☐	☑	0.0.0.0	2	N/A	0.0.0.0	N/A

Figure 64: `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 forward-all 1/1`	Activate the Forward All function for slot 1 / port 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".

7.3 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.

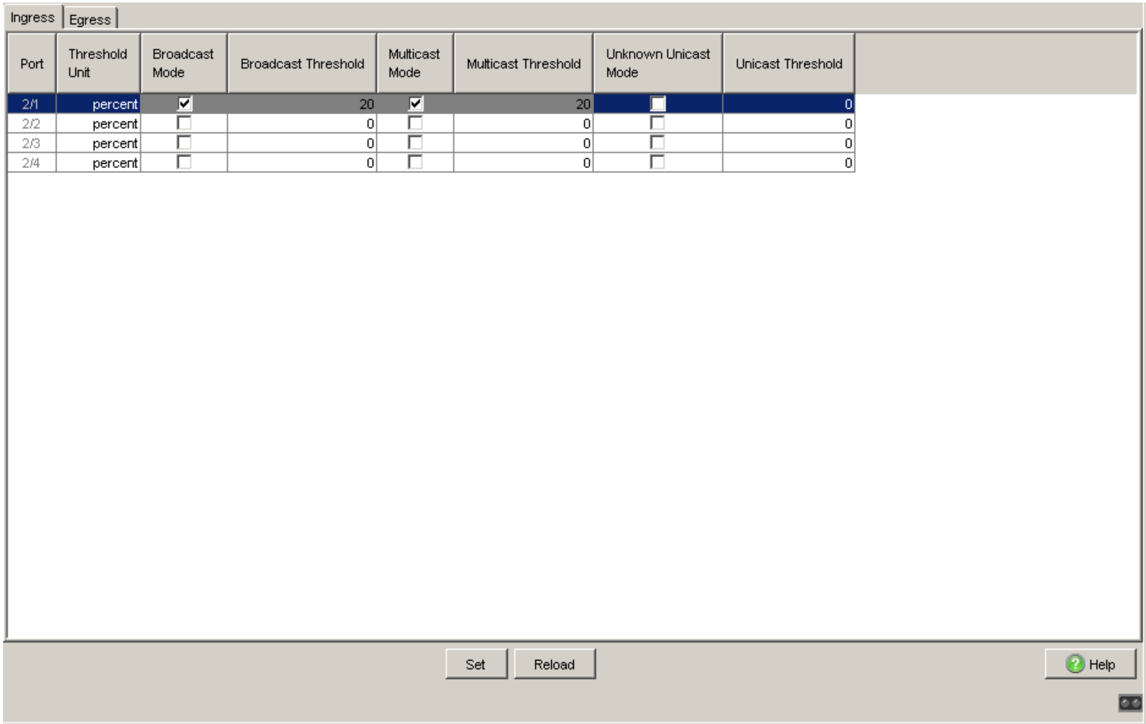
If the data rate on a port exceeds the defined limit, the device discards the overload on this port.

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 143 “Aging of learned MAC addresses”).

□ To configure the rate limiter function, proceed as follows:

🟦 □ Open the `Switching > Rate Limiter` dialog.



Port	Threshold Unit	Broadcast Mode	Broadcast Threshold	Multicast Mode	Multicast Threshold	Unknown Unicast Mode	Unicast Threshold
2/1	percent	☑	20	☑	20	□	0
2/2	percent	□	0	□	0	□	0
2/3	percent	□	0	□	0	□	0
2/4	percent	□	0	□	0	□	0

Figure 65: `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".

7.4 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.

7.4.1 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.

7.4.2 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.

7.4.3 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”).

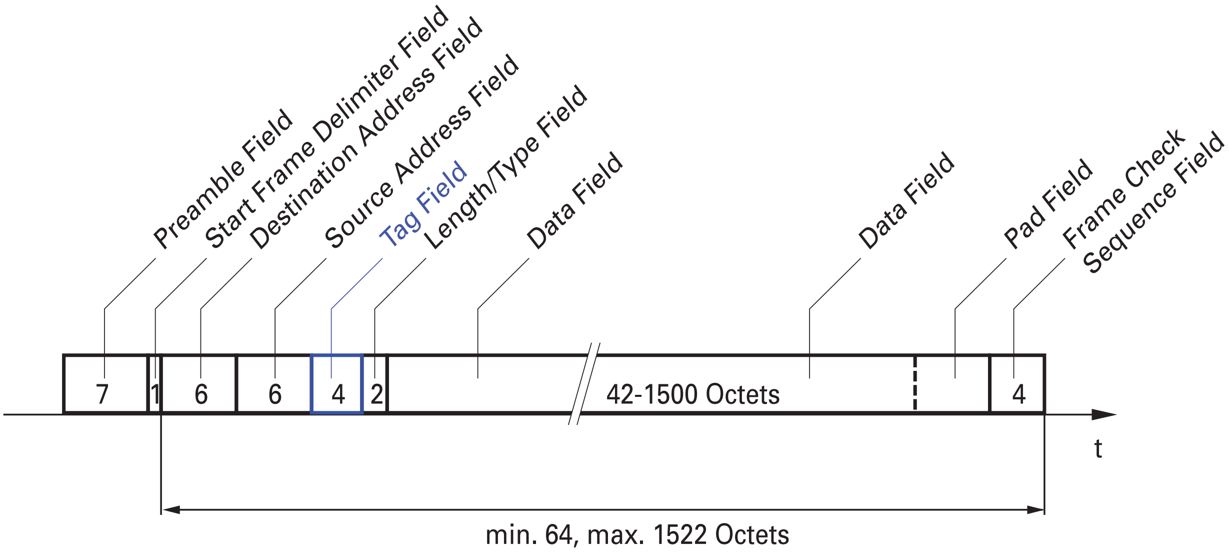


Figure 66: Ethernet data packet with tag

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

- Priority information
- VLAN tagging, if VLANs are configured

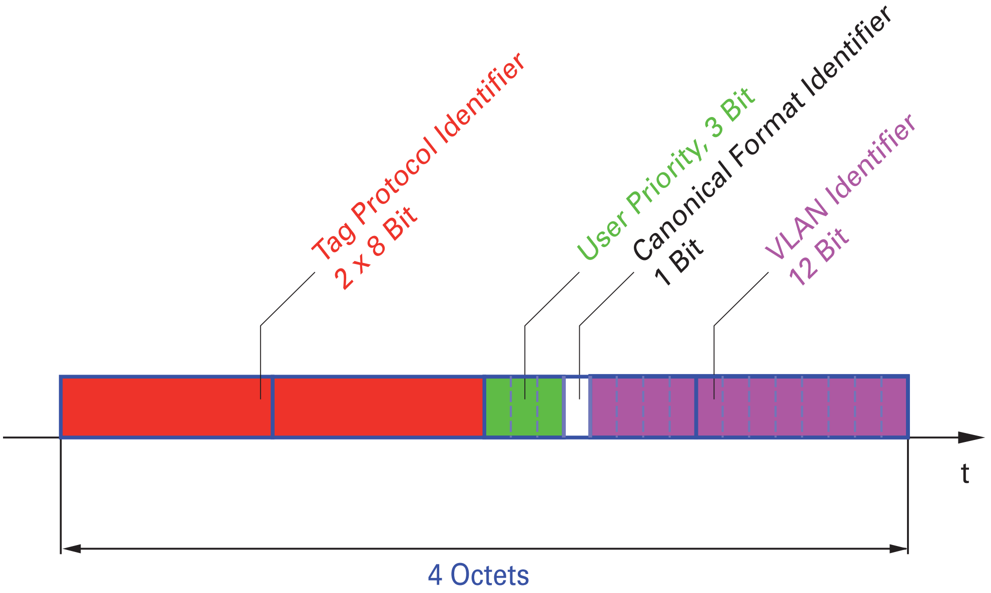


Figure 67: Structure of the VLAN tagging

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.

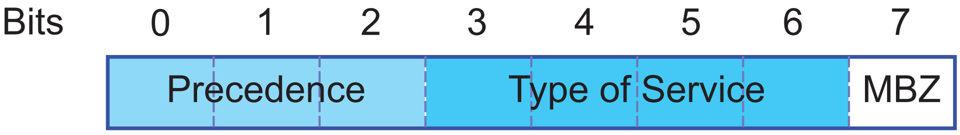
When using VLAN prioritizing, consider the following special features:

- 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.

7.4.4 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 - Immidiate		
001 - Priority		
000 - Routine		

Table 10: ToS field in the IP header

7.4.5 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.

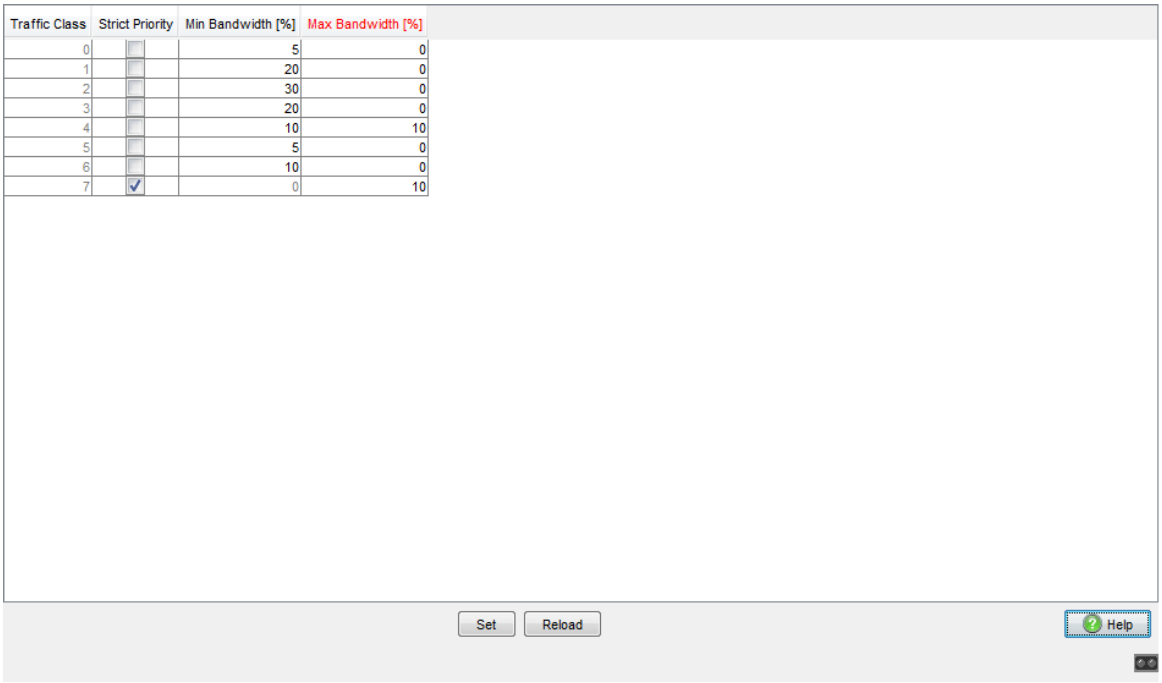
7.4.6 Queue Management

Queue Shaping

Queue shaping throttles the rate at which queues transmit packets. For example, using queue shaping, you rate-limit a higher strict-priority queue so that it allows a lower strict-priority queue to send packets even though higher priority packets are still available for transmission. The device allows you to setup queue shaping for any queue. You specify queue shaping as the maximum rate at which traffic passes through a queue by assigning a percentage of the available bandwidth.

Defining settings for Queue Management

□ Open the `Switching > QoS/Priority > Queue Management` dialog.



Traffic Class	Strict Priority	Min Bandwidth [%]	Max Bandwidth [%]
0	☐	5	0
1	☐	20	0
2	☐	30	0
3	☐	20	0
4	☐	10	10
5	☐	5	0
6	☐	10	0
7	☑	0	10

Figure 68: `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 Weighted Fair Queuing for "Traffic Class"`3`, proceed as follows:
- ▶ Unmark the "Strict Priority" checkbox for the class.
- ▶ In the "Min Bandwidth [%]" column enter `20`.

□ To combine Weight Fair Queuing and Queue Shaping for "Traffic Class"4, proceed as fllowos:

▶ Unmark the "Strict Priority" checkbox for the class.
▶ In the "Min Bandwidth [%]" column, enter 10.
▶ In the "Max Bandwidth [%]" column, enter 10.

When using a weighted fair queuing and queue shaping combination for a specific traffic class, set the "Max Bandwidth [%]" to a value that is higher than the value set in "Min Bandwidth [%]".

□ To activate Weighted Fair Queuing for "Traffic Class"5, 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"6, proceed as follows:

▶ Unmark the "Strict Priority" checkbox for the class.
▶ In the "Min Bandwidth [%]" column enter `10`.

□ To combine Strict Priority Queuing and Queue Shaping for "Traffic Class"7, proceed as follows:

▶ Mark the "Strict Priority" checkbox for the class.
▶ In the "Max Bandwidth [%]" column, enter 10.

□ 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 5`	Assign a weight of 5% to traffic class 0.
`cos-queue weighted 1`	Enable Weighted Fair Queuing for traffic class 1.
`cos-queue min-bandwidth: 1 20`	Assign a weight of 20% to traffic class 1.
`cos-queue weighted 2`	Enable Weighted Fair Queuing for traffic class 2.
`cos-queue min-bandwidth: 2 30`	Assign a weight of 30% to traffic class 2.
`cos-queue weighted 3`	Enable Weighted Fair Queuing for traffic class 3.

`cos-queue min-bandwidth: 3 20`	Assign Queue Shaping of 20 % to traffic class 3.

```
show cos-queue
Queue Id  Min. bandwidth  Max. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         0               0               strict
5         0               0               strict
6         0               0               strict
7         0               0               strict
```

Combining Weighted Fair Queuing and Queue Shaping

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`cos-queue weighted 4`	Enable Weighted Fair Queuing for traffic class 4.
`cos-queue min-bandwidth: 4 10`	Assign a weight of 10% to traffic class 4.
`cos-queue max-bandwidth: 4 10`	Assign Queue Shaping of 10% to traffic class 4.
`cos-queue weighted 5`	Enable Weighted Fair Queuing for traffic class 5.
`cos-queue min-bandwidth: 5 5`	Assign a weight of 5% to traffic class 5.
`cos-queue weighted 6`	Enable Weighted Fair Queuing for traffic class 6.
`cos-queue min-bandwidth: 6 10`	Assign a weight of 10% to traffic class 6.

```
show cos-queue
Queue Id  Min. bandwidth  Max. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         10              10              weighted
5         5               0               weighted
6         10              0               weighted
7         0               0               strict
```

Setting up Queue Shaping

```
enable                         Switch to the privileged EXEC mode.
configure                      Switch to the Configuration mode.
cos-queue max-bandwidth: 7     Assign Queue Shaping of 10% to traffic class 7.
10
show cos-queue
Queue Id  Min. bandwidth  Max. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         10              10              weighted
5         5               0               weighted
6         10              0               weighted
7         0               10              strict
```

7.4.7 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.

7.4.8 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".

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

Assigning VLAN priority to a traffic class

□ 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".

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

`exit`	Switch to the privileged EXEC mode.
`show classofservice dot1p-mapping`	Display the assignment.

Assign port priority to received 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 untrusted`	Assign the “untrusted” mode to the interface.
`classofservice dot1p-mapping 0 2`	Also assign traffic class 2 to VLAN priority 1.
`classofservice dot1p-mapping 1 2`	Also assign traffic class 2 to VLAN priority 1.
`vlan priority 1`	Set the port priority to 1.
`exit`	Switch to the Configuration mode.
`exit`	Switch to the privileged EXEC mode.
`show classofservice trust`	Display the trust mode.

```
 Interface Trust Mode
 --------- -------------
 1/1       untrusted
 1/2       dot1p
 1/3       dot1p
 1/4       dot1p
 1/5       dot1p
 1/6       dot1p
 1/7       dot1p
```

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

`classofservice ip-dscp-mapping cs1 1`	Assign traffic class 1 to DSCP CS1.
`show classofservice ip-dscp-mapping`	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`	Switch to the privileged EXEC mode.
`network management priority dot1p 7`	Assign the VLAN priority of 7 to management packets. The device sends management packets with the highest priority.
`show network parms`	Displays the management VLAN priority.

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

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`	Switch to the privileged EXEC mode.
`network management priority ip-dscp 56`	Assign the DSCP value of 56 to management packets. The device sends management packets with the highest priority.
`show network parms`	Displays the management VLAN priority.

```
IPv4 Network
------------
...
Management IP-DSCP value....................56
```

7.5 Differentiated Services

RFC 2474 defines the “Differentiated Services” field in the IP header. This field is also called “DiffServ Codepoint” or DSCP. The DSCP field is used for classification of packets into different quality classes. The DSCP field replaces the ToS field. The first 3 bits of the DSCP field are used to divide the packets into classes. The next 3 bits are used to further subdivide the classes on the basis of different criteria. This results in up to 64 different service classes.

