PSSnet SHL Series
Managed Ethernet Switches

Industrial Ethernet Switches – PSSnet S

pilz
more than automation
safe automation

Suggestions and comments for improving this documentation will be gratefully received.

Content

About this Manual

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

The following thematic sequence has proven itself in practice:

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

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

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

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

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

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

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

- Configuration of multiple devices simultaneously.
- Graphical interface with network layouts.
- Auto-topology discovery.
- Event log.
- Event handling.
- Client / Server structure.
- Browser interface
- ActiveX control for SCADA integration
- SNMP/OPC gateway

Key

The designations used in this manual have the following meanings:

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

Symbols used:

	Router with firewall
	Switch with firewall
	Router
	Switch
	Bridge

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

Introduction

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

1 Access to the user interfaces

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

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

1.1 System Monitor

The system monitor enables you to

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

Opening the system monitor

☐ Use the terminal cable (see accessories) to connect
  – the V.24 socket (RJ11) to
  – a terminal or a COM port of a PC with terminal emulation based on VT100

  (for the physical connection, see the "Installation" user manual).

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

Table 1: Data transfer parameters

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

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

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

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

Figure 1: Screen display during the boot process

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

```
   System Monitor

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

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


sysMon1>
```

Figure 2: System monitor 1 screen display

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

1.2 Command Line Interface

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

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

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

Opening the Command Line Interface

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

```
        Copyright (c) 2004-2005 Pilz GmbH & Co. KG
                             All rights reserved

                          PSSnet SHL Release L3P-01.0.00-K16

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



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


User:
```

Figure 3: Logging in to the Command Line Interface program

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

The start screen appears.

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


(Hirschmann PowerMICE) >
```

Figure 4: CLI screen after login

1.3 Web-based Interface

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

Opening the Web-based Interface

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

Note: The Web-based interface uses the Java software version 5 or later (Java™ Runtime Environment Version 1.5.x or 6.x). If it is not installed on your computer yet, it will be installed automatically via the Internet when you start the Web-based interface for the first time.

For Windows users: If you don´t have any access to the internet cancel the installation. Install the software from the enclosed CD-ROM. To do this, you go to “Additional Software”, select `Java Runtime Environment` and click on “Installation”.

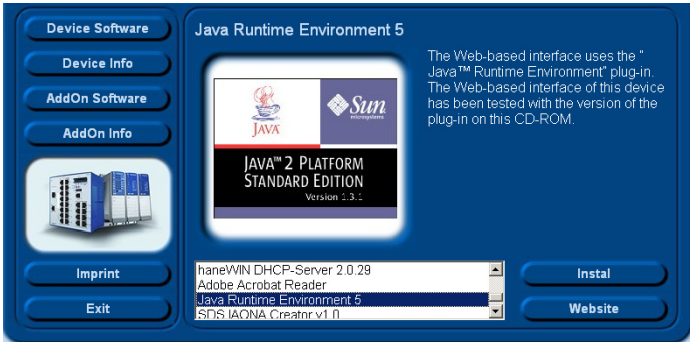


Figure 5: Installing Java

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

  The login window appears on the screen.

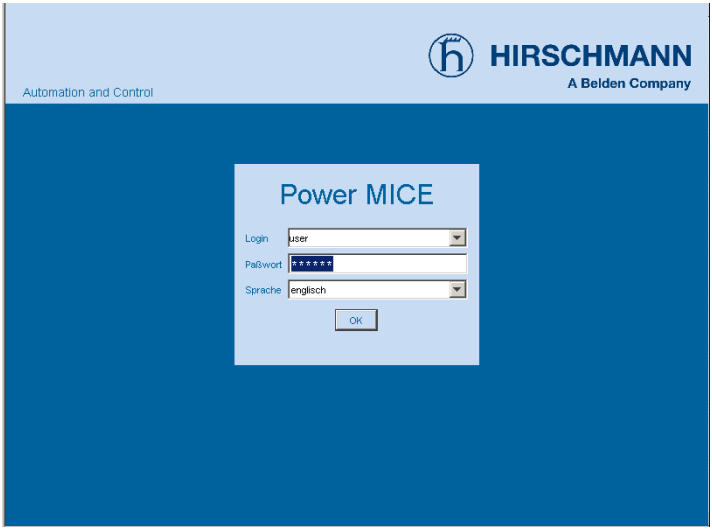


Figure 6: Login window

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

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

The website of the device appears on the screen.

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

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

2 Entering the IP Parameters

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

The device provides 7 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
  - you do not have network access (“in-band”) to the device

  (see page 33 „Entering IP parameters via CLI“).
- Entry using the HiDiscovery protocol.
  You choose this “in-band” method if the device is already installed in the network or if you have another Ethernet connection between your PC and the device
  (see page 36 „Entering the IP Parameters via HiDiscovery“).
- Configuration using the AutoConfiguration Adapter (SCA).
  You choose this method if you are replacing a device with a device of the same type and have already saved the configuration on an SCA (see page 39 „Loading the system configuration from the ACA“).
- Using BOOTP.
  You choose this “in-band” method if you want to configure the installed device using BOOTP. You need a BOOTP server for this. The BOOTP server assigns the configuration data to the device using its MAC address (see page 41 „System configuration via BOOTP“). Because the device is delivered with “DHCP mode” as the entry for the configuration data reference, you have to reset this to the BOOTP mode for this method.
- Configuration via DHCP.
  You choose this “in-band” method if you want to configure the installed device using DHCP. You need a DHCP server for this. The DHCP server assigns the configuration data to the device using its MAC address or its system name (see page 46 „System Configuration via DHCP“).

- Using DHCP Option 82.
  You choose this “in-band” method if you want to configure the installed device using DHCP Option 82. You need a DHCP server with Option 82 for this. The DHCP server assigns the configuration data to the device using its physical connection (see page 49 „System configuration via DHCP Option 82“).
- Configuration via the Web-based interface.
  If the device already has an IP address and can be reached via the network, then the Web-based interface provides you with another option for configuring the IP parameters.

2.1 IP Parameter Basics

2.1.1 IP address (version 4)

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

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

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

Table 2: IP address classes

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

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

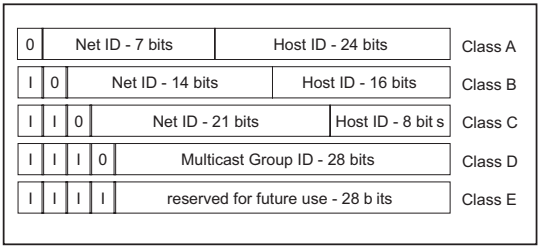


Figure 7: Bit representation of the IP address

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

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

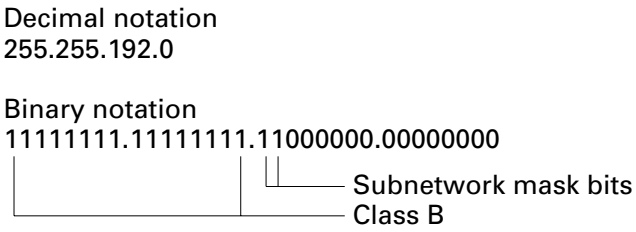
2.1.2 Netmask

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

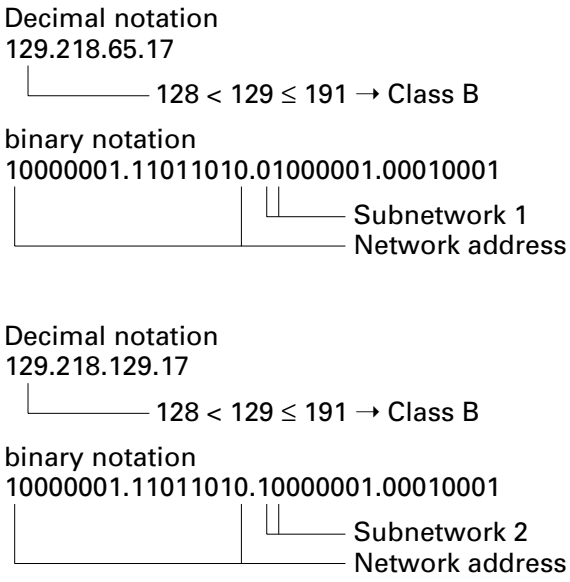
The division into subnetworks with the aid of the netmask is performed in much the same way as the division of the network addresses (net id) into classes A to C.

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

Example of a netmask:



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



Example of how the network mask is used

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

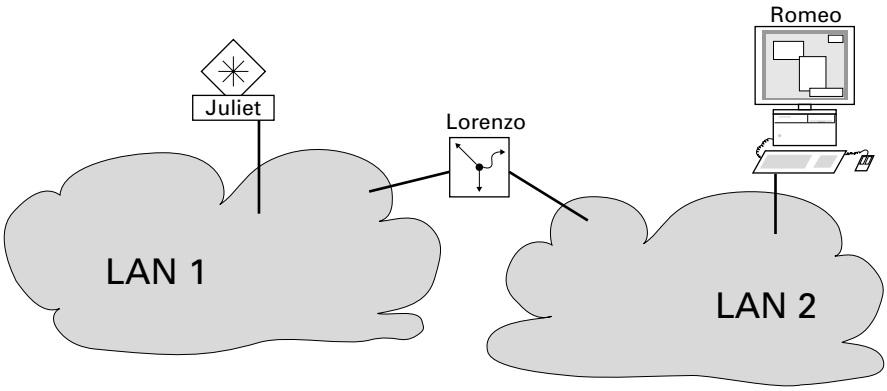


Figure 8: Management agent that is separated from its management station by a router

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

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

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

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

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

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

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

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

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

2.1.3 Classless Inter-Domain Routing

Class C with a maximum of 254 addresses was too small, and class B with a maximum of 65534 addresses was too large for most users, as they would never require so many addresses. This resulted in ineffective usage of the class B addresses available.
Class D contains reserved multicast addresses. Class E is reserved for experimental purposes. A gateway not participating in these experiments ignores datagrams with these destination addresses.

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

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

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

25 mask bits

CIDR notation: 149.218.112.0/25

Mask bits

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

2.2 Entering IP parameters via CLI

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

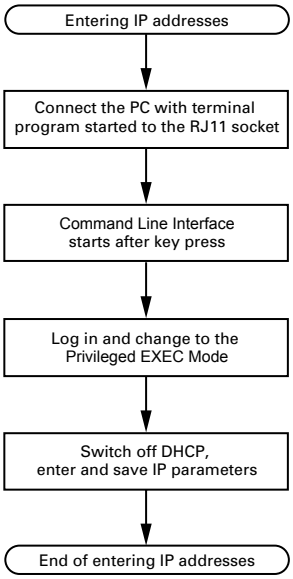


Figure 9: Flow chart for entering IP addresses

Note: If there is no terminal or PC with terminal emulation available in the vicinity of the installation location, you can configure the device at your own workstation, then take it to its final installation location.

☐ Set up a connection to the device (see on page 18 „Opening the Command Line Interface“).

The start screen appears.

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


(Hirschmann PowerMICE) >
```