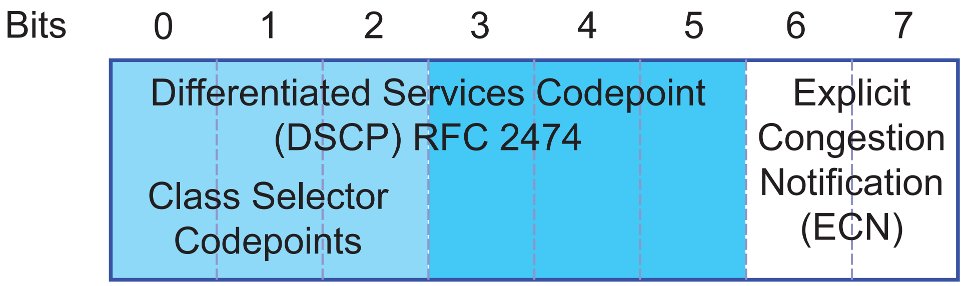

Bits
0
1
2
3
4
5
6
7
Differentiated Services Codepoint (DSCP) RFC 2474
Class Selector Codepoints
Explicit Congestion Notification (ECN)

Figure 69: Differentiated Services field in the IP header

The different DSCP values get the device to employ a different forwarding behavior, what is known as Per-Hop Behavior (PHB). The following PHB classes are defined:

- “Class Selector” (CS0–CS7): For backward compatibility, the Class Selector PHB assigns the 7 possible IP precedence values from the previous ToS field to specific DSCP values.
(see table 11).
- “Expedited Forwarding” (EF): For applications with high priority. The Expedited Forwarding PHB reduces delays (latency), jitter, and packet loss (RFC 2598).
- “Assured Forwarding” (AF): The Assured Forwarding PHB provides a differentiated schema for handling different data traffic (RFC 2597).
- “Default Forwarding”/“Best Effort”: This PHB stands for dispensing with a specific prioritization.

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

Table 11: Assigning the IP precedence values to the DSCP value

7.5.1 DiffServ example

Using the following steps configure the device to drop packets containing the source IP address 10.20.10.11, the TCP protocol and the source port 80 received on port 1/1.

Step 1: Create a traffic class.

- □ Open the `Switching > QoS/Priority > DiffServ > Class` dialog.
- □ To create a new traffic class, click "Create".
- □ In the "Class" frame, "Name" textbox, enter `class1`.
- □ In the "Rule" frame, "Type" pulldown menu, select `protocol`.
- □ In the "Parameter" frame, "Protocol Number" textbox, enter `6`.

The IANA defined the „Assigned Internet Protocol Numbers“ that you enter in the "Protocol Number" textbox.

Use this link to find a list of the protocol numbers:
http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml
A rule with the protocol number 255 matches every protocol in the IANA list.

- □ Click "OK".

□ To add the source IP address and Mask to the class, click "Create".
□ In the "Class" frame, "Name" pulldown menu, select `class1`.
□ In the "Rule" frame, "Type" pulldown menu, select `srcip`.
□ In the "Parameter" frame, "Source IP Address" textbox, enter 10.20.10.11 and in the "Source IP Address Mask" textbox, enter `255.255.255.0`.
□ Click "OK".
□ To add the source port to the class, click "Create".
□ In the "Class" frame, "Name" pulldown menu, select `class1`.
□ In the "Rule" frame, "Type" pulldown menu, select `scrL4port`.
□ In the "Parameter" frame, "Source Port" textbox, enter `80`.
□ Click "OK".
□ To save the change on the device, click "Set".

Step 2: Create a policy and a policy-class instance.

□ Open the `Switching > QoS/Priority > DiffServ > Policy` dialog.
□ To create a new policy, click "Create".
□ In the "Policy" frame, "Name" textbox, enter `policy1`.
□ In the "Policy" frame, "Direction" pulldown menu, select `in`.
□ In the "Class" frame, pulldown menu, select `class1`.
□ In the "Attribute" frame, "Type" pulldown menu, select `drop`.
□ Click "OK".
□ To save the change on the device, click "Set".

Step 3: Assign the policy to a port.

□ Open the `Switching > QoS/Priority > DiffServ > Assignment` dialog.
□ To assign the policy to an interface, click "Create".
□ In the "Assignment" frame, "Port" pulldown menu, select `1/1`.

□ In the "Assignment" frame, "Direction" pulldown menu, select `in`.
□ In the "Assignment" frame, "Policy" pulldown menu, select `policy1(1.1)`.
□ Click "OK".
□ To save the change on the device, click "Set".

Step 4: Enable the function globally.

□ Open the `Switching > QoS/Priority > DiffServ > Global` dialog.
□ To activate the function globally, in the "Operation" frame, click "On".
□ To save the change on the device, click "Set".

Note: In the `Switching > QoS/Priority > DiffServ > Assignment` dialog, the status of the previously created assignment is up solely if the link on port 1/1 is up.

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`class-map match-all class1`	Create a DiffServ class named „class1“.
`class-map name class1 match protocol tcp`	Add the TCP protocol as a match condition based on the IP protocol field.
`class-map name class1 match srcip 10.20.10.11 255.255.255.0`	Add the source IP address 10.20.10.11 as a match condition based on the source IP address.
`class-map name class1 match srcl4port http`	Add http, which is TCP port 80, as a match condition based on the layer 4 source port.
`policy-map create policy1 in`	Create a DiffServ policy named „policy1“ with the traffic direction „in“.
`policy-map name policy1 class add class1`	Add „class1“ to „policy1“.
`policy-map name policy1 class name class1 drop`	To drop packets with the above configured traffic conditions at ingress.
`interface 1/1`	Switch to the Interface Configuration mode of interface 1/1.
`service-policy in policy1`	Assign „policy1“ to interface 1/1.

`exit`	Switch to the Configuration mode.
`diffserv enable`	Enable the function globally.

7.6 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 transmition speed. This results in the receiving port no longer being overwhelmed and is able to process the incoming traffic.

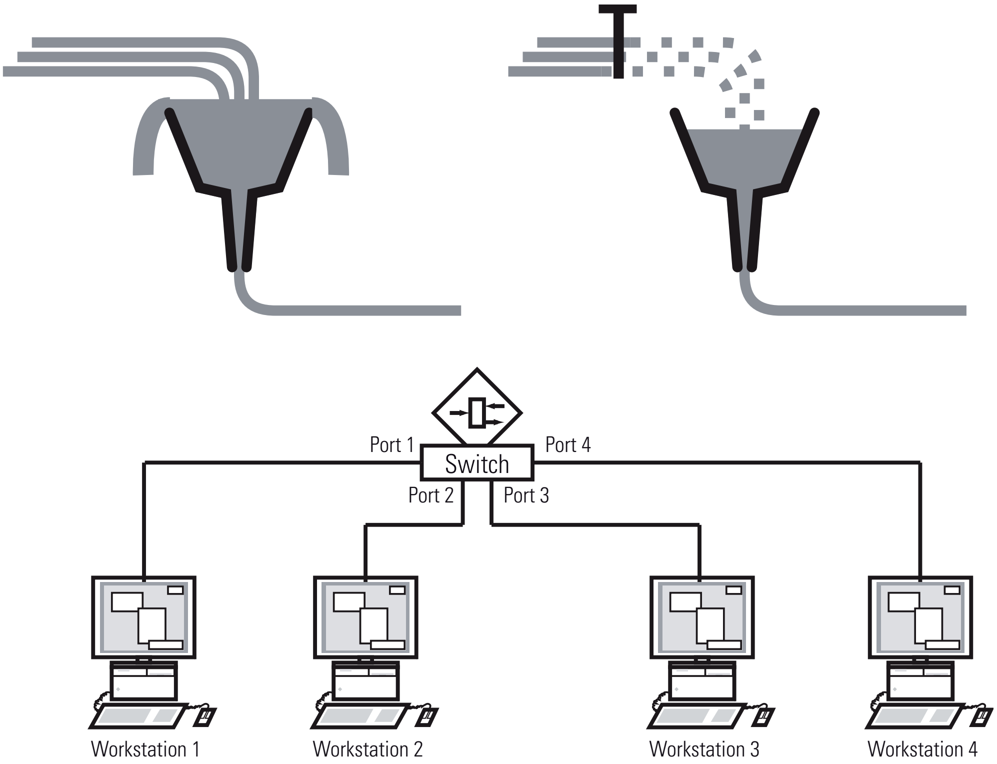


Figure 70: Example of flow control

7.6.1 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.

7.6.2 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.

8 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.

8.1 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.

8.1.1 Example 1

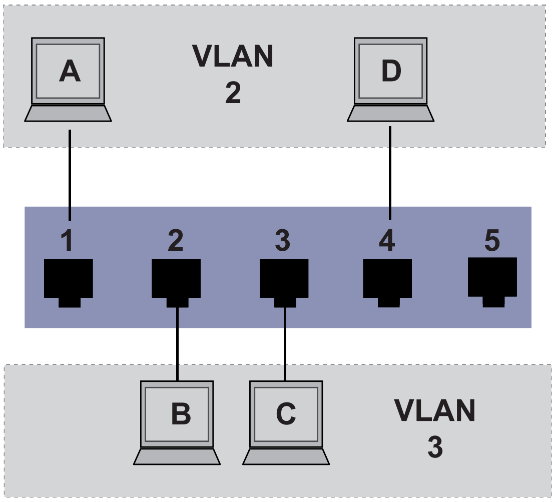


Figure 71: Example of a simple port-based VLAN

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

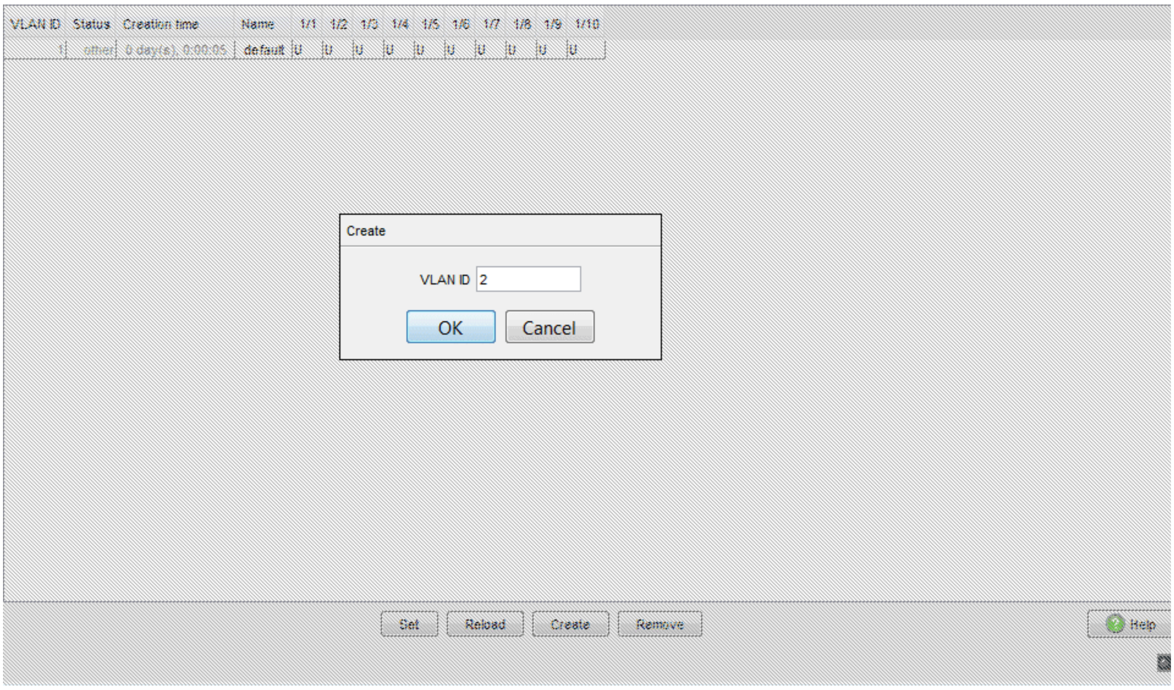
VLANID	Port				
	1	2	3	4	5
1					U
2	U			U	
3		U	U		

Table 13: Egress table

Proceed as follows to perform the example configuration:

□ Configure VLAN

□ Open the `Switching > VLAN > Configuration` dialog.



VLAN ID	Status	Creation time	Name	1/1	1/2	1/3	1/4	1/5	1/6	1/7	1/8	1/9	1/10
1	other	0 day(s), 0:00:05	default	U	U	U	U	U	U	U	U	U	U

Create

VLAN ID: 2

Figure 72: 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`.

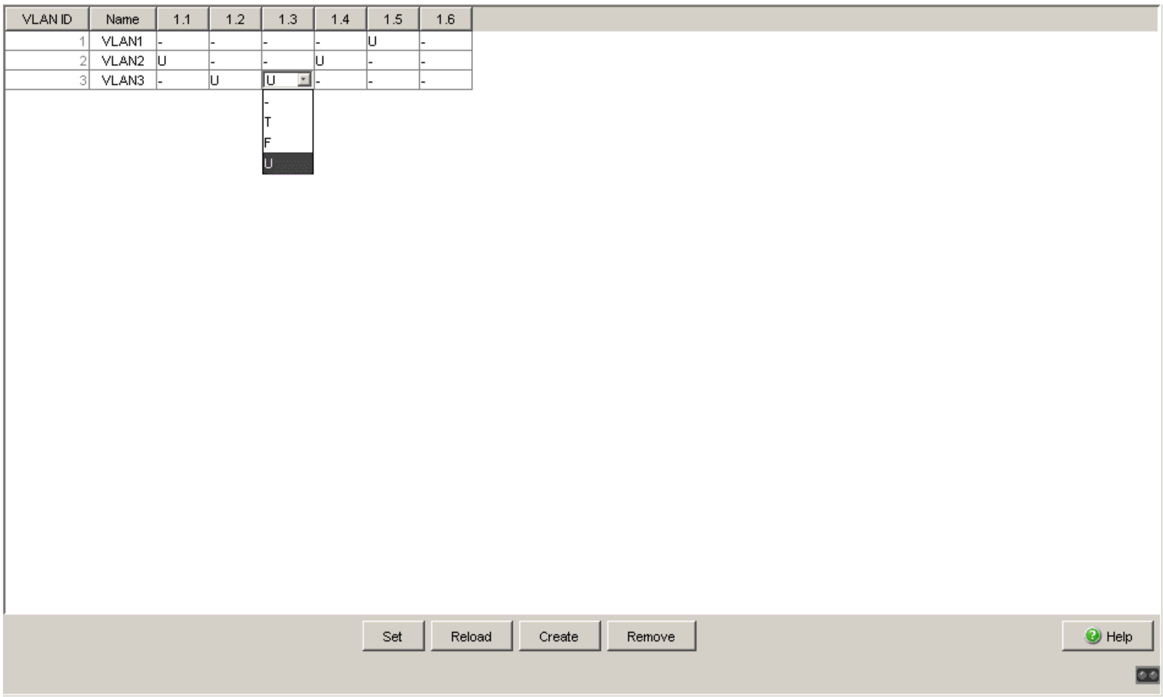
□ Repeat the previous steps and create another VLAN with the VLAN ID 3 and the name `VLAN3`.