☐ Deactivate DHCP.

☐ Enter the IP parameters.

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

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

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

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

2.3 Entering the IP Parameters via HiDiscovery

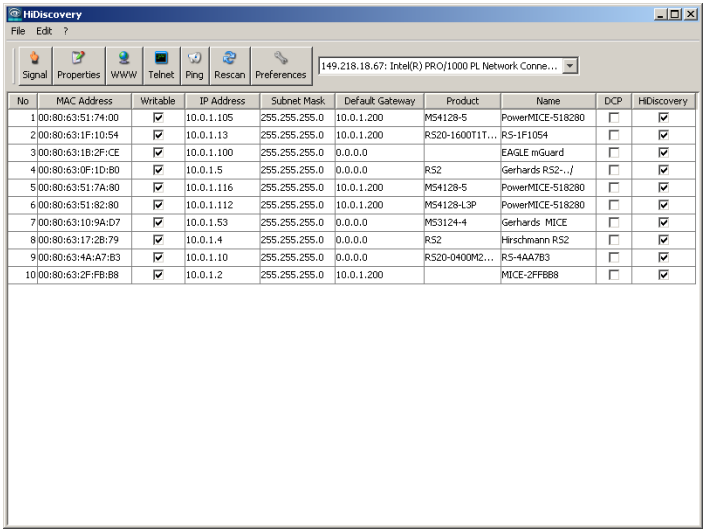
The HiDiscovery protocol enables you to assign IP parameters to the device via the Ethernet.
You can easily configure other parameters via the Web-based interface (see the "Web-based Interface" reference manual).

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

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

Note: The installation of HiDiscovery involves installing the WinPcap Version 3.1 software package.
If an earlier version of WinPcap is already installed on the PC, then follow the suggestion to uninstall it in the setup.
A newer version remains intact when you install HiDiscovery. However, this cannot be guaranteed for all future versions of WinPcap. In the event that the installation of HiDiscovery has overwritten a newer version of WinPcap, you uninstall WinPcap 3.1 and then re-install the new version.

☐ Start the HiDiscovery program.



No	MAC Address	Writable	IP Address	Subnet Mask	Default Gateway	Product	Name	DCP	HiDiscovery
1	00:80:63:51:74:00	☑	10.0.1.105	255.255.255.0	10.0.1.200	MS4128-5	PowerMICE-518280	☐	☑
2	00:80:63:1F:10:54	☑	10.0.1.13	255.255.255.0	10.0.1.200	RS20-1600T1T...	RS-1F1054	☐	☑
3	00:80:63:1B:2F:CE	☑	10.0.1.100	255.255.255.0	0.0.0.0		EAGLE mGuard	☐	☑
4	00:80:63:0F:1D:B0	☑	10.0.1.5	255.255.255.0	0.0.0.0	RS2	Gerhards RS2-../	☐	☑
5	00:80:63:51:7A:80	☑	10.0.1.116	255.255.255.0	10.0.1.200	MS4128-5	PowerMICE-518280	☐	☑
6	00:80:63:51:82:80	☑	10.0.1.112	255.255.255.0	10.0.1.200	MS4128-L3P	PowerMICE-518280	☐	☑
7	00:80:63:10:9A:D7	☑	10.0.1.53	255.255.255.0	0.0.0.0	MS3124-4	Gerhards MICE	☐	☑
8	00:80:63:17:2B:79	☑	10.0.1.4	255.255.255.0	0.0.0.0	RS2	Hirschmann RS2	☐	☑
9	00:80:63:4A:A7:B3	☑	10.0.1.10	255.255.255.0	0.0.0.0	RS20-0400M2...	RS-4AA7B3	☐	☑
10	00:80:63:2F:FB:B8	☑	10.0.1.2	255.255.255.0	10.0.1.200		MICE-2FFB88	☐	☑

Figure 10: HiDiscovery

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

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

HiDiscovery enables you to identify the devices displayed.
☐ Select a device line.
☐ Click on the symbol with the two green dots in the tool bar to set the LEDs for the selected device flashing. To switch off the flashing, click on the symbol again.

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

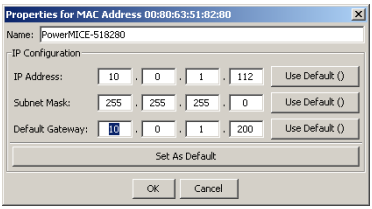


Figure 11: HiDiscovery - assigning IP parameters

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

Note: For security reasons, switch off the HiDiscovery function for the device in the Web-based interface, after you have assigned the IP parameters to the device (see on page 50 „Web-based IP configuration“).