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

`name 1 VLAN1`	Give the VLAN with the VLAN ID 1 the name VLAN1.
`exit`	Leave the VLAN configuration mode.
`show vlan brief`	Display the current VLAN configuration.

```
Max. VLAN ID................................. 4042
Max. supported VLANs......................... 256
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

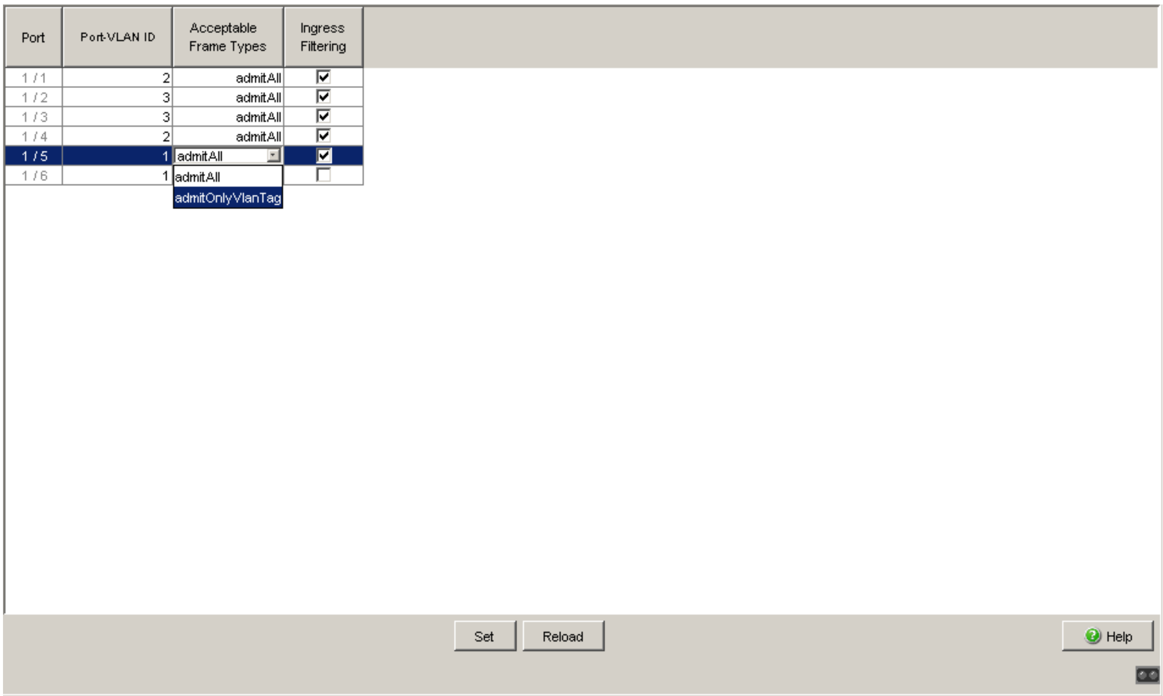


VLAN ID	Name	1.1	1.2	1.3	1.4	1.5	1.6
1	VLAN1	-	-	-	-	U	-
2	VLAN2	U	-	-	U	-	-
3	VLAN3	-	U	U	-	-	-

Figure 73: Defining the VLAN membership of the ports.

- □ Assign the ports of the device to the corresponding VLANs by clicking on the related table cell to open the selection menu and define the status. The selection options are:
  - ▶ - = currently not a member of this VLAN (GVRP allowed)
  - ▶ T = member of VLAN; send data packets with tag
  - ▶ U = Member of the VLAN; send data packets without tag
  - ▶ F = not a member of the VLAN (also disabled for GVRP)

  Because terminal devices usually interpret untagged data packets exclusivly, you select the U setting here.
- □ To temporarily save the 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	☑
1 / 2	3	admitAll	☑
1 / 3	3	admitAll	☑
1 / 4	2	admitAll	☑
1 / 5	1	admitAll	☑
1 / 6	1		☐

Figure 74: 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 affect 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`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`interface 1/1`	Switch to the Interface Configuration mode of interface 1/1.
`vlan participation include 2`	Port 1/1 becomes member untagged in VLAN 2.
`vlan pvid 2`	Port 1/1 is assigned the port VLAN ID 2.
`exit`	Switch to the Configuration mode.
`interface 1/2`	Switch to the interface configuration mode for interface 1/2.
`vlan participation include 3`	Port 1/2 becomes member untagged in VLAN 3.
`vlan pvid 3`	Port 1/2 is assigned the port VLAN ID 3.
`exit`	Switch to the Configuration mode.
`interface 1/3`	Switch to the Interface Configuration mode of Interface 1/3.
`vlan participation include 3`	Port 1/3 becomes member untagged in VLAN 3.
`vlan pvid 3`	Port 1/3 is assigned the port VLAN ID 3.
`exit`	Switch to the Configuration mode.
`interface 1/4`	Switch to the interface configuration mode of interface 1/4.
`vlan participation include 2`	Port 1/4 becomes member untagged in VLAN 2.
`vlan pvid 2`	Port 1/4 is assigned the port VLAN ID 2.
`exit`	Switch to the Configuration mode.
`exit`	Switch to the privileged EXEC mode.
`show vlan id 3`	Show details for VLAN 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
```

8.1.2 Example 2

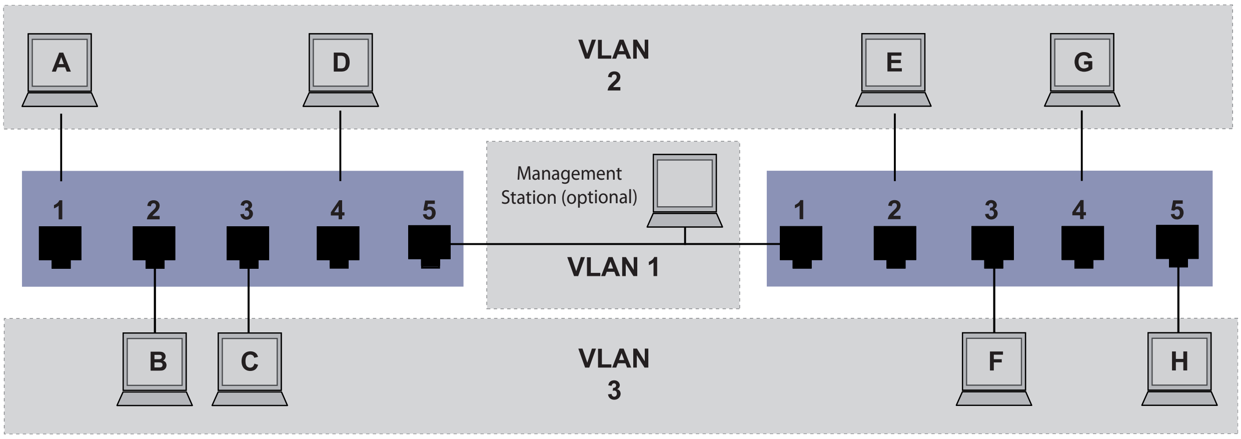


Figure 75: Example of a more complex VLAN configuration

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.

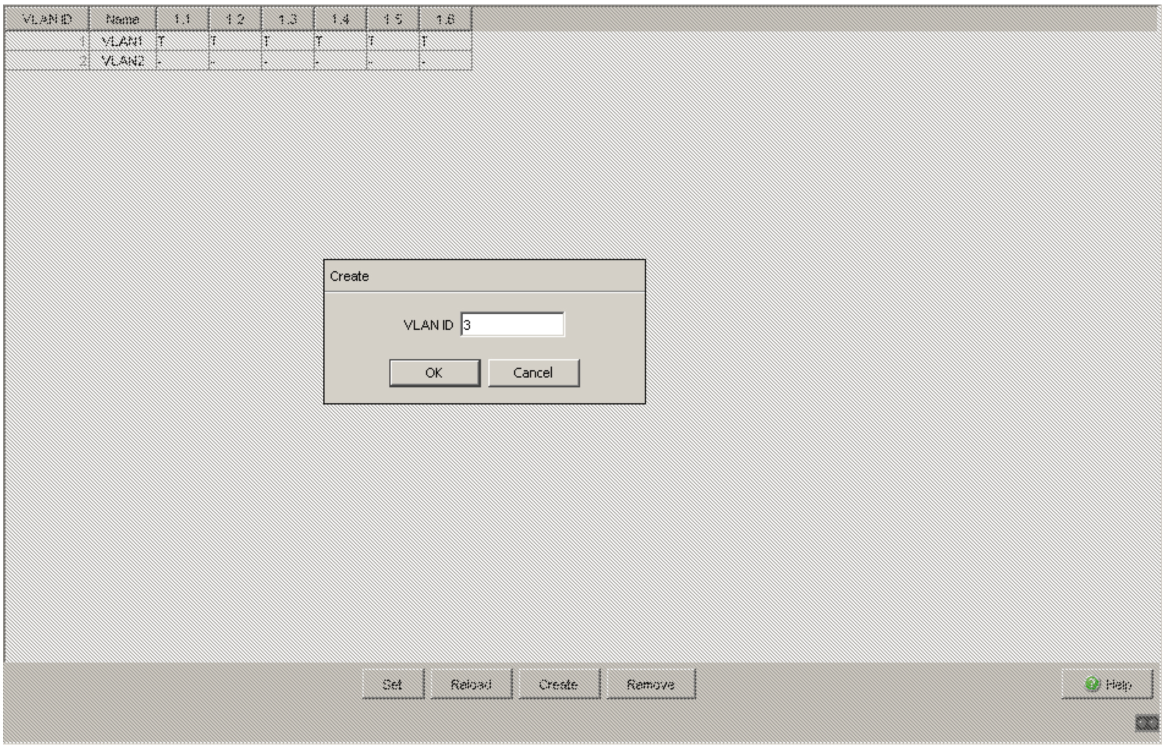
Here, the devices use VLAN tagging (IEEE 801.1Q) within the VLAN with the ID 1 (Uplink). The letter T in the egress table of the ports indicates VLAN tagging.

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.



VLAN ID	Name	1.1	1.2	1.3	1.4	1.5	1.6
1	VLAN1	T	T	T	T	T	T
2	VLAN2	-	-	-	-	-	-

Create

VLAN ID 3

Figure 76: 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.

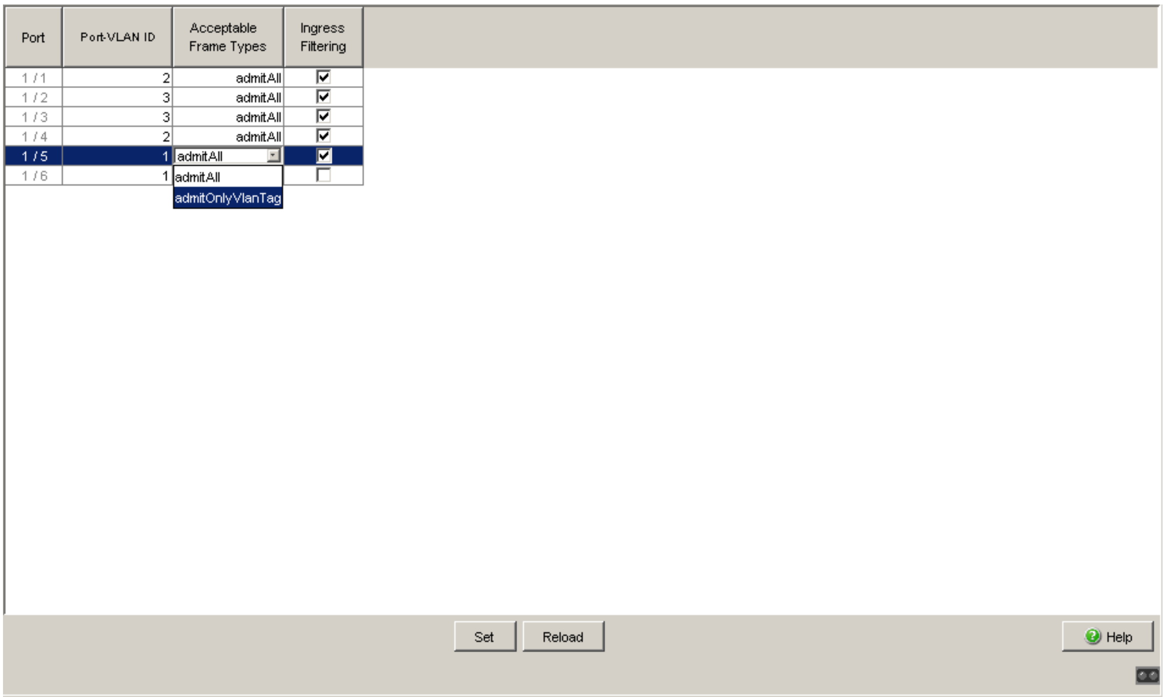
□ You give this VLAN the name `VLAN2` by clicking on the field and entering the name. Also change the name from `Default` to `VLAN1`.

□ Repeat the previous steps and create another VLAN with the VLAN ID 3 and the name `VLAN3`.

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

```
show vlan brief                   Display the current VLAN configuration.
Max. VLAN ID................................ 4042
Max. supported VLANs........................ 256
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



Port	Port-VLAN ID	Acceptable Frame Types	Ingress Filtering
1 / 1	2	admitAll	☑
1 / 2	3	admitAll	☑
1 / 3	3	admitAll	☑
1 / 4	2	admitAll	☑
1 / 5	1	admitAll	☑
1 / 6	1		☐

Figure 77: Defining the VLAN membership of the ports.

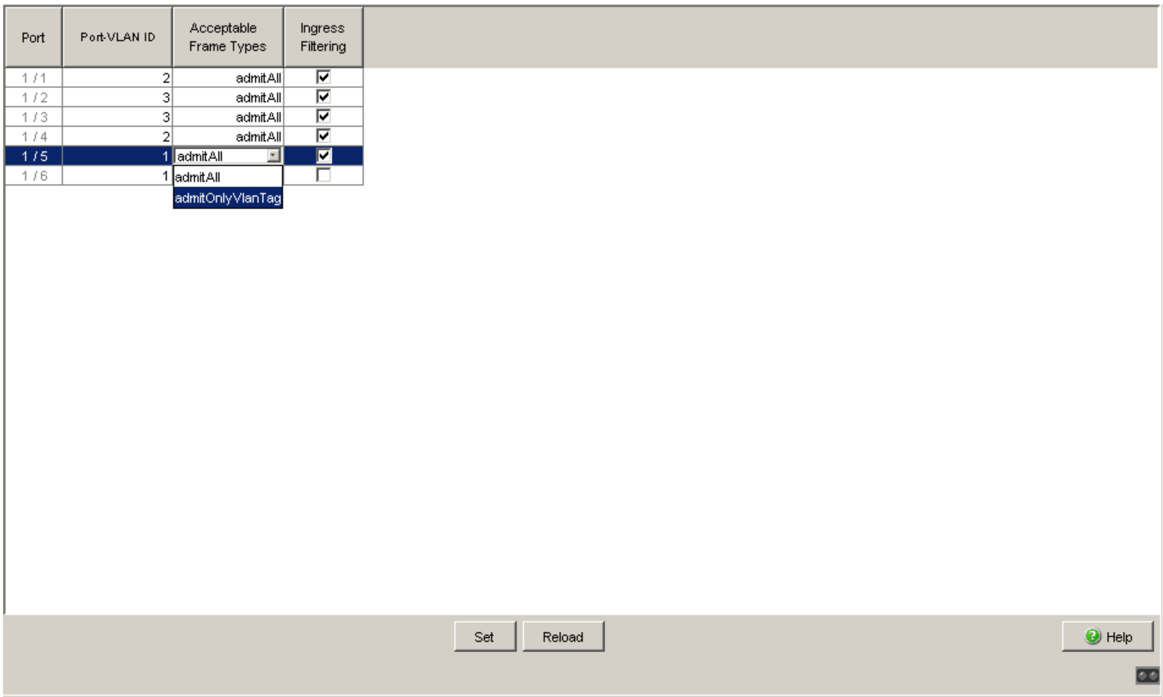
☐ Assign the ports of the device to the corresponding VLANs by clicking on the related table cell to open the selection menu and define the status. The selection options are:

- - = 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 Tsetting 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	☑
1 / 2	3	admitAll	☑
1 / 3	3	admitAll	☑
1 / 4	2	admitAll	☑
1 / 5	1	admitAll	☑
1 / 6	1	admitAll	□

Figure 78: 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`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`interface 1/1`	Switch to the Interface Configuration mode of interface 1/1.
`vlan participation include 1`	Port 1/1 becomes member untagged in VLAN 1.
`vlan participation include 2`	Port 1/1 becomes member untagged in VLAN 2.
`vlan tagging 2 enable`	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.

8.2 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 responds 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`	Switch to the privileged EXEC mode.
`vlan database`	Switch to the VLAN mode.
`vlan add 10`	Create VLAN 10.
`vlan add 20`	Create VLAN 20.
`name 10 Guest`	Rename VLAN 10 to Guest.
`name 20 Unauth`	Rename VLAN 20 to Unauth.
`exit`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`dot1x system-auth-control enable`	Enable the 802.1X function globally.
`dot1x port-control auto`	Enable port control on port 1/4.
`interface 1/4`	Switch to the Interface Configuration mode of interface 1/4.
`dot1x guest-vlan 10`	Assign the guest vlan to port 1/4.
`dot1x unauthenticated-vlan 20`	Assign the unauthorized vlan to port 1/4.
`exit`	Switch to the Configuration mode.

8.3 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.

8.4 Creating a Voice VLAN

Use the Voice VLAN feature to separate voice and data traffic on a port, by VLAN and/or priority. A primary benefit of using Voice VLAN is to safeguard the sound quality of an IP phone when the data traffic on the port is high.

The device uses the source MAC address to identify and prioritize the voice data flow. Using a MAC address to identify devices helps prevent a rogue client from connecting to the same port causing the voice traffic to deteriorate.

Another benefit of the Voice VLAN feature is that a VoIP phone obtains a VLAN ID or priority information using LLDP-MED. As a result, the VoIP phone sends voice data as tagged, priority tagged or untagged depending on the Voice VLAN Interface configuration.

The following Voice VLAN interface modes are possible. The first 3 methods segregate and prioritize voice and data traffic. Traffic segregation results in an increased voice traffic quality during high traffic periods.

- Configuring the port to using the `vlan` mode allows the device to tag the voice data coming from a VOIP phone with the user-defined voice VLAN ID. The device assigns regular data to the port default PVID.
- Configuring the port to use the `dot1p-priority` mode allows the device to tag the data coming from a VOIP phone with VLAN 0 and the user-defined priority. The device assigns the default priority of the port to regular data.
- Configure both the voice VLAN ID and the priority using the `vlan/dot1p-priority` mode. In this mode the VOIP phone sends voice data with the user-defined voice VLAN ID and priority information. The device assigns the default PVID and priority of the port to regular data.
- When configured as `untagged`, the phone sends untagged frames.
- When configured as `none`, the phone uses its own configuration to send voice traffic.

8.5 MAC-based VLANs (HiOS-2A, HiOS-3S)

Use the MAC-based VLAN to forward traffic based on the source MAC address associated with the VLAN. A MAC-based VLAN defines the filtering criteria for untagged or priority tagged packets.

Define a MAC-based VLAN filter by assigning a specific source address to a MAC-based VLAN. The device forwards untagged frames received with the source MAC address on the MAC-based VLAN ID. The other untagged packets are subject to normal VLAN classification rules.

8.6 IP subnet-based VLANs (HiOS-2A, HiOS-3S)

In an IP subnet-based VLAN, the device forwards traffic based on the source IP address and subnet mask associated with the VLAN. User-defined filters determine whether a packet belongs to a particular VLAN.

Use the IP subnet-based VLAN to define the filtering criteria for untagged or priority tagged packets. For example, assign a specific subnet address to an IP subnet-based VLAN. When the device receives untagged packets from the subnet address, it forwards them to the IP subnet-based VLAN. Other untagged packets are subject to normal VLAN classification rules.

To configure an IP subnet-based VLAN, define an IP address, a subnet mask and the associated VLAN ID. In case of multiple matching entries, the device associates the VLAN ID to the entry with the longer prefix first.

8.7 Protocol-based VLAN (HiOS-2A, HiOS-3S)

In a protocol-based VLAN, the device bridges traffic through specified ports based on the protocol associated with the VLAN. User-defined packet filters determine whether a packet belongs to a particular VLAN.

Configure protocol-based VLANs using the "Ethertype" field as the filtering criteria for untagged packets. For example, assign a specific protocol to a protocol-based VLAN. When the device receives untagged packets with the protocol, it forwards them to the protocol-based VLAN. The device assigns the other untagged packets to the port VLAN ID.

8.8 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.

9 Operation Diagnosis

The device provides you with the following diagnostic tools:

- Sending Traps
- Monitoring the device status
- Out-of-band signaling via signal contact
- Port status indication
- Event counter at port level
- Detecting non-matching duplex modes
- SFP status display
- 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

9.1 Sending Traps

The device reports unusual events which occur during normal operation immediately to the management station. This is done by messages called traps that bypass the polling procedure ("Polling" means querying the data stations at regular intervals). Traps allow you to react quickly to unusual events.

Examples of such events are:

- Hardware reset
- Changes to the configuration
- Segmentation of a port

The device sends traps to various hosts to increase the transmission reliability for the messages. The unacknowledged trap message consists of a packet containing information about an unusual event.

The device sends traps to those hosts entered in the trap destination table. The device allows you to configure the trap destination table with the management station via SNMP.

9.1.1 List of SNMP traps

The following table shows a 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.
hm2DevMonSenseExt NvmRemoval	This is sent when the external memory has been removed.
linkDown	This is sent if the connection to a port is interrupted.
linkUp	This is sent when connection is established to a port.
hm2DevMonSense Temperature	This is sent if the temperature exceeds the set threshold limits.
hm2DevMonSense PSState	This is sent if the status of a power supply unit changes.
hm2SigConStateChange	This is sent if the status of the signal contact changes in the operation monitoring.
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.
hm2SfpChangeTrap	This is sent when a supported or unsupported SFP device is inserted or removed.
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 exceds 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.

Table 18: Possible traps

Trap name	Meaning
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 (cont.)

9.1.2 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.

9.1.3 Configuring Traps

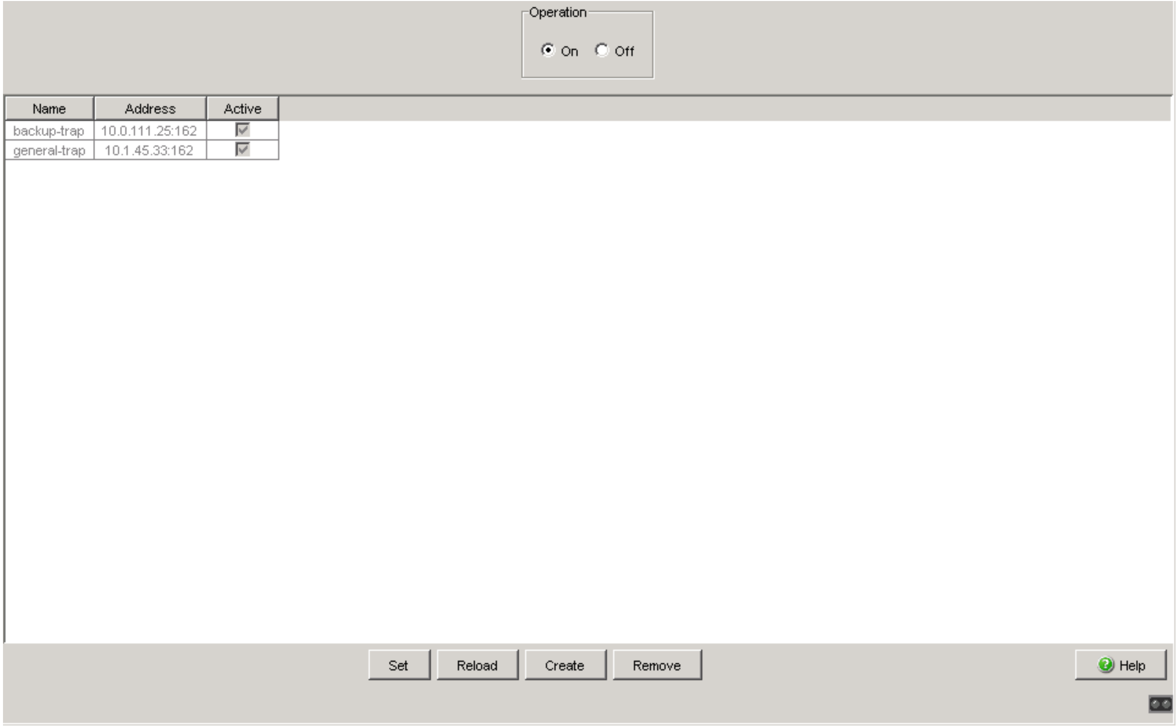
□ Open the `Diagnostics > Status Configuration > Alarms (Traps)` dialog.

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 lease 1 SNMP Manager that receives traps.

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



Operation

● On ○ Off

Name	Address	Active
backup-trap	10.0.111.25:162	☑
general-trap	10.1.45.33:162	☑

Figure 79: Alarms dialog

9.1.4 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.

9.2 Monitoring the Device Status

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

The device displays its current status as "Error" or "Ok" in the "Device status" frame. The device determines this status from the individual monitoring results.

The device enables you to:

- signal the out-of-band device status via a signal contact
- 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:

- Incorrect supply voltage
  - at least one of the 2 supply voltages is not operating
  - the internal supply voltage is not operating
- When the device is operating outside of the user-defined temperature threshold
- 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.
- The removal of the external memory.
- The configuration in the external memory is out-of-sync with the configuration in the device.
- The removal of a module

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

Note: With a non-redundant voltage supply, the device reports the absence of a supply voltage. To disable this message, feed the supply voltage over both inputs or ignore the monitoring.

9.2.1 Events which can be monitored

Name	Meaning
Temperature	If the temperature exceeds or falls below the value specified.
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.
Module removal	Enable this global function to monitor the removal of a module. Also enable the individual module to monitor.
External memory removal	Enable this function to monitor the presence of an external memory storage device.
External memory not in sync	The device monitors sychronization between the device configuration and the configuration stored on the ENVM.
Power Supply {0}	Enable this function to monitor the power supply.

Table 19: "Device Status" events

9.2.2 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 monitor the temperature, you also set the temperature thresholds in the `Basic Settings > System` dialog at the bottom of the "System Data" frame.

☐ 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`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`device-status trap`	Enable a trap to be sent if the device status changes.
`device-status monitor envm-not-in-sync`	Sets the monitoring of whether the external non-volatile memory and the current configuration match.
`device-status monitor envm-removal`	Sets the monitoring of the external non-volatile memory device removal.
`device-status monitor power-supply 1`	Enables the monitoring of the power supply 1
`device-status monitor ring-redundancy`	Sets the monitoring of the ring-redundancy
`device-status monitor temperature`	Sets the monitoring of the device temperature
`device-status monitor module-removal`	Enables the global monitoring of module removal.
`device-status module 1`	Enables the monitoring of module 1 removal.

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.

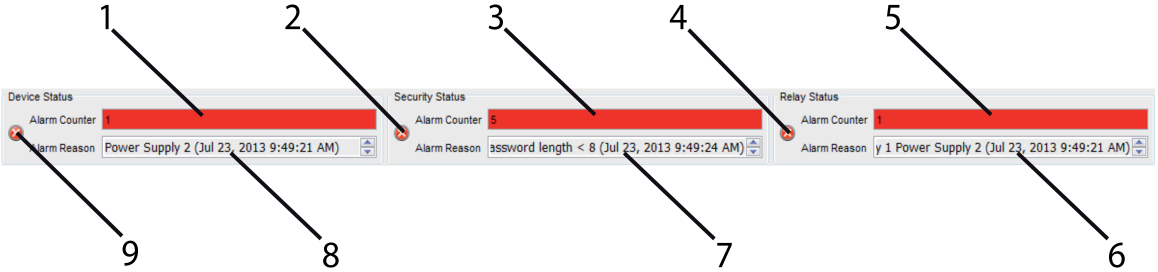
`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`device-status monitor link-failure`	Sets the monitoring of the network connection

`interface 1/1`	Select interface 1 port 1.
`device-status link-alarm`	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.)

9.2.3 Displaying the Device Status

☐ Open the `Basic Settings > System` dialog.



Device Status
Alarm Counter 1
Alarm Reason Power Supply 2 (Jul 23, 2013 9:49:21 AM)

Security Status
Alarm Counter 5
Alarm Reason assword length < 8 (Jul 23, 2013 9:49:24 AM)

Relay Status
Alarm Counter 1
Alarm Reason y 1 Power Supply 2 (Jul 23, 2013 9:49:21 AM)

Figure 80: 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.

9.3 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 out-of-band via a signal contact
- 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

9.3.1 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.

Table 20: "Security Status" events

Name	Meaning
Password Policy settings deactivated	The device monitors the settings located in the `Device Security >` User Management 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.
Saving the Configuration Profile on the External Memory possible	The device monitors the possibility to save configurations to the external non-volatile memory.
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.
Load unencrypted config from external memory	The device monitors the security settings for loading the configuration from the external NVM.
IEC61850-MMS active	The device monitors the IEC 61850-MMS protocol activation setting.

Table 20: "Security Status" events (cont.)

9.3.2 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`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`security-status monitor pwd-change`	Sets the monitoring of default password change for ‘user‘ and ‘Admin‘.
`security-status monitor pwd-min-length`	Sets the monitoring of minimum length of the password (smaller 8) .
`security-status monitor pwd-policy-config`	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".
`security-status monitor pwd-policy-inactive`	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.
`security-status monitor telnet-enabled`	Sets the monitoring of the activation of telnet on the switch.
`security-status monitor http-enabled`	Sets the monitoring of the activation of http on the switch.
`security-status monitor snmp-unsecure`	To monitor SNMP security. (When enabling SNMPv1/v2, or disabling v3 encryption).
`security-status monitor sysmon-enabled`	To monitor the activation of System Monitor 1 on the device.
`security-status monitor extnvm-upd-enabled`	To monitor the activation of the external non volatile memory update.
`security-status monitor iec61850-mms-enabled`	To monitor the activation of the IEC 61850-MMS protocol.
`security-status trap`	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.

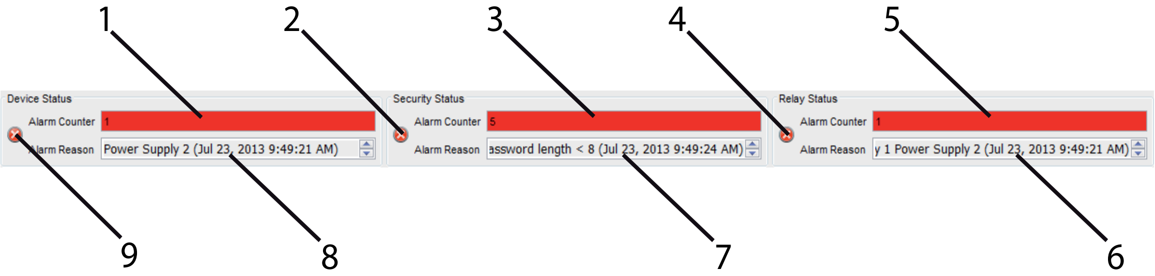
□ Open the "Port" tab of the `Diagnostics > Status Configuration >` Device Status dialog.

□ In the "Link interrupted on enabled device ports" row, you select the ports to monitor.

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`security-status monitor no-link-enabled`	Sets the monitoring of no link detection.
`interface 1/1`	Select interface 1 port 1.
`security-status no-link`	Sets the monitoring of no link detection status of interface 1 port 1.

9.3.3 Displaying the Security Status

□ Open the `Basic Settings > System` dialog.



Device Status
Alarm Counter: 1
Alarm Reason: Power Supply 2 (Jul 23, 2013 9:49:21 AM)

Security Status
Alarm Counter: 5
Alarm Reason: assword length < 8 (Jul 23, 2013 9:49:24 AM)

Relay Status
Alarm Counter: 1
Alarm Reason: y 1 Power Supply 2 (Jul 23, 2013 9:49:21 AM)

Figure 81: 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.

9.4 Out-of-band Signalling

The device uses the signal contact to control external devices and monitor device functions. Function monitoring enables you to perform remote diagnostics.
The device reports the operating status via a break in the potential-free signal contact (relay contact, closed circuit) for the selected mode. The device monitors the following functions:

- Incorrect supply voltage
  - at least one of the 2 supply voltages is not operating,
  - the internal supply voltage is not operating.
- When the device is operating outside of the user-defined temperature threshold
- Events for ring redundancy:
  Loss of the redundancy (in ring manager mode). On delivery, ring redundancy monitoring is inactive.
  The device is a normal ring participant and detects an error in the local configuration.
- The interruption of link connection(s). Configure at least one port for this feature. In the "Propagate Connection Error" frame, you specify which ports the device signals if the link is down. On delivery, link monitoring is inactive.
- The removal of the external memory.
- The configuration on the external memory does not match that in the device.
- The removal of a module

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

Note: With a non-redundant voltage supply, the device reports the absence of a supply voltage. To disable this message, feed the supply voltage over both inputs or ignore the monitoring.

9.4.1 Controlling the Signal Contact

With the `Manual Setting` mode you control this signal contact remotely.

Application options:

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

□ Open the `Diagnostics > Status Configuration > Signal Contact` dialog.

□ To set the signal contact manually, you select the `Manual Setting` option from the "Mode" pull down menu in the "Configuration" frame.

□ To open the signal contact, you select the `Opened` option in the "Configuration" frame.

□ To close the signal contact, you select the `Closed` option in the "Configuration" frame.

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

9.4.2 Monitoring the Device and Security Statuses

The "Mode" pull down menu in the "Configuration" frame controls the signal contact. When you change modes click "Set" then "Reload" to display the current status.

When you select `Device Status` from the "Mode" pull down menu in the "Configuration" frame, then the signal contact displays the status from the `Diagnostics > Status Configuration > Device Status` dialog.