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

2.4 Loading the system configuration from the SCA

The AutoConfiguration Adapter (SCA) is a device for

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

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

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

The password is valid if

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

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

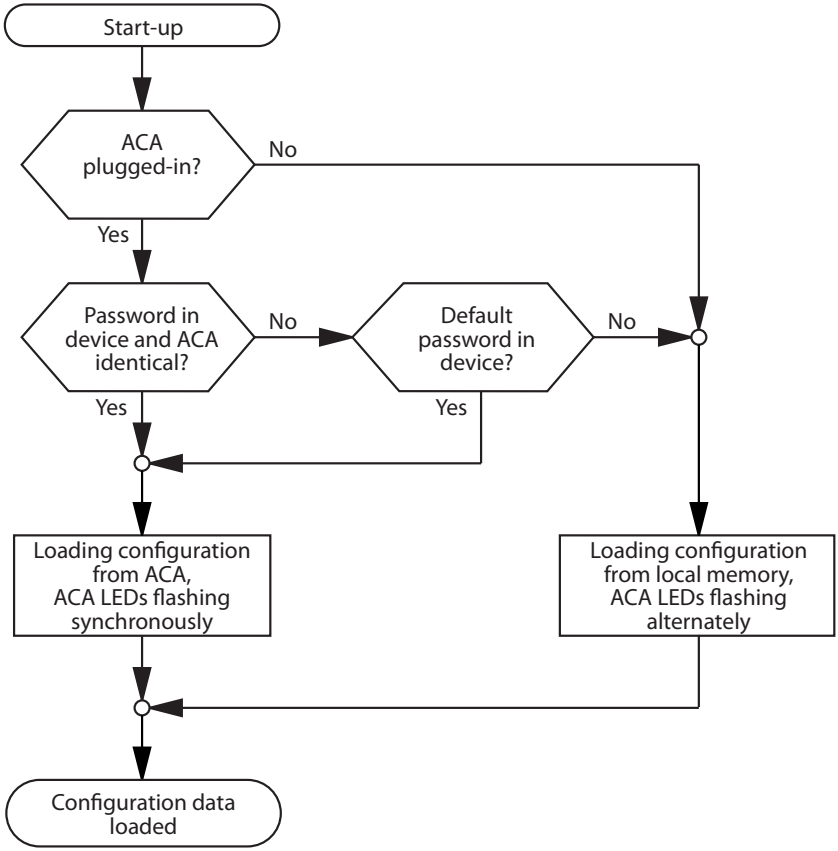


Figure 12: Flow chart of loading configuration data from the SCA

2.5 System configuration via BOOTP

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

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

☐ Activate BOOTP to receive the configuration data (see on page 50 „Web-based IP configuration“) or see in the CLI:

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

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

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

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

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

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

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

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

In the appendix under „Setting up DHCP/BOOTP server“ on page 180 you will find an example for the configuration of a BOOTP/DHCP server.

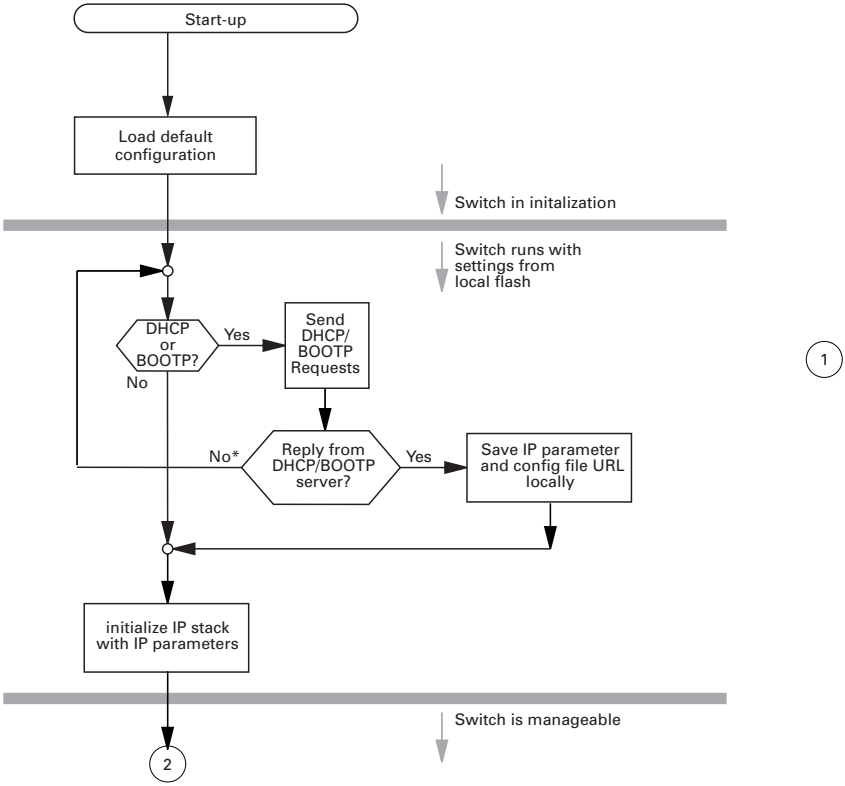


Figure 13: Flow chart for the BOOTP/DHCP process, part 1
** see note fig. 14*

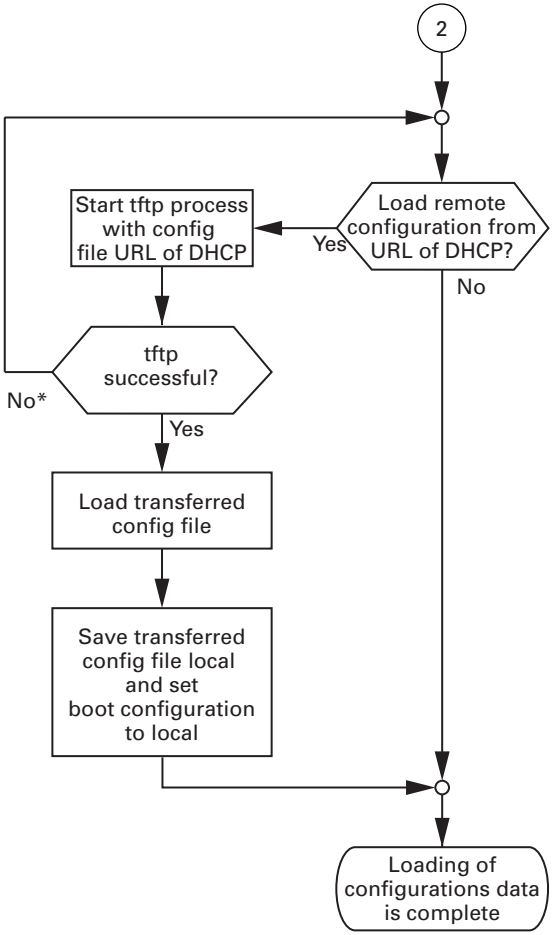


Figure 14: Flow chart for the BOOTP/DHCP process, part 2
** see note*

Note: The loading process started by DHCP/BOOTP (see on page 41 „System configuration via BOOTP“) shows the selection of "from URL & save locally" in the "Load" frame. If you get an error message when saving a configuration, this could be due to an active loading process. DHCP/BOOTP only finishes a loading process when a valid configuration has been loaded. If DHCP/BOOTP does not find a valid configuration, then finish the loading process by loading the local configuration in the "Load" frame.

2.6 System Configuration via DHCP

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

During startup operation, a device receives its configuration data according to the “DHCP process” flowchart (see fig. 13).
The device sends its system name to the DHCP server. The DHCP server can then use the system name to allocate an IP address as an alternative to the MAC address.
In addition to the IP address, the DHCP server sends
– the tftp server name (if available),
– the name of the configuration file (if available).

The device accepts this data as configuration parameters (see on page 50 „Web-based IP configuration“).
If an IP address was assigned by a DHCP server, it will be permanently saved locally.

Option	Meaning
1	Subnet Mask
2	Time Offset
3	Router
4	Time server
12	Host Name
61	Client Identifier
66	TFTP Server Name
67	Bootfile name

Table 3: DHCP options which the device requests

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

On delivery, DHCP is activated.
As long as DHCP is activated, the device attempts to obtain an IP address. If it cannot find a DHCP server after restarting, it will not have an IP address.
To activate/deactivate DHCP (see on page 50 „Web-based IP configuration“).

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

In the appendix, you will find an example for the configuration of a BOOTP/DHCP server (see on page 180 „Setting up DHCP/BOOTP server“).

Example of a DHCP configuration file:

```
# /etc/dhcpd.conf for DHCP Daemon
#
subnet 149.218.112.0 netmask 255.255.240.0 {
option subnet-mask 255.255.240.0;
option routers 149.218.112.96;
}
#
# Host berta requests IP configuration
# with her MAC address
#
host berta {
hardware ethernet 00:80:63:08:65:42;
fixed-address 149.218.112.82;
}
#
# Host hugo requests IP configuration
# with his client identifier.
#
host hugo {
#
option dhcp-client-identifier "hugo";
option dhcp-client-identifier 00:68:75:67:6f;
fixed-address 149.218.112.83;
server-name "149.218.112.11";
filename "/agent/config.dat";
}
```

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

2.7 System configuration via DHCP Option 82

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

While the system configuration is based on the classical DHCP protocol (see on page 46 „System Configuration via DHCP“) on the device being configured, Option 82 is based on the network topology. This procedure gives you the option of always assigning the same IP address to any device which is connected to a particular location (port of a device) on the LAN.
The installation of a DHCP server is described in the chapter „Setting up DHCP Server Option 82“ on page 186.