When you select `Security Status` from the "Mode" pull down menu in the "Configuration" frame then, the signal contact displays the status from the `Diagnostics > Status Configuration > Security Status` dialog.

When you select `Device Status/Security Status` from the "Mode" pull down menu in the "Configuration" frame then, the signal contact displays the combined device and security status.

Configuring the operation monitoring

- □ Open the `Diagnostics > Status Configuration > Signal Contact` dialog.
- □ Select the `Monitoring Correct Operation` option from the "Mode" pull down menu in the "Configuration" frame to use the signal contact to monitor the device functions.
- □ In the "Monitor" column, you select the events to monitor.
- □ You specify the temperature thresholds for the temperature monitoring in the `Basic Settings > System` dialog.
- □ 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.
- □ To save the configuration in the non-volatile memory, click "Set".
- □ To display the current status, click "Reload".

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`signal-contact 1 monitor temperature`	Sets the monitoring of the device temperature
`signal-contact 1 monitor ring-rundancy`	Sets the monitoring of the ring-redundancy
`signal-contact 1 monitor link-failure`	Enables the monitoring of the network connection.
`signal-contact 1 monitor envm-removal`	Sets the monitoring of the external non-volatile memory device removal.
`signal-contact 1 monitor envm-not-in-sync`	Sets the monitoring of synchronization between the external non-volatile memory and the current configuration.
`signal-contact 1 monitor power-supply`	Sets the monitoring of the power supply
`signal-contact 1 monitor module-removal 1`	Enables the monitoring of module 1 removal.

`signal-contact 1 trap`	Enables the device to send a trap the status of the operation monitoring changes.
`no signal-contact 1 trap`	Disables a trap messaging.

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

- □ 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.

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`signal-contact 1 monitor link-failure`	Sets the monitoring of the network connection
`interface 1/1`	Select interface 1 port 1.
`signal-contact 1 link-alarm`	Sets the monitoring of a active link without a connection for this port.

Events which can be monitored

Name	Meaning
Temperature	If the temperature exceeds or falls below the value specified.
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.
Module removal	Enable this global function to monitor the removal of a module. Also enable the individual module to monitor.
External memory not in sync with NVM	The device monitors sychronization between the device configuration and the configuration stored on the ENVM.
External memory removed	Enable this function to monitor the presence of an external memory storage device.
Power Supply {0}	Enable this function to monitor the power supply.

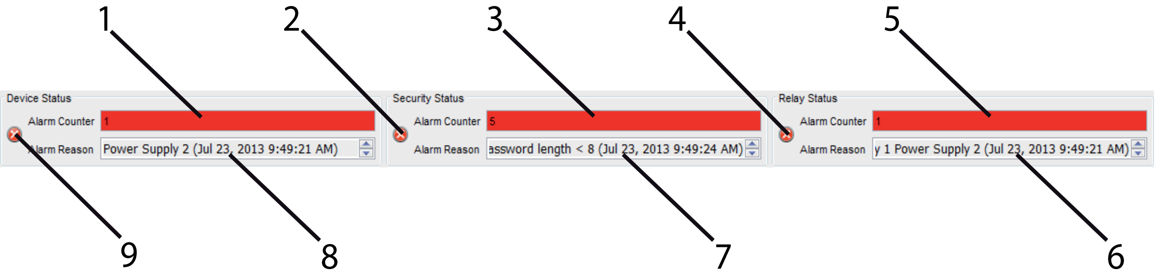
Table 21: "Device Status" events

■ Displaying the signal contact’s status

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

- ▶ display in the graphical user interface,
- ▶ query in the Command Line Interface.

☐ Open the `Basic Settings > System` dialog.



Device Status
Alarm Counter: 1
Alarm Reason: Power Supply 2 (Jul 23, 2013 9:49:21 AM)

Security Status
Alarm Counter: 5
Alarm Reason: assword length < 8 (Jul 23, 2013 9:49:24 AM)

Relay Status
Alarm Counter: 1
Alarm Reason: y 1 Power Supply 2 (Jul 23, 2013 9:49:21 AM)

Figure 82: 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 signal-contact 1 all` Displays signal contact settings for the specified signal contact.

9.5 Port Status Indication

□ Open the `Basic Settings > System` dialog.

The dialog displays the device with the current configuration. Furthermore, the dialog indicates the status of the individual ports with a symbol.

The following symbols represent the status of the individual ports. In some situations, these symbols interfere with one another. If you position the mouse pointer over the port icon, a bubble help displays a detailed description of the port state.

Criterion	Symbol	
Bandwidth of the device port	•	10 Mbit/s Port activated, connection okay, full-duplex mode
	●	100 Mbit/s Port activated, connection okay, full-duplex mode
	⬤	1000 Mbit/s Port activated, connection okay, full-duplex mode
Operating state	◐	Half-duplex mode activated See the `Basic Settings > Port` dialog, "Configuration" tab, "Automatic Configuration" checkbox, "Manual Configuration" field and "Manual Cable Crossing (Auto. Conf. off)" field.
	◎	Autonegotiation activated See the `Basic Settings > Port` dialog, "Configuration" tab, "Automatic Configuration" checkbox.
	⊝	Port is blocked by a redundancy function.
AdminLink	⊖	Port is deactivated, connection okay
	⊖	Port is deactivated, no connection set up See the `Basic Settings > Port` dialog, "Configuration" tab, "Port on" checkbox, and "Link/ Current Settings" field.

Table 22: Symbols identifying the status of the device ports

9.6 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 obseverd by selecting the
Diagnostics:Ports:Statistics Table
dialog.

Counter	Indication of known possible weakness
Received fragments	– Non-functioning controller of the connected device – Electromagnetic interference in the transmission medium
CRC error	– Non-functioning controller of the connected device – Electromagnetic interference in the transmission medium – Inoperable component in the network
Collisions	– Non-functioning controller of the connected device – Network over extended/lines too long – Collision or a detected fault with a data packet

Table 23: 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.

9.6.1 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 24: 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

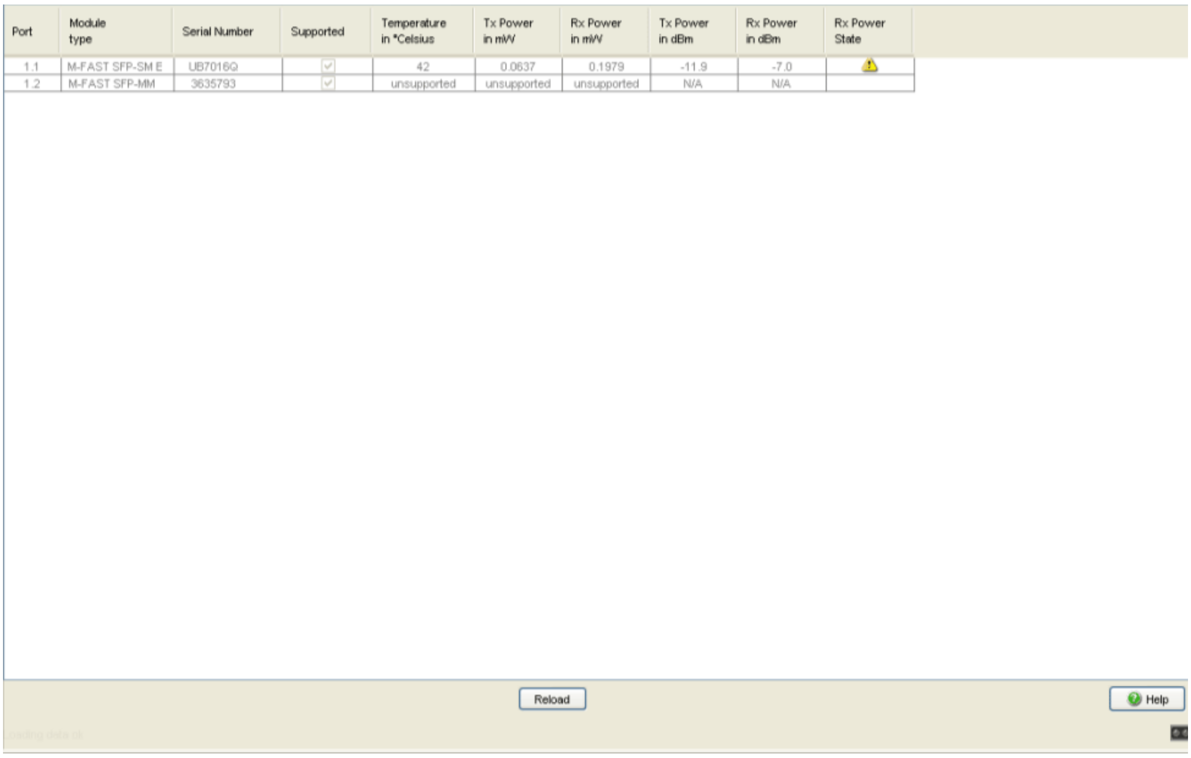
Table 24: Evaluation of non-matching of the duplex mode (cont.)

9.7 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	✓	42	0.0637	0.1979	-11.9	-7.0	⚠
1.2	M-FAST SFP-MM	3635793	✓	unsupported	unsupported	unsupported	N/A	N/A	

Figure 83: SFP Modules dialog

9.8 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 querys 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.

9.8.1 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.

9.8.2 LLDP-Med

LLDP for Media Endpoint Devices (LLDP-MED) is an extension to LLDP that operates between endpoint devices. Endpoints include devices such as IP phones, or other Voice over IP (VoIP) devices or servers and network devices such as switches. It specifically provides support for VoIP applications. LLDP-MED provides this support using an additional set of common type-length-value (TLV) advertisement messages, for capabilities discovery, network policy, Power over Ethernet, inventory management and location information.

The device supports the following TLV messages:

- capabilities TLV
  Allows LLDP-MED endpoints to determine the capabilities that the connected device supports and what capabilities the device has enabled.
- Network policy TLV
  Allows both network connectivity devices and endpoints to advertise VLAN configurations and associated attributes for the specific application on that port. For example, the device notifies a phone of the VLAN number. The phone connects to a switch, obtain its VLAN number, and then starts communicating with the call control.

LLDP-MED provides the following functions:

- Network policy discovery, including VLAN ID, 802.1p priority and Diffserv code point (DSCP)
- Device location and topology discovery based on LAN-level MAC/port information
- Endpoint move detection notification, from network connectivity device to the associated VoIP management application
- Extended device identification for inventory management
- Identification of endpoint network connectivity capabilities, for example, multi-port IP Phone with embedded switch or bridge capability
- Application level interactions with the LLDP protocol elements to provide timely startup of LLDP to support rapid availability of an Emergency Call Service
- Applicability of LLDP-MED to Wireless LAN environments, support for Voice over Wireless LAN

9.9 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.

BPDU frames 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.

9.10 Email Notification (HiOS-2A, HiOS-3S)

The device allows you to inform users by email about events that have occurred. Prerequisite is that a mail server is available through the network on which the device transfers the email messages.

To setup the device to send email messages, use the following steps:
□ Specifying the sender address
□ Specifying the the triggering events
□ Specifying the receivers
□ Specifying the mail server
□ Enabling/disabling of the function
□ Sending of a test message

9.10.1 Specifying the sender address

The sender address is the email address that indicates the device which sent the email message. In the device, the value `switch@hirschmann.com` is preset.

To change the preset value, perform the following work steps:

□ Open the `Diagnostics > Email Notification > Global` dialog.
□ In the "Sender" frame, change the value in the "Address" field.
Add a valid email address.
□ Click the "Set" button.

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`logging email from-addr <user@doma.in>`	Changes the sender address.

9.10.2 Specifying the the triggering events

The device differentiates between the following severities:

Severity	Meaning
`emergency`	Device not ready for operation
`alert`	Immediate user intervention required
`critical`	Critical status
`error`	Error status
`warning`	Warning
`notice`	Significant, normal status
`informational`	Informal message
`debug`	Debug message

Table 25: Meaning of the severities for events

You have the option of specifying the events of which the device informs you. For this, assign the desired minimum severity to the notification levels of the device.

The device informs the receivers as follows:

▶ "Notification Immediate"
The device sends an email message immediately when an event of the severity assigned or more critical occurs.

▶ "Notification Periodic"
- In the log file buffer, the device logs if an event of the severity assigned or more critical occurs.
- The device sends an email message with the log file periodically or if the log file buffer overflows.
- If an event of a lesser severity occurs, the device does not send an email message.

Perform the following work steps:

□ Open the `Diagnostics > Email Notification > Global` dialog.

In the "Notification Immediate" frame, you specify the settings for instant messages.

□ In the "Severity" field, you specify the minimum severity.
□ In the "Subject" field, you specify the subject line.

In the "Notification Periodic" frame, you specify the settings for periodic messages.

□ In the "Severity" field, you specify the minimum severity.
□ In the "Subject" field, you specify the subject line.

□ Click the "Set" button.

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`logging email severity urgent <level>`	Specifies the minimum severity for the serious events.
`logging email severity non-urgent <level>`	Specifies the minimum severity for non-serious events.
`logging email subject add <urgent | non-urgent> TEXT`	Creates a subject line with the content ‚TEXT‘ for the email messages.

9.10.3 Changing the send interval

The device allows you to specify in which interval the device sends email messages with the log file. `30` minutes are preset.

Perform the following work steps:

□ Open the `Diagnostics > Email Notification > Global` dialog.
You specify the settings for non-serious events "Notification Periodic" frame.

□ Change the value in the "Sending Interval [min]" field to change the interval.

□ Click the "Set" button.

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`logging email duration <30..1440>`	Specifies the interval at which the device sends email messages with log file.

9.10.4 Specifying the receivers

The device allows you to inform up to 10 different receivers.

Perform the following work steps:

□ Open the `Diagnostics > Email Notification > Receiver` dialog.

□ Click the "Create" button.
Adds a new table entry.

□ Click in the "Notification" field:
- To inform the receiver about serious events, select "Immediate".
- To inform the receiver about non-serious events, select "Periodic".

□ Click in the "Address" field: specify the email address of the receiver.

□ Mark the checkbox in the "Active" column.

□ Click the "Set" button.

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`logging email to-addr add <1..10> addr <user@doma.in> msgtype <urgent|non-urgent>`	Specifies the receiver with the email address `user@doma.in`. The device manages the settings on the memory place `1..10`.

9.10.5 Specifying the mail server

The device sends the email messages through 1 of up to 5 mail servers encrypted or unencrypted using the SMTP protocol.

Perform the following work steps:

□ Open the `Diagnostics > Email Notification > Mail Server` dialog.

□ Use the "Create" button to add a new table entry.

□ Click in the "IP Address" field: add the IP address of the mail server.

□ Click in the "Encryption" field: select the value `tlsv1`, if the mail server encrypts the connection using TLS (SMTP over SSL). Otherwise, leave the value at `none`.
The device adapts the value in the "TCP Port" field automatically. You see the change after clicking the buttons "Set" and "Reload".

If the mail server uses a port other than the default port:

□ Click in the "TCP Port" field: enter the number of the TCP port.

If the mail server requests an authentication:

□ Click in the fields "User ID" and "Password" to enter the user name and password.
The device logs in to the mail server using these login data, provided that in the "Encryption" field you set the value `tlsv1`.

□ Click in the "Description" field: enter a meaningful designation for the mail server.

□ Mark the checkbox in the "Active" column.

□ Click the "Set" button.

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`logging email mail-server add <1..5> addr <IP ADDRESS> [security <none|tlsv1>] [username <USER NAME>] [password <PASSWORD>] [port <1..65535>]`	Specifies the mail server with the IP address `IP ADDRESS`. The device manages the settings in memory `1..5`.

9.10.6 Enabling/disabling of the function

Perform the following work steps:

- □ Open the `Diagnostics > Email Notification > Global` dialog.
- □ Select in the "Operation" frame the "On" radio button.
- □ Click the "Set" button.

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`logging email operation`	Enables the sending of email messages.
`no logging email operation`	Disables the sending of email messages:

9.10.7 Sending of a test message

The device allows you to check the settings by sending a test message.

Prerequisite:
- The settings for the email message are specified.
- The function is enabled.

Perform the following work steps:

- □ Open the `Diagnostics > Email Notification > Mail Server` dialog.
- □ Click the "Connection Test" button to display the "Connection Test" dialog.
- □ Click in the "Severity" field:
  - Select the value `urgent` to send the test message to the recipients which the device informs about serious events.
  - Select the value `urgent` to send the test message to the recipients which the device informs about serious events.
- □ Click in the "Message Text" field: enter the text of the email message.
- □ Click the "OK" button to send the test message.

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`logging email test msgtype <urgent|non-urgent> <STRING>`	Sends an email message with the `STRING` content to the receivers.

If you do not see any error message and the receivers obtain the message, the device settings are correct.

9.11 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.
- Persistent Logging
  The device saves log entries in a file in the external memory, when present. These files are available after power down. The maximum size, maximum number of retainable files and the severity of logged events are configurable. After obtaining the user-defined maximum size or maximum number of retainable files, the device archives the entries and starts a new file. The device deletes the oldest file and renames the other files to maintain the configured number of files. To review these files use the CLI or copy them to an external server for future reference.
- 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.

9.11.1 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".

9.11.2 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`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`logging host add 1 addr 10.0.1.159 severity 3`	Add a new recipient of the log messages . The “3” indicates the seriousness of the message sent by the device. “3” means “error”.
`logging syslog operation`	Enable the Syslog function.
`exit`	Switch to the privileged EXEC mode.
`show logging host`	Display the syslog host settings.

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

`configure`	Switch to the Configuration mode.
`logging snmp-requests get operation`	Create log events from reading SNMP requests.
`logging snmp-requests get severity 5`	The “5” indicates the seriousness of the message that the device allocates to messages from reading SNMP requests. “5” means “note”.
`logging snmp-requests set operation`	Create log events from writing SNMP requests.
`logging snmp-requests set severity 5`	The “5” indicates the seriousness of the message that the device allocates to messages from writing SNMP requests. “5” means “notice”.
`exit`	Switch to the privileged EXEC mode.
`show logging snmp`	Display the SNMP logging settings.

```
Log SNMP GET requests              : enabled
Log SNMP GET severity              : notice
Log SNMP SET requests              : enabled
Log SNMP SET severity              : notice
```

9.11.3 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.

9.11.4 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

9.12 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.

9.13 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.

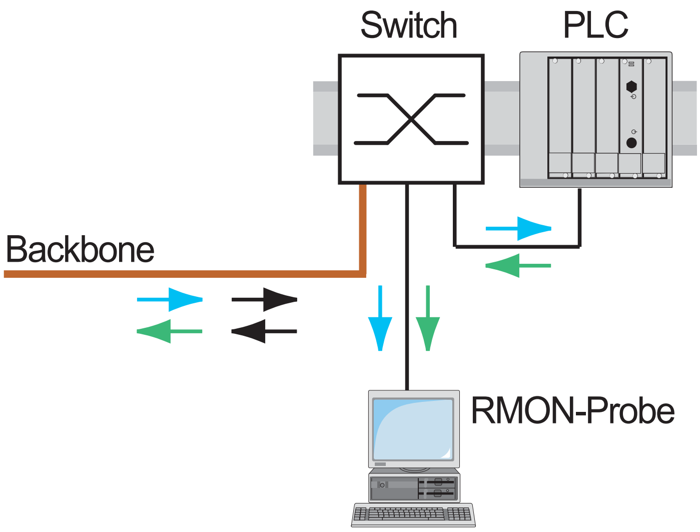


Figure 84: Port mirroring

9.14 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`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`selftest action task log-only`	To send a message to the event log when a task is unsuccessful.
`selftest action resource send-trap`	To send a flag to the manamgement station when there is a lack of resources.
`selftest action software send-trap`	To send a flag to the manamgement station when there is a loss of software integrity.
`selftest action hardware reboot`	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`	Enable RAM selftest on cold start.
`no selftest ramtest`	Switch off the "ramtest“ function.
`selftest system-monitor`	Enable the "SysMon1“ function.
`no selftest system-monitor`	Switch off the "SysMon1“ function.
`show selftest action`	Show status of the actions to be taken in the event of device degradation.
`show selftest settings`	Show ramtest and sysmon settings in event of a cold start.

9.15 Network Monitoring with sFlow (HiOS-2A, HiOS-3S)

sFlow is a standard protocol for monitoring networks. The device provides this function for visibility into network activity, enabling effective management and control of network resources.

The sFlow monitoring system consists of an sFlow agent, embedded in the device and a central sFlow collector. The agent uses sampling technology to capture traffic statistics. sFlow instances associated with individual data sources within the agent perform packet flow and counter sampling. Using sFlow datagrams the agent forwards the sampled traffic statistics to an sFlow collector for analysis.

The agent uses 2 forms of sampling, a statistical packet based sampling of packet flows and a timed based sampling of counters. An sFlow datagram contains both types of samples. Packet flow sampling, based on a sampling rate, sends a steady, but random stream of datagrams to the collector. For time-based sampling, the agent polls the counters at set intervals to fill the datagrams.

The device implements datagram version 5 for the sFlow agent.

The user-defined sFlow functions are:

Sampler configuration, packet flow sampling:
- data source port number, to sample physical ports
- receiver index associated with the sampler
- sampling rate, the device counts the packets of received data, when the count reaches the user-defined number the agent samples the packet, 0 = disable, range: 256 - 65535.
- header size in bytes to sample, range: 20-256

Poller configuration, counter sampling:
- data source port number, available for physical ports
- receiver index associated with the poller
- interval, in seconds, between samples, range: 0-86400

Receiver configuration, up to 8 entries:
- owner name, to claim an sFlow entry
- timeout, in seconds, until sampling is stopped and the device releases the receiver along with the sampler and the poller

- datagram size
- IP address
- port number

To configure the sFlow agent for a monitoring session, first configure an available receiver. Then, configure a sampling rate to perform packet flow sampling, and configure a polling interval for counter sampling.

For example, Company XYZ wishes to monitor data flow on a device. The IP address for the remote server containing the sFlow collector, is 10.10.10.10. XYZ requires a sample of the first 256 bytes of every 300th packet. Furthermore, XYZ requires counter polling every 400 s.

□ Open the `Diagnostics > SFlow > Configuration` dialog.

□ For the name of the person or organization controlling the receiver, enter `XYZ` in the "Name" cell.

□ For the remote server IP Address, on which the sFlow collector software runs, enter `10.10.10.10` in the "IP Address" cell.

□ Open the `Diagnostics > SFlow > Configuration` dialog, "Sampler" tab.

□ Select the index number of the receiver configured in the previous steps from the "Receiver" pull down menu.

□ For the number of packets the device receives before the agent samples a packet, enter `300` in the "Sampling Rate" cell.

□ For the number of bytes to sample from a packet, enter `256` in the "Maximum Header Size" cell.

□ Open the `Diagnostics > SFlow > Configuration` dialog, "Poller" tab.

□ Select the index number of the receiver configured the previous steps from the "Receiver" pull down menu.

□ For the time, in seconds, between samples, enter `400` in the "Interval [s]" cell.

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`sflow receiver 1 owner XYZ ip 10.10.10.10`	Configure an sFlow receiver
`interface 1/1`	Switch to the Interface Configuration mode of interface 1/1.
`sflow sampler receiver 1 rate 300`	To assign the sFlow sampler on the port to the previously configured receiver with a sampling rate of 300.

`sflow sampler maxheadersize 256`	To configure the maximum header size of the sFlow sampler to 256.
`sflow poller receiver 1interval 400`	To assign the sFlow poller to the previously configured receiver and to sample data for 400 s.

10 Advanced functions of the device

10.1 Using the device as a DHCP Server

A Dynamic Host Configuration Protocol (DHCP) server assigns IP addresses, gateways, and other networking definitions such as DNS and NTP parameters to clients.

The DHCP operations fall into 4 basic phases: IP discovery, IP lease offer, IP request, and IP lease acknowledgment. Use the acronym DORA which stands for Discovery, Offer, Request, and Acknowledgement to help remember the phases. The server receives client data on UDP port 67 and sends data to the client on UDP port 68.

The DHCP server provides an IP address pool or "pool", from which it allocates IP addresses to clients. The pool consists of a list of entries. An entry defines either a specific IP address or an IP address range.

The device allows you to activate the DHCP server globally and per interface.

10.1.1 IP Addresses assigned per port or per VLAN

The DHCP server assigns a static IP address or dynamic range of IP addresses to a client connected to a port or a VLAN. The device allows you to create entries for either a port or a VLAN. When creating an entry to assigning IP addresses to a VLAN the port entry grays out. When creating an entry to assigning IP addresses to a port the VLAN entry grays out.

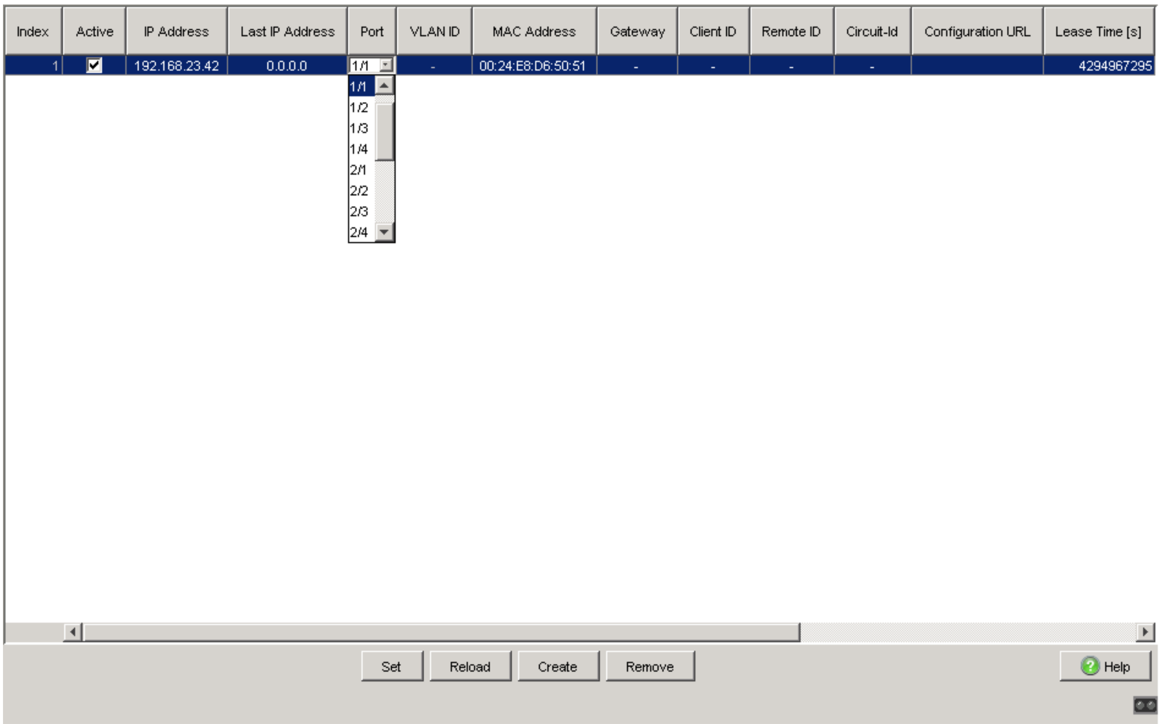
Static allocation means that the DHCP server assigns the same IP address to a specific client. The DHCP server identifies the client using a unique hardware ID. A static address entry contains 1 IP address, and applies it to a port or VLAN on which the server receives a request from a specific client. For static allocation, create a pool entry for the ports or one specific port, enter the IP address, and leave the "Last IP Address" field empty. Enter a hardware ID with which the DHCP server uniquely identifies the client. This ID is either a MAC address, a client ID, a remote ID, or a circuit ID. If a client contacts the server with the configured hardware ID, the DHCP server allocates the static IP address.

The device also allows you to assign a dynamic IP address range to ports or VLANs from which the DHCP server allocates a free IP address from a pool. To create a dynamic pool entry for the ports or VLANs, enter the first and last IP addresses for the IP address range, leaving the "MAC Address", "Client ID", "Remote ID", and "Circuit ID" fields empty. Creating multiple pool entries allows you to have IP address ranges that contain gaps.

10.1.2 DHCP server static IP address example

In this example, configure the device to allocate a static IP address to a port. The device recognizes clients with unique hardware identification. The hardware ID in this case is the client MAC address 00:24:E8:D6:50:51.

☐ Open the `Advanced > DHCP Server > Pool` dialog.
☐ To add a new entry to the table, click "Create".
☐ Enter `192.168.23.42` in "IP Address".
☐ Select `1/1` from the "Port" pull down menu.
☐ Enter `00:24:E8:D6:50:51` in "MAC Address".
☐ To assign the IP address to the client infinitely, enter `4294967295` in "Lease Time [s]".
☐ To enable the entry, click "Active".
☐ Open the `Advanced > DHCP Server > Global` dialog.
☐ Verify that port 1/1 is active in the "DHCP Server active" column.
☐ To enable the function, select in the "Operation" frame the "On" radio button.



Index	Active	IP Address	Last IP Address	Port	VLAN ID	MAC Address	Gateway	Client ID	Remote ID	Circuit-Id	Configuration URL	Lease Time [s]
1	☑	192.168.23.42	0.0.0.0	1/1	-	00:24:E8:D6:50:51	-	-	-	-		4294967295

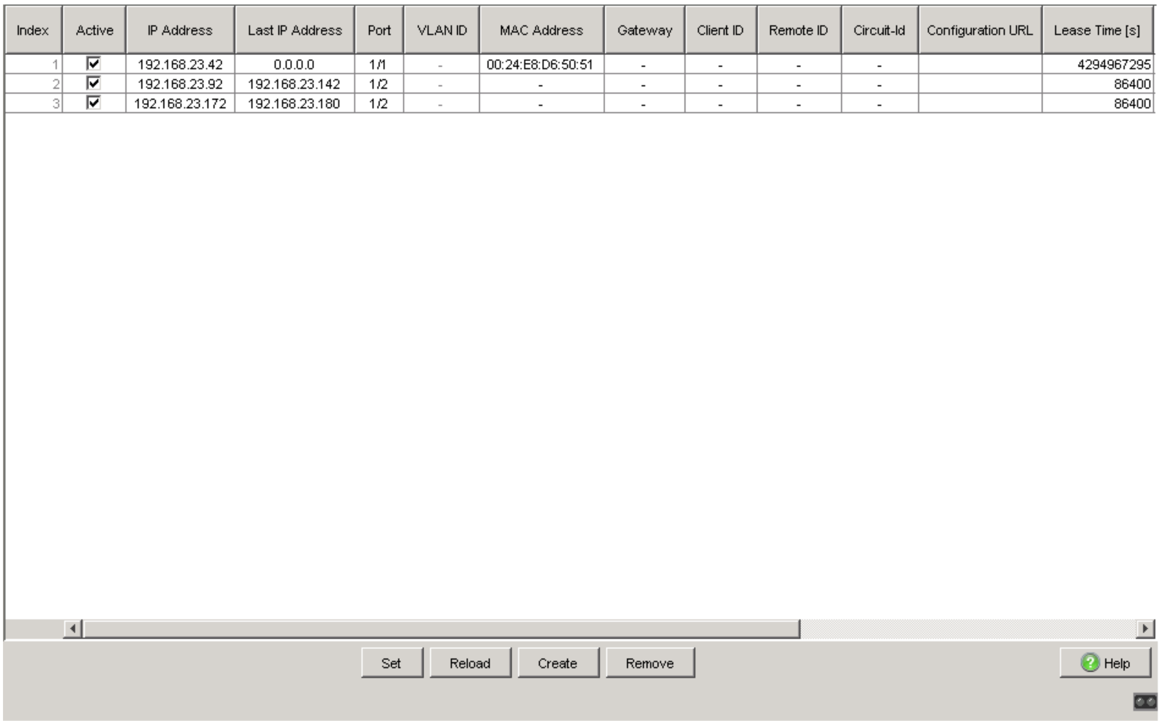
Figure 85: Table in the `Advanced > DHCP Server > Pool` dialog.

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`dhcp-server pool add 1 static 192.168.23.42`	Creates index 1 and assigns the IP address 192.168.23.42 statically.