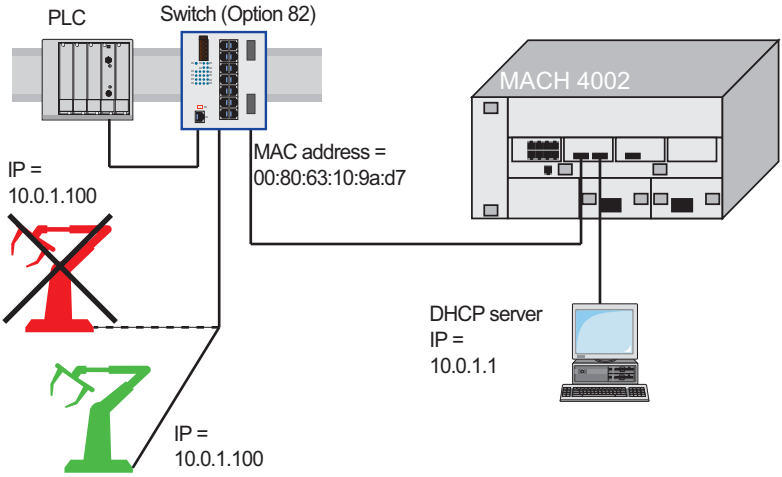


Figure 15: Application example of using Option 82

2.8 Web-based IP configuration

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

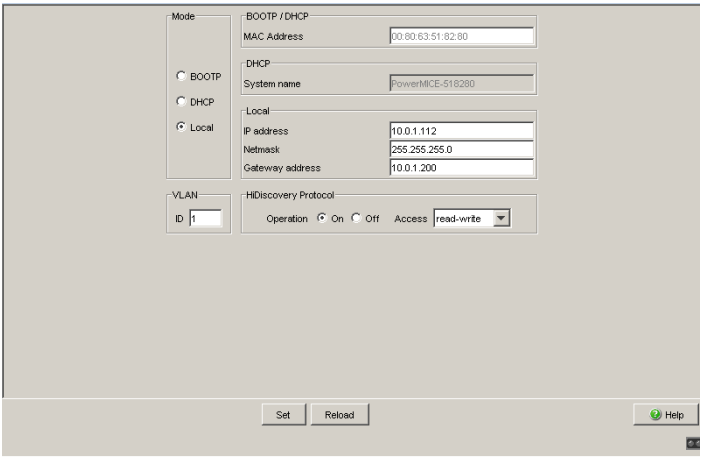


Figure 16: Network parameters dialog

☐ Under "Mode", enter where the device is to obtain its IP parameters:
- In the BOOTP mode, the configuration is via a BOOTP or DHCP server on the basis of the MAC address of the device (see page 180).
- In the DHCP mode, the configuration is via a DHCP server on the basis of the MAC address or the name of the device (see page 186).
- In the local mode the net parameters in the device memory are used.

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

☐ You enter the name applicable to the DHCP protocol in the "Name" line in the system dialog of the Web-based interface.

☐ The "VLAN ID" frame enables you to assign a VLAN to the agent. If you enter the illegal VLAN ID "0" here, the agent can be accessed by all VLANs.

☐ The HiDiscovery protocol allows you to assign an IP address to the device on the basis of its MAC address. Activate the HiDiscovery protocol if you want to assign an IP address to the device from your PC with the enclosed HiDiscovery software (setting on delivery: active).

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

2.9 Faulty device replacement

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

- Configuring the new device via an AutoConfiguration Adapter (see on page 39 „Loading the system configuration from the ACA“) or
- Configuration via DHCP Option 82 (see on page 186 „Setting up DHCP Server Option 82“).

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

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

3 Loading/saving settings

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

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

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

3.1 Loading settings

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

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

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

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

3.1.1 Loading from the local non-volatile memory

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

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

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

3.1.2 Loading from the AutoConfiguration Adapter

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

3.1.3 Loading from a file

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

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

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

Example of loading from a tftp server

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

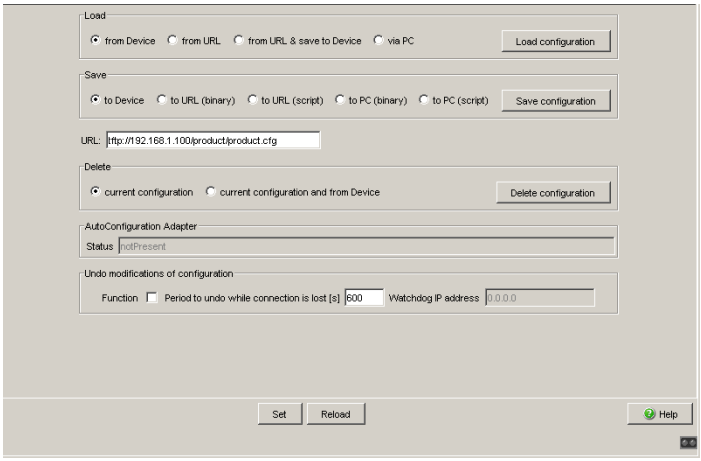


Figure 17: Load/store dialog

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

Note: The loading process started by DHCP/BOOTP (see on page 41 „System configuration via BOOTP“) shows the selection of "from URL & save locally" in the "Load" frame. If you get an error message when saving a configuration, this could be due to an active loading process. DHCP/BOOTP only finishes a loading process when a valid configuration has been loaded. If DHCP/BOOTP does not find a valid configuration, then finish the loading process by loading the local configuration in the "Load" frame.

3.1.4 Resetting the configuration to the state on delivery

The device enables you to

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

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

Setting in the system monitor:

☐ Select `5` “Erase main configuration file”
This menu item allows you to reset the device to its state on delivery. The device saves configurations other than the original one in its Flash memory in the configuration file `*.cfg`.
☐ Press the Enter key to delete the configuration file.

3.2 Saving settings

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

- save the current configuration on the device
- save the current configuration in binary form in a file under the specified URL
- save the current configuration in binary form on the PC

3.2.1 Saving locally (and on the SCA)

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

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

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

Switch to the Privileged EXEC mode.
The device saves the current configuration data in the local non-volatile memory and, if an SCA is connected, also in the SCA

3.2.2 Saving in a file on URL

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

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

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

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

- ☐ Click "Save configuration".

`enable`	Switch to the Privileged EXEC mode.
`copy nvram:startup-config tftp://10.1.112.159/switch/config.dat`	The device saves the configuration data in a binary file on a tftp server in the connected network
`copy nvram:script tftp://10.0.1.159/switch/config.txt`	The device saves the configuration data in a script file on a tftp server in the connected network

3.2.3 Saving as a script on the PC

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

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

4 Loading software updates

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

Checking the software release installed

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

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

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

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

Loading the software

The device gives you three options for loading the software:

- From the SCA(out-of-band)

- Via tftp from a tftp server (in-band)
- Via a file selection dialog from your PC.

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

4.1 Loading the software from the SCA

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

☐ Connect the SCA onto which you copied the device software with the USB port of the device.