`dhcp-server pool modify 1 mode interface 1/1`	Assigns the static address in index 1 to port 1/1.
`dhcp-server pool modify 1 mode mac 00:24:E8:D6:50:51`	Assigns the IP address in index 1 to the device with the MAC address 00:24:E8:D6:50:51.
`dhcp-server pool mode 1`	Enables the index 1 pool entry.
`dhcp-server pool modify 1 leasetime infinite`	Modifies index 1, to allocate the IP address to the client infinitely.
`dhcp-server operation`	Enables the DHCP server.
`interface 1/1`	Change to the Interface Configuration mode of port 1/1.
`dhcp-server operation`	Enables the DHCP server operation on this port.

10.1.3 DHCP server dynamic IP address range example

The device allows you to create dynamic IP address ranges. Leave the "MAC Address", "Client ID", "Remote ID", and "Circuit ID" fields blank. To create dynamic IP address ranges with gaps between the ranges add several entries to the table.

- □ Open the `Advanced > DHCP Server > Pool` dialog.
- □ To add a new entry to the table, click "Create".
- □ Enter `192.168.23.92`, in "IP Address" for the first IP address of the range and enter `192.168.23.142` in "Last IP Address" for the last IP address of the range.
- □ The default setting for "Lease Time [s]" is 60 days. Set this value for the appropriate interval.
- □ Select `1/2` from the "Port" pull down menu.
- □ To enable the entry, click "Active".
- □ Open the `Advanced > DHCP Server > Global` dialog.
- □ Activate port `1/2` in the "DHCP Server active" column.
- □ To enable the function, select in the "Operation" frame the "On" radio button.



Index	Active	IP Address	Last IP Address	Port	VLAN ID	MAC Address	Gateway	Client ID	Remote ID	Circuit-Id	Configuration URL	Lease Time [s]
1	☑	192.168.23.42	0.0.0.0	1/1	-	00:24:E8:D6:50:51	-	-	-	-		4294967295
2	☑	192.168.23.92	192.168.23.142	1/2	-	-	-	-	-	-		86400
3	☑	192.168.23.172	192.168.23.180	1/2	-	-	-	-	-	-		86400

Figure 86: Table in the `Advanced > DHCP Server > Pool` dialog.

enable	Switch to the privileged EXEC mode.
configure	Switch to the Configuration mode.
dhcp-server pool add 2 dynamic 192.198.23.92 192.168.23.142	Adds a dynamic pool with an IP range from 192.168.23.92 to 192.168.23.142.
dhcp-server pool modify 2 leasetime {seconds | infinite}	Enters the lease time in seconds or infinite.
dhcp-server pool add 3 dynamic 192.198.23.172 192.168.23.180	Creates index 3 and assigns the IP address range from 192.168.23.172 to 192.168.23.180. A dynamic pool consists of a range of IP addresses.
dhcp-server pool modify 3 leasetime {seconds | infinite}	Enters the lease time in seconds or infinite.
dhcp-server pool mode 2	Enables the index 2 pool entry.
dhcp-server pool mode 3	Enables the index 3 pool entry.
dhcp-server operation	Enables the DHCP server.
interface 2/1	Switch to the interface configuration mode.
dhcp-server operation	Enables the DHCP server operation on this port.

10.2 DHCP L2 Relay

A network administrator uses the DHCP Layer 2 Relay agent to add DHCP client information required by Layer 3 Relay agents and DHCP servers to assign an address and configuration to a client.

When a DHCP client and server are in the same IP subnet, they exchange IP address requests and replies directly. However, having a DHCP server on each subnet is expensive and often impractical. An alternative to having a DHCP server in every subnet is to use the network devices to relay packets between a DHCP client and a DHCP server located in a different subnet.

A Layer 3 Relay agent is generally a router that has IP interfaces in both the client and server subnets and routes traffic between them. However, in Layer 2 switched networks, there are one or more network devices, switches for example, between the client and the Layer 3 Relay agent or DHCP server. In this case, this device provides a Layer 2 Relay agent to add the information that the Layer 3 Relay agent and DHCP server require to perform their roles in address and configuration assignment.

The follow list contains the default settings for this function:

- Global setting:
  - Active setting: disable
- Interface settings:
  - Active setting: disable
  - Trusted Port: disable
- VLAN settings:
  - Active setting: disable
  - Circuit ID: enable
  - Remote ID Type: mac
  - Remote ID: blank

10.2.1 Circuit and Remote IDs

Before forwarding the request of a client to the DHCP server, the device adds the Circuit ID and the Remote ID to the Option 82 field of the DHCP request packet.

- The Circuit ID stores on which port the device received the request of the client.
- The remote ID contains the MAC address, the IP address, the system name, or a user-defined character string. Using it, the participating devices identify the relay agent that received the request of the client.

The device and other relay agents use this information to re-direct the answer from the DHCP relay agent to the original client. The DHCP server is able to analyze this data e.g. to assign the client an IP address from a specific address pool.

Also, the replay packet of the DHCP server contains the Circuit-ID and the Remote ID. Before forwarding the answer to the client, the device removes the information from the Option 82 field.

10.2.2 DHCP L2 Relay Configuration

The `Advanced > DHCP L2 Relay > Configuration` dialog allows you to activate the function on the active ports and on the VLANs.

The ports on which the DHCP Layer 2 Relay function is active and are marked as "Trusted Port", the device forwards DHCP packets with Option 82 information. Typically, these are ports in the network of the DHCP server.

The ports to which the DHCP clients are connected, you activate the DHCP Layer 2 Relay function, but leave the "Trusted Port" checkbox unmarked. On these ports, the device discards DHCP packets with Option 82 information.

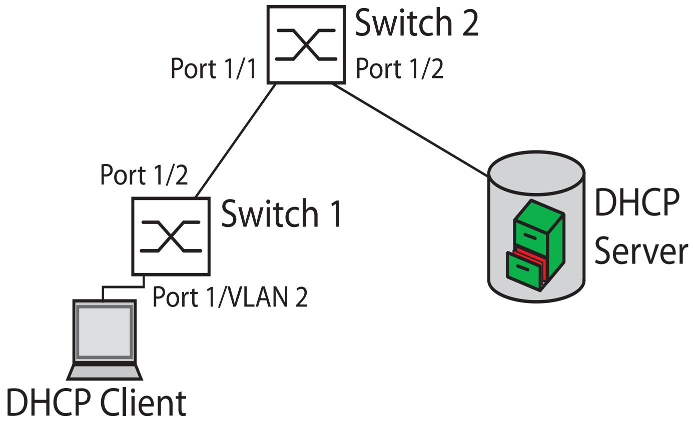


Figure 87: DHCP Layer 2 Example Network

Perform the following work steps on Switch 1:

- □ Set up the VLAN 2, and specify port 1/1 as a member of VLAN 2.
- □ Open the `Advanced > DHCP L2 Relay > Configuration` dialog, "Interface" tab.
- □ Specify the settings for port 1/1 as follows:
  - – Mark the "Active" checkbox.
- □ Specify the settings for port 1/2 as follows:
  - – Mark the "Active" checkbox.
  - – Mark the "Trusted Port" checkbox.
- □ Open the "VLAN" tab.
- □ Specify the settings for VLAN 2 as follows:
  - – Mark the "Active" checkbox.
  - – Mark the "Circuit ID" checkbox.
  - – To use the IP address of the device as the Remote ID, in the "Remote ID Type" field select the value `ip`.
- □ To enable the function, select in the "Operation" frame the "On" radio button.
- □ To temporarily save the changes, click "Set".
- □ To permanently save the changes, you open the `Basic Settings >` Load/Save dialog and click "Save".

Perform the following work steps on Switch 2:

- □ Open the `Advanced > DHCP L2 Relay > Configuration` dialog, "Interface" tab.

□ Specify the settings for port 1/1 and port 1/2 as follows:
  – Mark the "Active" checkbox.
  – Mark the "Trusted Port" checkbox.

□ To enable the function, select in the "Operation" frame the "On" radio button.

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

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

Verify that VLAN 2 is present then perform the following steps on Switch 1:

□ Set up the VLAN 2, and specify port 1/1 as a member of VLAN 2.

`enable`	Switch to the privileged EXEC mode.
`vlan database`	Switch to the VLAN mode.
`dhcp-l2relay circuit-id 2`	Activate the Circuit ID and the DHCP Option 82 on VLAN2.
`dhcp-l2relay remote-id ip 2`	Specify the IP address of the device as the Remote ID on VLAN2.
`dhcp-l2relay mode 2`	Activate the DHCP Layer 2 Relay function on VLAN2.
`exit`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`interface 1/1`	Change to the Interface Configuration mode of port 1/1.
`dhcp-l2relay mode`	Activate the DHCP Layer 2 Relay function on the port.
`exit`	Switch to the Configuration mode.
`interface 1/2`	Switch to the interface configuration mode for interface 1/2.
`dhcp-l2relay trust`	Specify the port as "Trusted Port".
`dhcp-l2relay mode`	Activate the DHCP Layer 2 Relay function on the port.
`exit`	Switch to the Configuration mode.
`dhcp-l2relay mode`	Enable the DHCP Layer 2 Relay function on the device.

Perform the following work steps on Switch 2:

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`interface 1/1`	Change to the Interface Configuration mode of port 1/1.
`dhcp-l2relay trust`	Specify the port as "Trusted Port".
`dhcp-l2relay mode`	Activate the DHCP Layer 2 Relay function on the port.
`exit`	Switch to the Configuration mode.
`interface 1/2`	Switch to the interface configuration mode for interface 1/2.
`dhcp-l2relay trust`	Specify the port as "Trusted Port".
`dhcp-l2relay mode`	Activate the DHCP Layer 2 Relay function on the port.
`exit`	Switch to the Configuration mode.
`dhcp-l2relay mode`	Enable the DHCP Layer 2 Relay function on the device.

10.3 Using the device as a DNS client (HiOS-2A, HiOS-3S)