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

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

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

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

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

4.1.1 Selecting the software to be loaded

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

```
   Select Operating System Image

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

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

Figure 18: Update operating system screen display

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

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

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

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

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

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

4.1.2 Starting the software

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

4.1.3 Performing a cold start

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

4.2 Loading the software from the tftp server

For a tftp update, you need a tftp server on which the software to be loaded is stored (see on page 190 „tftp server for software updates“).

☐ Select the `Basics:Software` dialog.

The URL identifies the path to the software stored on the tftp server. The URL is in the format tftp://IP address of the tftp server/path name/file name (e.g. `tftp://192.168.1.100/product/product.bin`).

☐ Enter the path of the device software.

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

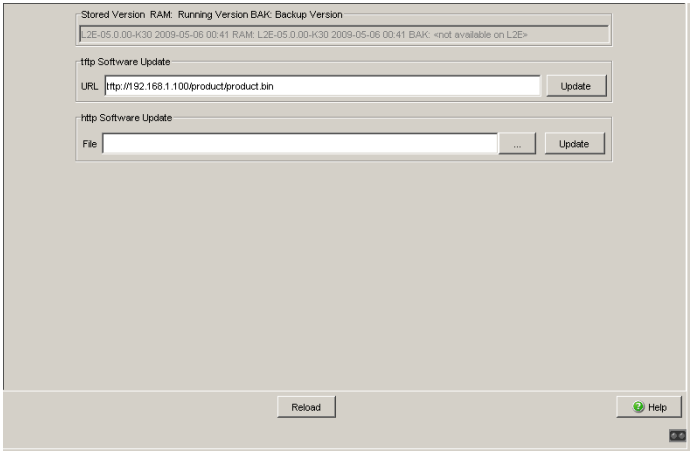


Figure 19: Software update dialog

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

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

`enable`	Switch to the Privileged EXEC mode.
`copy tftp://10.0.1.159/ rsL2E.bin system:image`	Transfer the "rsL2E.bin" software file to the device from the tftp server with the IP address 10.0.1.159.

4.3 Loading the software via file selection

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

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

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

- Update completed successfully.
- Update failed. Reason: incorrect file.
- Update failed. Reason: error when saving.
- File not found (reason: file name not found or does not exist).
- Connection error (reason: path without file name).

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

5 Configuring the ports

The port configuration consists of:

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

Switching the port on and off

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

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

Selecting the operating mode

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

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

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

Displaying connection error messages

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

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

Configuring Power over ETHERNET (if available)

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

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

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

- ☐ In the “POE on” column, you can enable/disable PoE at this port.
- ☐ The “Status” column indicates the PoE status of the port.
- ☐ to “low”, “high” or “critical”.
- ☐ The “Class” column shows the class of the connected device:
  ClassMaximum power delivered
  0: 15.4 W = state on delivery
  1: 4.0 W
  2: 7.0 W
  3: 15,4 W
  4: reserved, treat as class 0
- ☐ The “Name” column indicates the name of the port, see `Basic settings:Port configuration`.

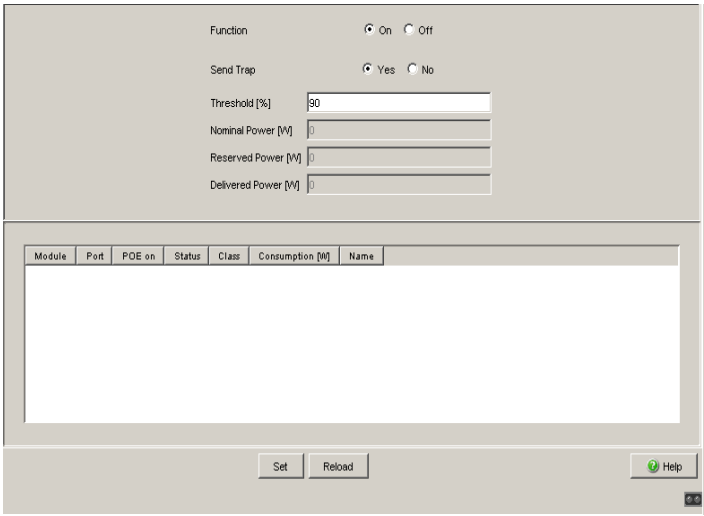


Figure 20: Power over Ethernet dialog

6 Protection from unauthorized access

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

- Password for SNMP access
- Telnet/Web access disabling
- HiDiscovery function disabling
- Port access control via IP or MAC address

6.1 Password for SNMP access

6.1.1 Description of password for SNMP access

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

The device receives the SNMP packet and compares the IP address of the sending computer and the password with the entries in the device MIB (see on page 196 „Management Information Base (MIB)“).
If the password has the appropriate access right, and if the IP address of the sending computer has been entered, then the device will allow access.

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

To protect your device from unwanted access:

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

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

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

6.1.2 Entering the password for SNMP access

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

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

☐ Select "Modify read-only password (user) " to enter the read password.
☐ Enter the new read password in the "New password" line and repeat your entry in the "Please retype" line.
☐ Select "Modify read-write password (admin)" to enter the read/write password.
☐ Enter the read/write password and repeat your entry.

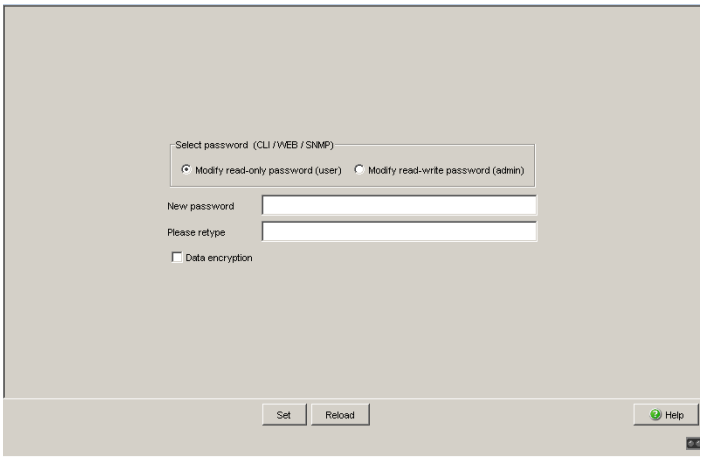


Figure 21: Password dialog

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

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

Note: For security reasons, SNMP version 3 encrypts the password. With the “SNMPv1” or “SNMPv2” setting in the Security:SNMPv1/v2 access dialog, the password is passed on unencrypted and can therefore also be read!

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

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

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

Index	Serial number for this table entry
Password	Password with which this computer can access the device. This password is independent of the SNMPv2 password.
IP address	IP address of the computer that can access the device.

IP mask	IP mask for the IP address
Access mode	The access mode determines whether the computer has read-only or read-write access.
Active	Enable/disable this table entry.

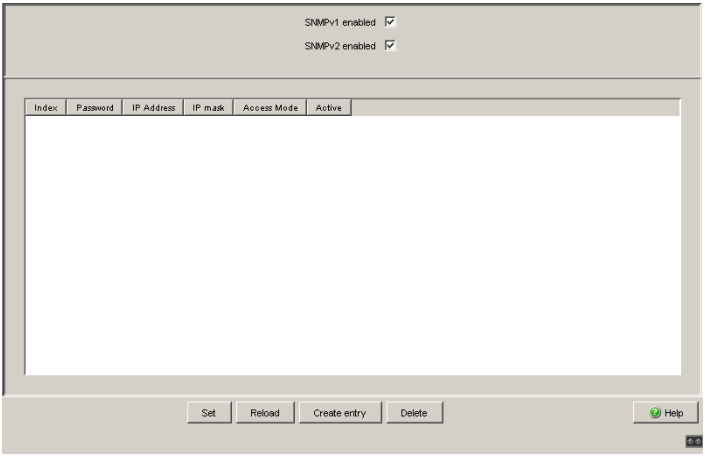


Figure 22: SNMPv1/v2 access dialog

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

6.2 Telnet/Web access

6.2.1 Description of Telnet access

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

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

6.2.2 Description of Web access

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

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

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

6.2.3 Enabling/disabling Telnet/Web access

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

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

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

6.3 Enabling/disabling the HiDiscovery function

6.3.1 Description of the HiDiscovery protocol

The HiDiscovery protocol allows you to assign the device an IP address based on its MAC address (see on page 36 „Entering the IP Parameters via HiDiscovery“). HiDiscovery is a layer 2 protocol.

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

6.3.2 Enabling/disabling the HiDiscovery function

- ☐ Select the `Basics:Network` dialog.
- ☐ Disable the HiDiscovery function in the "HiDiscovery Protocol" frame or limit the access to "read-only".

`enable`	Switch to the Privileged EXEC mode.
`network protocol hidiscovery off`	Disable HiDiscovery function.

`network protocol hidiscovery read-only`	Enable HiDiscovery function with "read-only" access
`network protocol hidiscovery read-write`	Enable HiDiscovery function with "read-write" access

6.4 Port access control

6.4.1 Description of the port access control

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

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

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

6.4.2 Application example for port access control

You have a LAN connection in a room that is accessible to everyone.
To ensure that only defined users can use this LAN connection, you activate the port access control at this port. In the case of unauthorized access, the device is to switch off the port and inform you with an alarm message.
The following is known:

Parameter	Value	Explanation
Allowed IP Addresses	10.0.1.228 10.0.1.229	The defined users are the device with the IP address 10.0.1.228 and the device with the IP address 10.0.1.229
Action	portDisab	Disable the port with the corresponding entry in the port configuration table (see on page 71 „Configuring the ports“) and send an alarm

Prerequisities for further configuration:

- The port for the LAN connection is enabled and configured correctly (see on page 71 „Configuring the ports“)
- Prerequisites for the device to be able to send an alarm (trap) (see on page 155 „Configuring traps“):
  - You have entered at least one recipient
  - You have set the flag in the “Active” column for at least one recipient
  - In the “Selection” frame, you have selected “Port Security”

☐ Configure the port security.

☐ Select the `Security:Port Security` dialog.

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

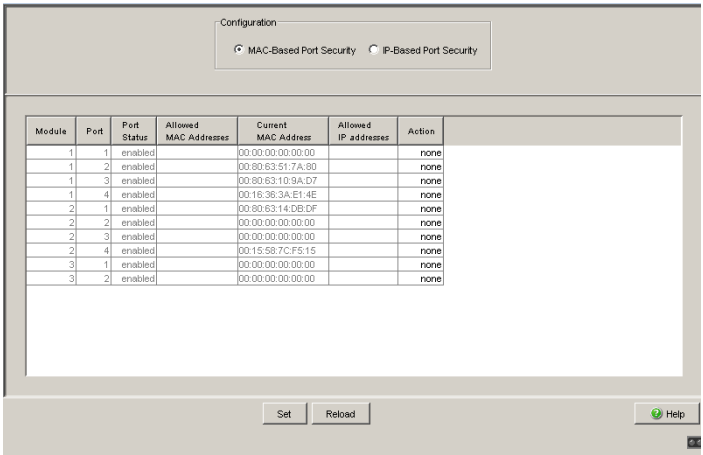


Figure 23: Port Security dialog

☐ Save the settings in the non-volatile memory.

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

7 Synchronizing the system time in the network

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

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

If you only require an accuracy in the order of milliseconds, the Simple Network Time Protocol (SNTP) provides a low-cost solution. The accuracy depends on the signal runtime.

Examples of application areas include:
- log entries
- time stamping of production data
- production control, etc.

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

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

7.1 Entering the time

If no reference clock is available, you have the option of entering the system time in a device and then using it like a reference clock.(see on page 94 „Configuring SNTP“).

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

☐ Select the `Time` dialog.

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

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

- The “System time” uses the “IEEE 1588 / SNTP time”, allowing for the local time difference from “IEEE 1588 / SNTP time”.
  “System time” = “IEEE 1588 / SNTP time” + “Local offset”.
- “Time source” displays the source of the following time data. The device automatically selects the source with the greatest accuracy.

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

☐ The “Local Offset” is for displaying/entering the time difference between the local time and the “IEEE 1588 / SNTP time”.

With “Set offset from PC”, the agent determines the time zone on your PC and uses it to calculate the local time difference.

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

7.2 SNTP

7.2.1 Description of SNTP

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

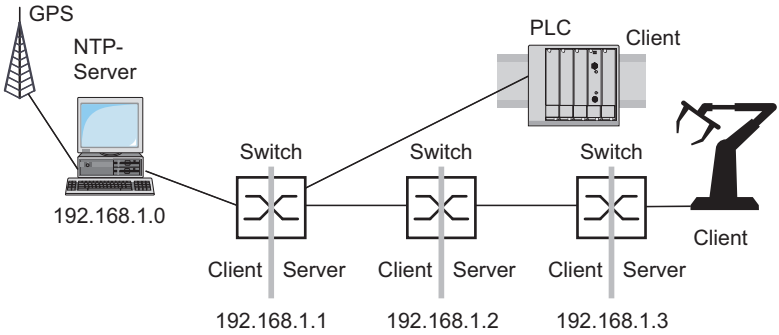


Figure 24: SNTP cascade

7.2.2 Preparing the SNTP coordination

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

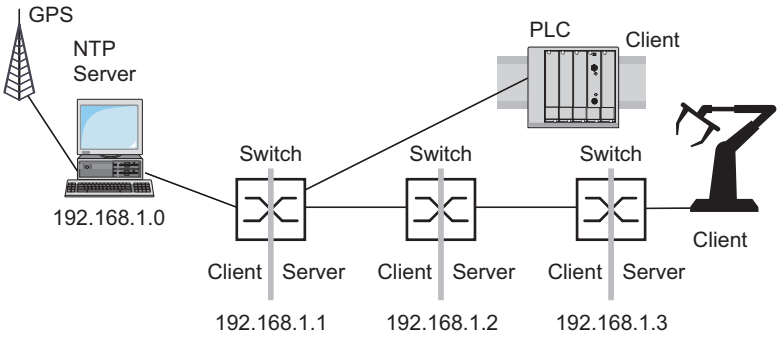


Figure 25: Example of SNTP cascade

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

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

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

7.2.3 Configuring SNTP

☐ Select the `Time:SNTP` dialog.

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

▶ SNTP Status
- ☐ The “Status message” displays conditions such as “Server 1 is not responding”.

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

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

Table 4: Periodic sending of SNTP packets

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

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

  - ☐ In “Server request interval” you specify the interval at which the device requests SNTP packets (valid entries: 1 second to 3600 seconds, on delivery: 30 seconds).
  - ☐ With “Accept SNTP Broadcasts” the device takes the system time from SNTP Broadcast/Multicast packets that it receives.

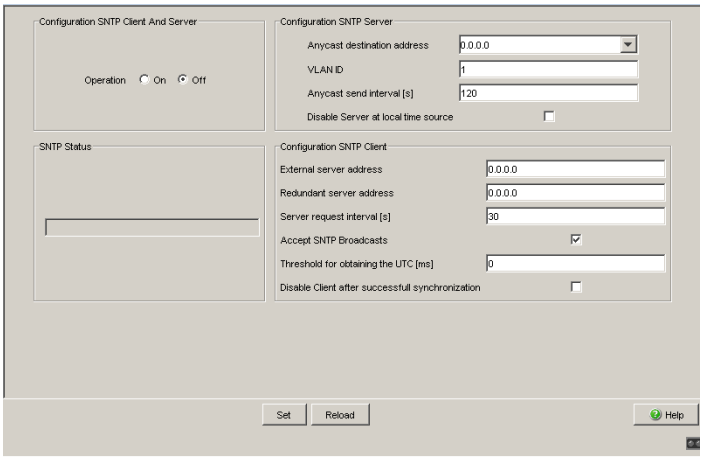


Figure 26: SNTP dialog

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

Table 5: Settings for the example (see fig. 25)

7.3 Precision Time Protocol

7.3.1 Description of PTP functions

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

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

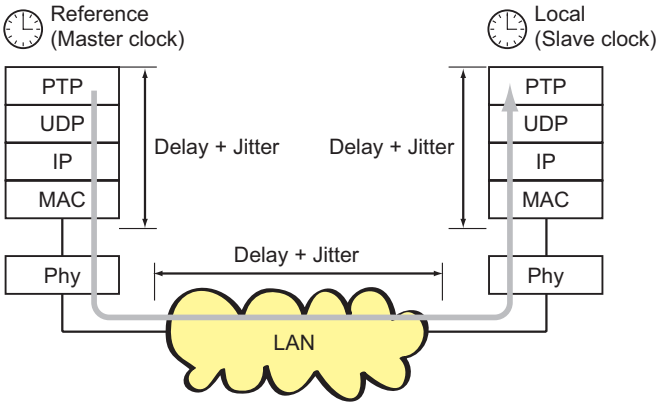
Factors influencing precision are:

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

PTPv1 Stratum number	PTPv2 Clock class	Specification
0	– (priority 1 = 0)	For temporary, special purposes, in order to assign a higher accuracy to one clock than to all other clocks in the network.
1	6	Indicates the reference clock with the highest degree of accuracy. The clock can be both a boundary clock and an ordinary clock. Stratum 1/ clock class 6 clocks include GPS clocks and calibrated atomic clocks. A stratum 1 clock cannot be synchronized using the PTP from another clock in the PTP system.
2		Indicates the second-choice reference clock.
3	187	Indicates the reference clock that can be synchronized via an external connection.
4	248	Indicates the reference clock that cannot be synchronized via an external connection. This is the standard setting for boundary clocks.
5–254	–	Reserved.
255	255	Such a clock should never be used as the best master clock.

Table 6: Stratum – classifying the clocks

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



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

Figure 27: Delay and jitter problems when synchronizing clocks

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

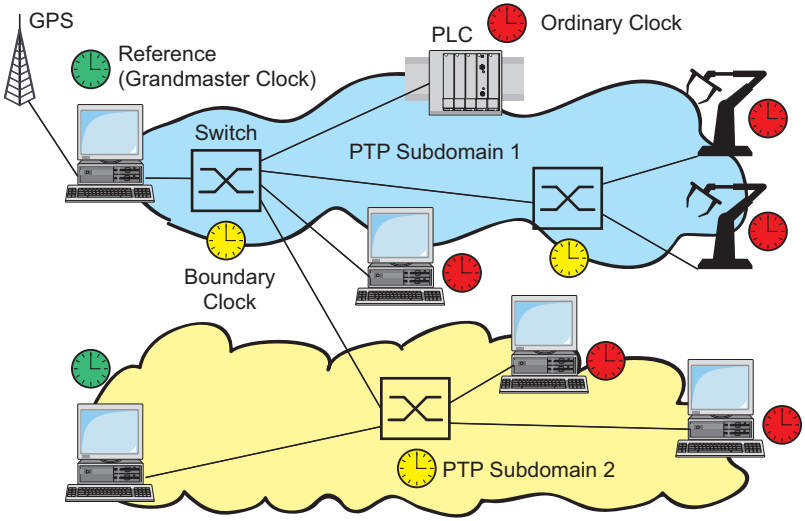


Figure 28: PTP Subdomains

8 Network load control

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

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

8.1 Direct packet distribution

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

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

8.1.1 Store-and-forward

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

8.1.2 Multi-address capability

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