The Domain Name System (DNS) client queries DNS servers to resolve host names and IP addresses of network devices. Much like a telephone book, the DNS client converts names of devices into IP addresses. When the DNS client receives a request to resolve a new name it first queries its internal static database, then the assigned DNS servers for the information. The DNS client saves the queried information in a cache for future requests. The device offers the possibility to configure the DNS client from the DHCP server using the management VLAN. The device also offers you the possibility to assign host names to IP addresses statically.

The DNS client provides the following user functions:

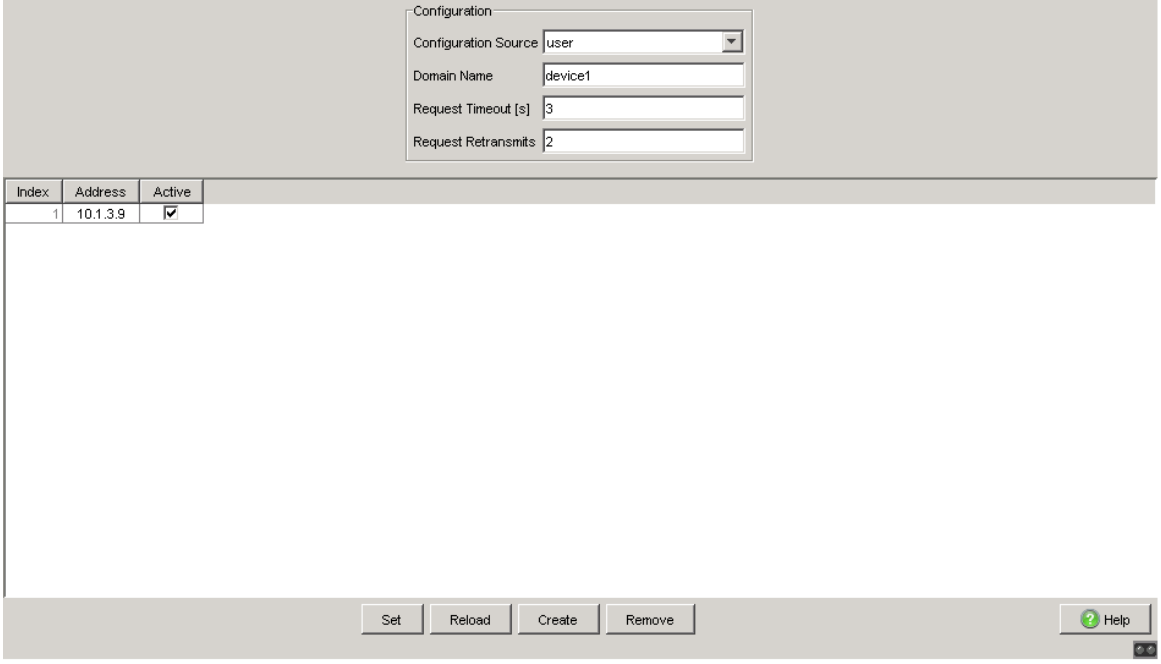
- DNS server list, with space for 4 domain name server IP addresses
- static hostname to IP address mapping, with space for 64 configurable static hosts
- host cache, with space for 128 entries

10.3.1 Configuring a DNS server example

Name the DNS client and configure it to query a DNS server to resolve host names.

- ☐ Open the `Advanced > DNS > Client > Static` dialog.
- ☐ In the "Configuration" frame, select `user` from the "Configuration Source" pull down menu.
- ☐ Enter `device1` for a unique device name in the "Domain Name" text box.
- ☐ To add a new entry to the table, click "Create".
- ☐ Enter `10.1.3.5` for a DNS server in "Address".
- ☐ To enable the entry, click "Active".
- ☐ Open the `Advanced > DNS > Client > Global` dialog.

□ To enable the function, select in the "Operation" frame the "On" radio button.



Configuration

Configuration Source: user

Domain Name: device1

Request Timeout [s]: 3

Request Retransmits: 2

Index	Address	Active
1	10.1.3.9	☑

Figure 88: Advanced:DNS:Server:Static dialog

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`dns client source user`	Sets the function to user to manually configure the DNS client.
`dns client domain-name device1`	Enters device1 as a unique domain name for the device.
`dns client servers add 1 ip 10.1.3.5`	Adds a DNS server with IP address of 10.1.3.5 as index 1.
`dns client adminstate`	Activates the DNS client function.

Configure the DNS client to map static hosts with IP addresses.

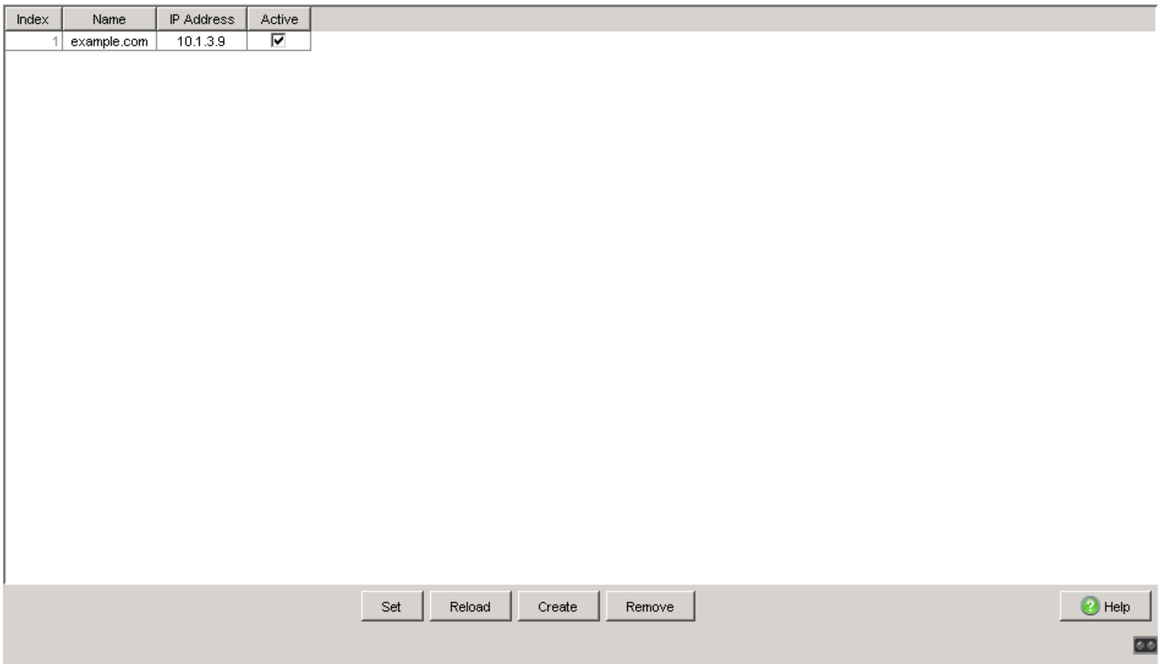
□ Open the `Advanced > DNS > Client > Static Hosts` dialog.

□ To add a new entry to the table, click "Create".

□ In the "Name" cell, enter `example.com` which is a name of a device in the network.

□ In the "IP Address" cell, enter `10.1.3.9`.

□ To enable the entry, click "Active".



Index	Name	IP Address	Active
1	example.com	10.1.3.9	☑

Figure 89: Table in the `Advanced > DNS > Client > Static Hosts` dialog.

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`dns client host add 1 name example.com ip 10.1.3.9`	Adds example.com as a static host with an IP address of 10.1.3.9.
`dns client adminstate`	Activates the DNS client function.

10.4 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
- **Applies to HiOS-2A, HiOS-3S:** DHCP Snooping
- **Applies to HiOS-2A, HiOS-3S:** ARP Rate
- 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`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`auto-disable reason crc-error`	Activate the auto-disable CRC function.
`interface 1/1`	Change to the Interface Configuration mode of port 1/1.
`auto-disable timer 120`	Specifies the elapse reset timer as 120 s for this port.
`auto-disable operation`	Activate the auto-disable function settings for this port.
`auto-disable reset`	Allows you to enable the port before the "Reset Timer [s]" counts down.

10.5 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.

10.5.1 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:
  ≥ (2x 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.

10.5.2 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.

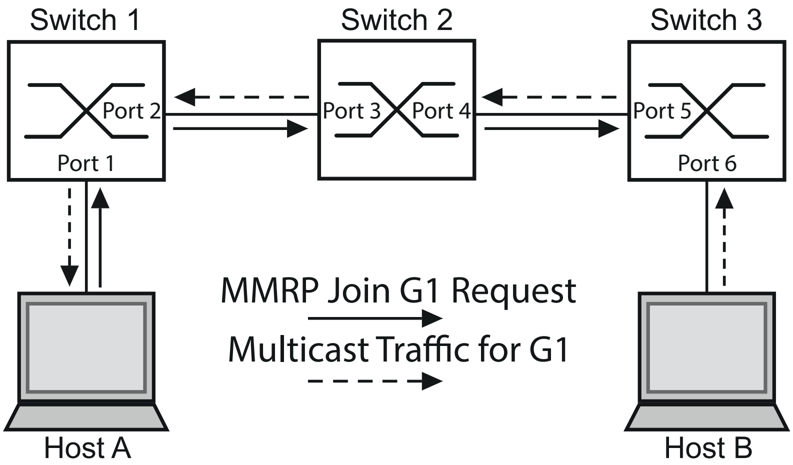


Figure 90: MMRP Network for MAC address Registration

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.

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

`mrp-ieee mrp periodic-state-machine`	Enable the MMRP periodic state machine globally.
`mrp-ieee mmrp operation`	Enable MMRP globally.

10.5.3 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.

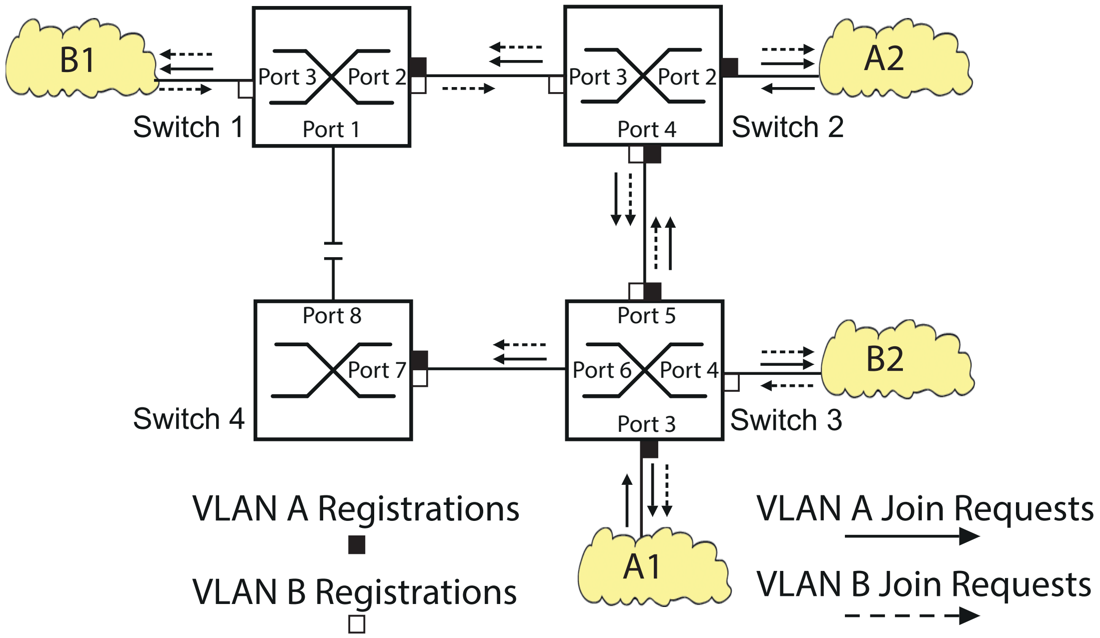


Figure 91: MVRP Example Network for VLAN Registration

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.

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

10.6 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.

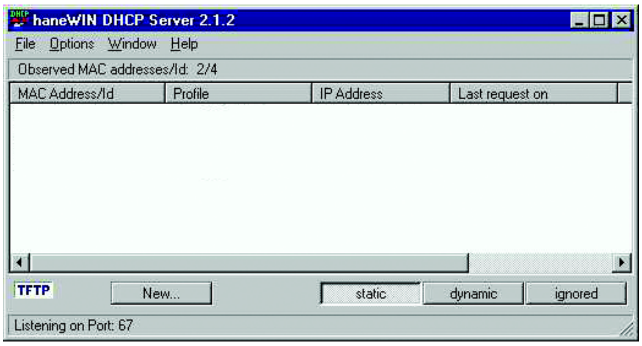
A Setting up the Configuration Environment

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.



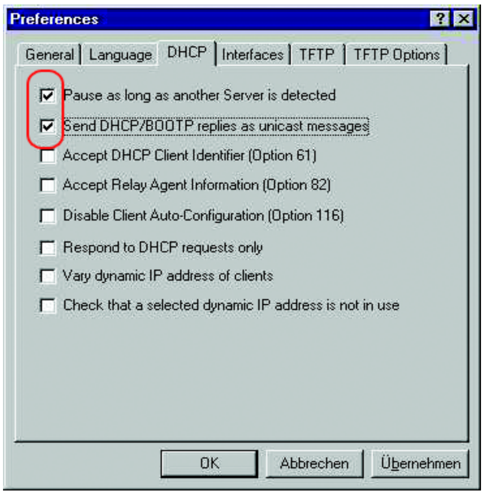
Observed MAC addresses/Id: 2/4

Listening on Port: 67

Figure 92: 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.

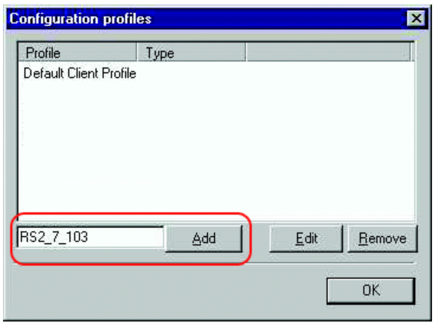
- ☐ Open the window for the program settings in the menu bar: `Options:Preferences` and select the `DHCP` tab page.
- ☐ Enter the settings shown in the illustration and click `OK`.



☑ Pause as long as another Server is detected
☑ Send DHCP/BOOTP replies as unicast messages
☐ Accept DHCP Client Identifier (Option 61)
☐ Accept Relay Agent Information (Option 82)
☐ Disable Client Auto-Configuration (Option 116)
☐ Respond to DHCP requests only
☐ Vary dynamic IP address of clients
☐ Check that a selected dynamic IP address is not in use

Figure 93: 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`.



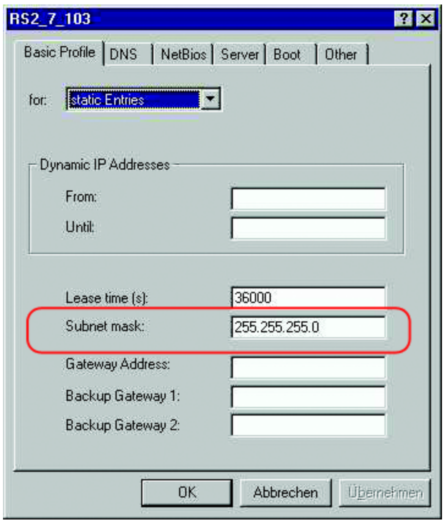
Configuration profiles

Profile	Type
Default Client Profile	

RS2_7_103

Figure 94: Adding configuration profiles

□ Enter the netmask and click `Apply`.



RS2_7_103

for: static Entries

Dynamic IP Addresses

From:

Until:

Lease time (s): 36000

Subnet mask: 255.255.255.0

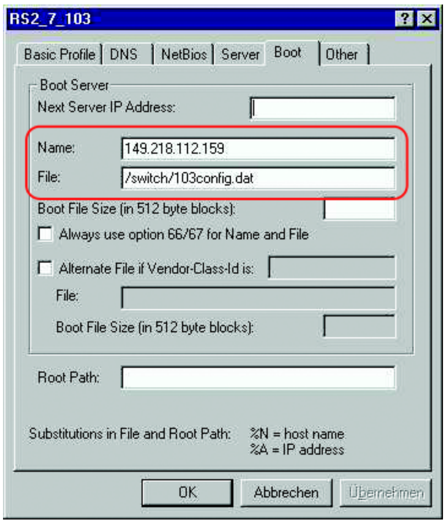
Gateway Address:

Backup Gateway 1:

Backup Gateway 2:

Figure 95: 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`.



Boot Server

Next Server IP Address:

Name: 149.218.112.159

File: /switch/103config.dat

Boot File Size (in 512 byte blocks):

□ Always use option 66/67 for Name and File

□ Alternate File if Vendor-Class-Id is:

File:

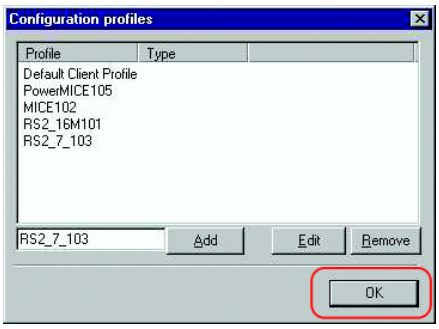
Boot File Size (in 512 byte blocks):

Root Path:

Substitutions in File and Root Path: %N = host name
%A = IP address

Figure 96: 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`.

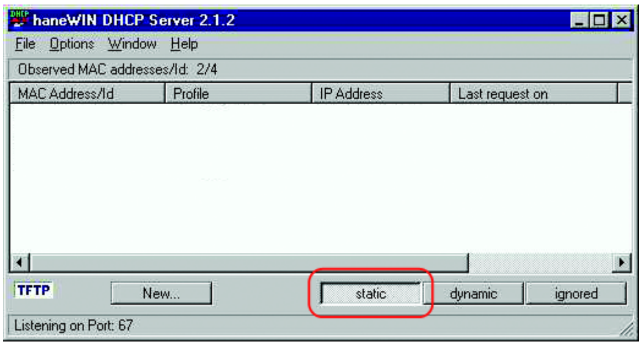


Profile	Type
Default Client Profile	
PowerMICE105	
MICE102	
RS2_16M101	
RS2_7_103	

RS2_7_103

Figure 97: Managing configuration profiles

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

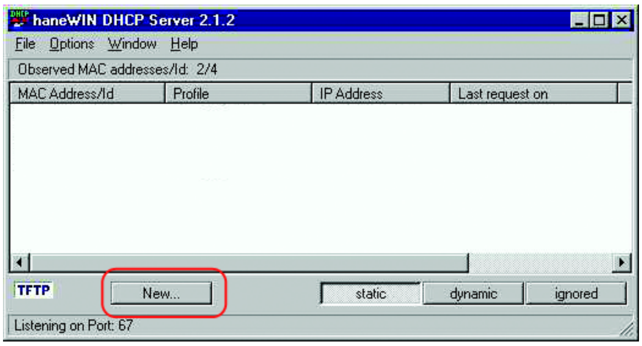


Observed MAC addresses/Id: 2/4

Listening on Port: 67

Figure 98: Static address input

□ Click `New`.



Observed MAC addresses/Id: 2/4

Listening on Port: 67

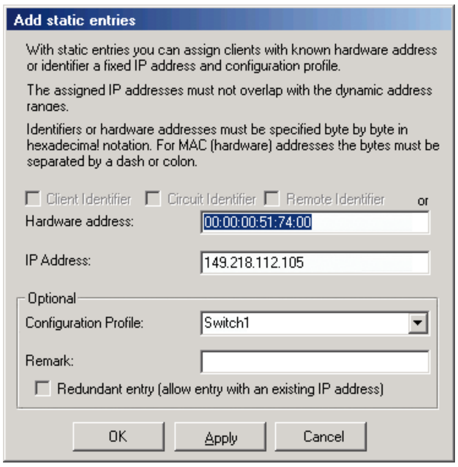
Figure 99: Adding static addresses

□ 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`.



With static entries you can assign clients with known hardware address or identifier a fixed IP address and configuration profile.

The assigned IP addresses must not overlap with the dynamic address ranges.

Identifiers or hardware addresses must be specified byte by byte in hexadecimal notation. For MAC (hardware) addresses the bytes must be separated by a dash or colon.

□ Client Identifier □ Circuit Identifier □ Remote Identifier or

Hardware address: 00:00:00:51:74:00

IP Address: 149.218.112.105

Optional

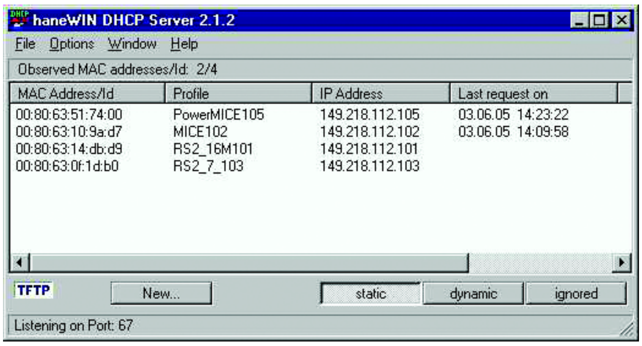
Configuration Profile: Switch1

Remark:

□ Redundant entry (allow entry with an existing IP address)

Figure 100:Entries for static addresses

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



Observed MAC addresses/Id: 2/4

MAC Address/Id	Profile	IP Address	Last request on
00:80:63:51:74:00	PowerMICE105	149.218.112.105	03.06.05 14:23:22
00:80:63:10:9a:d7	MICE102	149.218.112.102	03.06.05 14:09:58
00:80:63:14:db:d9	RS2_16M101	149.218.112.101	
00:80:63:0f:1d:b0	RS2_7_103	149.218.112.103	

Listening on Port: 67

Figure 101:DHCP server with entries

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
`hm2PSState (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. 1.3.6.1.1.4.1.248...)
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.

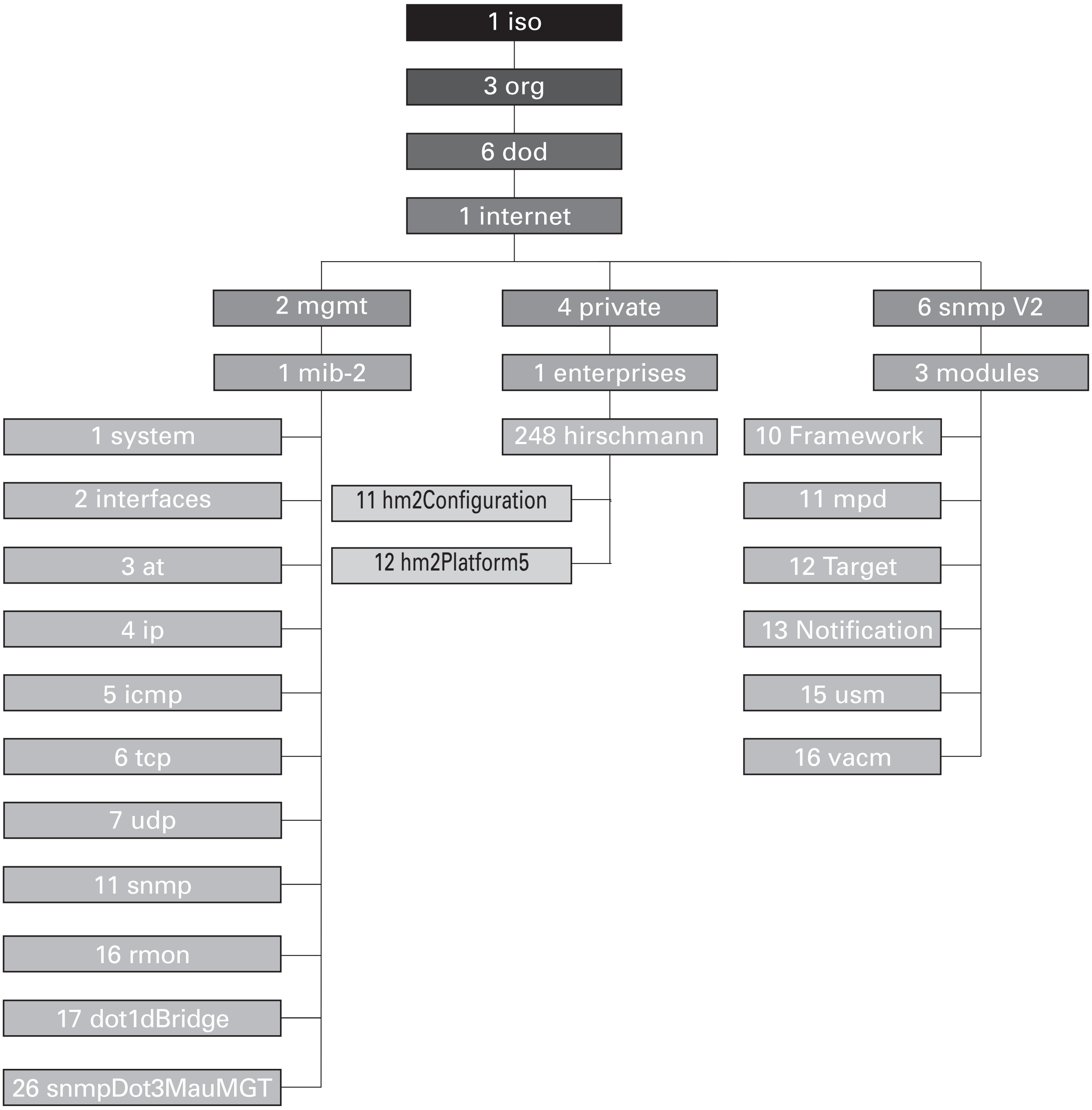


Figure 102:Tree structure of the Hirschmann MIB

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

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	O	O	O	O	O
Readability	O	O	O	O	O
Understandability	O	O	O	O	O
Examples	O	O	O	O	O
Structure	O	O	O	O	O
Comprehensive	O	O	O	O	O
Graphics	O	O	O	O	O
Drawings	O	O	O	O	O
Tables	O	O	O	O	O

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

Suggestions for improvement and additional information:

General comments:

Sender:

Company / Department:

Name / Telephone number:

Street:

Zip code / City:

E-mail:

Date / Signature:

Dear User,

Please fill out and return this page

- as a fax to the number +49 (0)7127/14-1600 or
- per mail to

Hirschmann Automation and Control GmbH
Department 01RD-NT
Stuttgarter Str. 45-51
72654 Neckartenzlingen

C Index

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