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

in the destination address field are sent to this port. The device enters learned source addresses in its filter table (see on page 104 „Entering static address entries“).
The device can learn up to 8000 addresses. This is necessary if more than one terminal device is connected to one or more ports. It is thus possible to connect several independent subnetworks to the device.

8.1.3 Aging of learned addresses

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

Note: A reboot deletes the learned address entries.

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

8.1.4 Entering static address entries

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

The following are valid filter criteria:

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

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

- The management administrator describes the static part of the filter table (`dot1qStaticTable`).
- During operation, the device is capable of learning which of its ports receive data packets from which source address (see on page 102 „Multi-address capability“). This information is written to a dynamic part (`dot1qTpFdbTable`).
- Addresses learned dynamically from neighboring agents and those learned via GMRP are written to the other dynamic part.

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

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

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

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

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

- `learned`: the filter was created automatically by the device.
- `invalid`: with this status you delete a manually created filter.
- `permanent`: the filter is stored permanently in the device or on the URL (see on page 59 „Saving settings“).
- `gmrp`: the filter was created by GMRP.
- `gmrp/permanent`: GMRP added further port markings to the filter after it was created by the administrator. The port markings added by the GMRP are deleted by a restart .
- `igmp`: the filter was created by IGMP.

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

8.1.5 Disabling the direct packet distribution

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

☐ Select the `Switching:Global` dialog.

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

8.2 Multicast application

8.2.1 Description of the Multicast application

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

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

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

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

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

8.2.2 Example of a Multicast application

The cameras for monitoring machines normally transmit their images to monitors located in the machine room and to the monitoring room. In an IP transmission, a camera sends its image data with a Multicast address via the network.

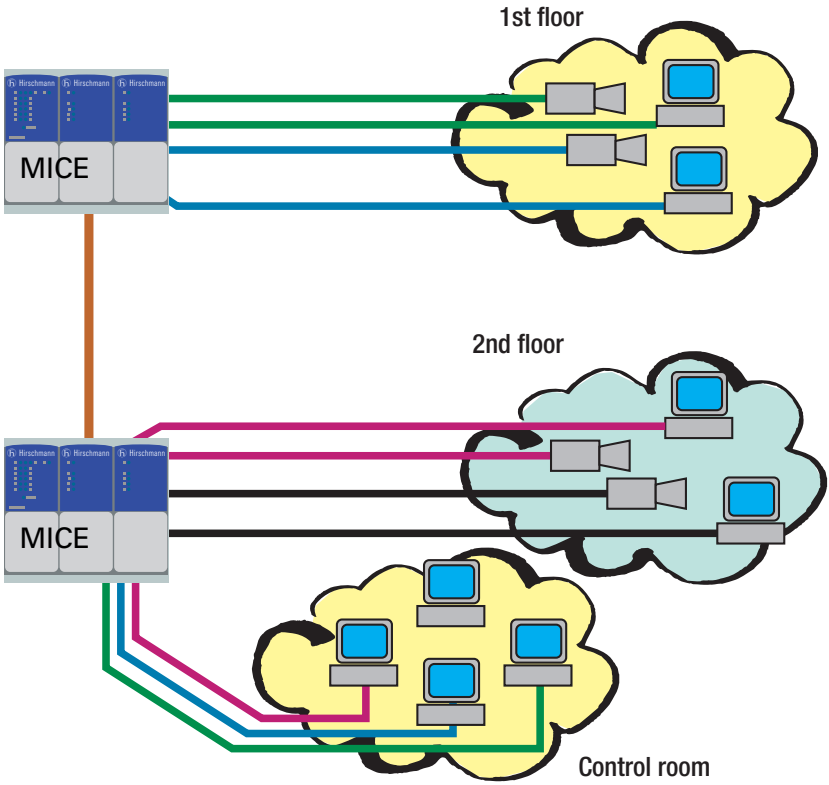


Figure 29: Example: Video surveillance in machine rooms

8.2.3 Description of IGMP Snooping

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

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

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

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

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

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

8.2.4 Setting up the Multicast application

☐ Select the `Switching:Multicasts` dialog.

Global Configuration

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

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

"inactive" disables IGMP Snooping.

IGMP Querier and IGMP settings

With these frames you can enter global settings for the IGMP settings.
Prerequisite: In the `Switching:Multicasts:Global Settings` dialog, the `IGMP Snooping` mode is selected.

IGMP Querier

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

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

In “Send interval” you specify the interval at which the device sends query packets (valid entries: 2-3599 s, default setting: 125 s).
Note the connection between the parameters Max. Response Time, Send Interval and Group Membership Interval (see on page 112 „Parameter values“).

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

Current querier IP address

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

In “Max. Response Time” you specify the period within which the Multicast group members respond to a query (valid values: 1-3598 s, default setting: 10 s).
Note the connection between the parameters Max. Response Time, Send Interval and Group Membership Interval (see on page 112 „Parameter values“).

The Multicast group members select a random value within the response time for their response, to prevent all the Multicast group members responding to the query at the same time.
Select a large value if you want to reduce the load on your network and can accept the resulting longer switching times.
Select a small value if you require short switching times and can accept the resulting network load.

Group Membership Interval

In “Group Membership Interval” you specify the period for which a dynamic Multicast group remains entered in the device if it does not receive any report messages (valid values: 3-3600 s, default setting: 260 s).
Note the connection between the parameters Max. Response Time, Send Interval and Group Membership Interval (see on page 112 „Parameter values“).

Parameter values

The parameters
– Max. Response Time,
– Send Interval and
– Group Membership Interval
have a relationship to each other:

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

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

Parameter	Protocol Version	Value range	Default setting
Max. Response Time	1, 2 3	1-25 seconds 1-3598 seconds	10 seconds
Send Interval	1, 2, 3	2-3599 seconds	125 seconds
Group Membership Interval	1, 2, 3	3-3600 seconds	260 seconds

Table 7: Value range for
- Max. Response Time
- Send Interval
- Group Membership Interval

Unknown Multicasts

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

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

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

Known Multicasts

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

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

Settings per port (table)

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

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

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

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

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

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

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

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

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

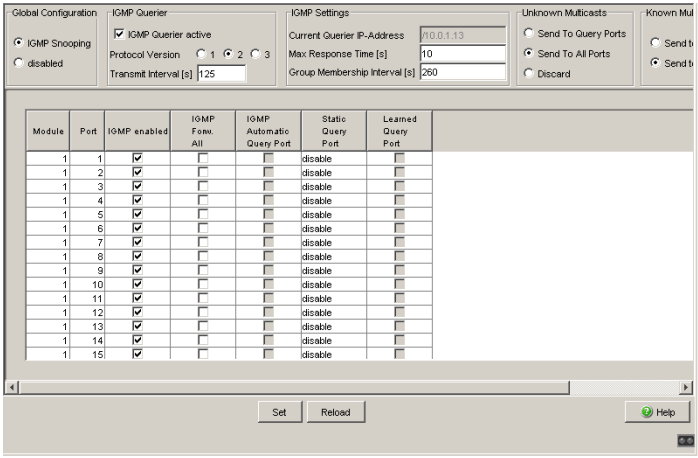


Figure 30: Multicasts dialog

8.3 Rate Limiter

8.3.1 Description of the Rate Limiter

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

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

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

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

8.3.2 Rate Limiter settings

☐ Select the `Switching:Rate Limiter` dialog.

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

Setting options per port:

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

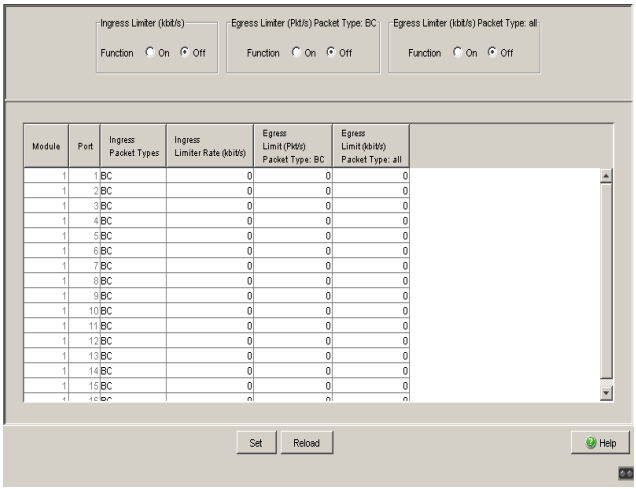


Figure 31: Rate Limiter

8.4 QoS/Priority

8.4.1 Description of Prioritization

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

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

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

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

Data packets can contain prioritizing/QoS information:

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

8.4.2 VLAN tagging

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

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

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

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

Table 8: Assignment of the priority entered in the tag to the four traffic classes

Note: Network protocols and redundancy mechanisms use the highest traffic class 3. Therefore, you select other traffic classes for application data.

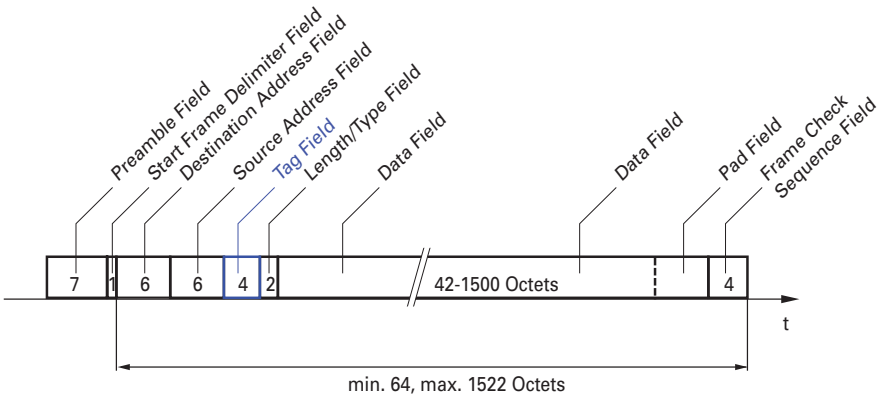


Figure 32: Ethernet data packet with tag

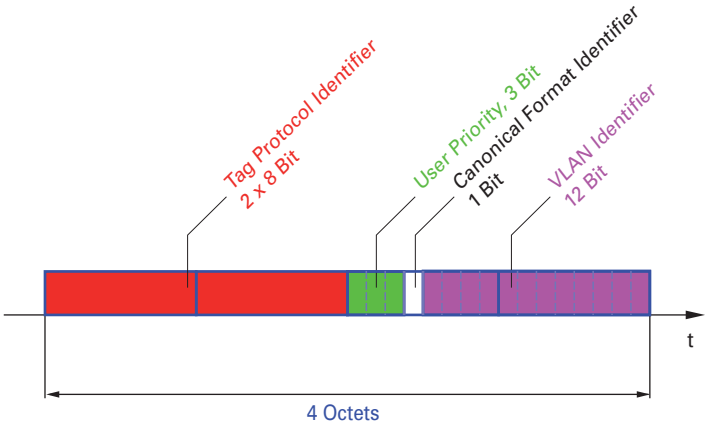


Figure 33: Tag format

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

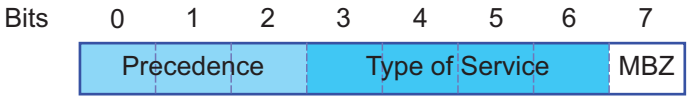
- The additional 4-byte VLAN tag enlarges the data packets. With small data packets, this leads to a larger bandwidth load.

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

8.4.3 IP ToS / DiffServ

TYPE of Service

The Type of Service (ToS) field in the IP header (see table 9) has been part of the IP protocol from the start, and it is used to differentiate various services in IP networks. Even back then, there were ideas about differentiated treatment of IP packets, due to the limited bandwidth available and the unreliable connection paths. Because of the continuous increase in the available bandwidth, there was no need to use the ToS field. Only with the real-time requirements of today's networks has the ToS field become significant again. Selecting the ToS byte of the IP header enables you to differentiate between different services. However, this field is not widely used in practice.



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

Table 9: ToS field in the IP header

Differentiated Services

The newly defined Differentiated Services field in the IP header in RFC 2474 (see fig. 34) - often known as the DiffServ Code Point or DSCP, replaces the ToS field and is used to mark the individual packets with a DSCP. Here the packets are divided into different quality classes. The first three bits of the DSCP are used to divide the packets into classes. The next three bits are used to further divide the classes on the basis of different criteria. In contrast to the ToS byte, DiffServ uses six bits for the division into classes. This results in up to 64 different service classes.

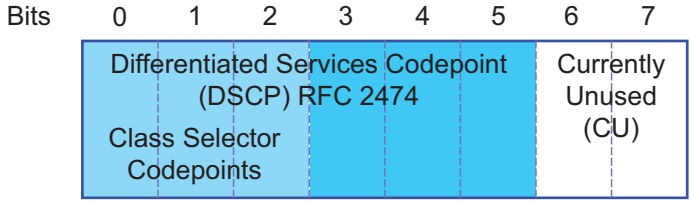


Figure 34: Differentiated Services field in the IP header

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

- Class Selector (CS0-CS7): For reasons of compatibility to TOS/IP Precedence
- Expedited Forwarding (EF): Premium service. Reduced delay, jitter + packet loss (RFC 2598)

- Assured Forwarding (AF): Provides a differentiated schema for handling different data traffic (RFC 2597).
- Default Forwarding/Best Effort: No particular prioritizing.

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

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

Table 10: Assigning the IP precedence values to the DSCP value

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

Table 11: Mapping the DSCP values onto the traffic classes

8.4.4 Management prioritizing

In order for you to have full access to the management of the device, even when there is a high network load, the device enables you to prioritize management packets.
In prioritizing management packets (SNMP, Telnet, etc.), the device sends the management packets with priority information.

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

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

8.4.5 Handling of received priority information

The device provides three options, which can be chosen globally for all ports, for selecting how it handles received data packets that contain priority information.

- trust dot1p
  The device assigns VLAN-tagged packets to the different traffic classes according to their VLAN priorities. The assignment is based on the pre-defined table (see on page 119 „VLAN tagging“). You can modify this assignment. The device assigns the port priority to packets that it receives without a tag.

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

- trust ip-dscp
  The device assigns the IP packets to the different traffic classes according to the DSCP value in the IP header, even if the packet was also VLAN-tagged. The assignment is based on the pre-defined values (see table 11). You can modify this assignment.
  The device prioritizes non-IP packets according to the port priority.

8.4.6 Handling of traffic classes

For the handling of traffic classes, the device provides:

- Strict Priority

Description of Strict Priority

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

8.4.7 Setting prioritization

Assigning the port priority

☐ Select the `QoS/Priority:Port Configuration` dialog.
☐ In the “Port Priority” column, you can specify the priority (0-7) with which the device sends data packets which it receives without a VLAN tag at this port.

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

`enable`	Switch to the Privileged EXEC mode.
`configure`	Switch to the Configuration mode.

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

```
vlan priority 3
```
Assign port priority 3 to interface 1/1.

```
exit
```
Switch to the Configuration mode.

Assigning the VLAN priority to the traffic classes

```
enable
```
Switch to the Privileged EXEC mode.

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

```
classofservice dot1p-mapping 0 4
classofservice dot1p-mapping 1 4
```
Assign traffic class 4 to VLAN priority 0. Also assign traffic class 4 to VLAN priority 1.

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

```
show classofservice dot1p-mapping
```
Display the assignment.

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

Assigning the traffic class to a DSCP

```
enable
```
Switch to the Privileged EXEC mode.

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

```
classofservice ip-dscp-mapping cs1 1
```
Assign traffic class 1 to DSCP CS1.

```
show classofservice ip-dscp-mapping

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

Always assign the DSCP priority to received IP data packets globally

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

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

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

Configuring Layer 2 management priority

☐ Configure the VLAN ports to which the device sends management packets as a member of the VLAN that sends data packets with a tag (see on page 134 „Examples of VLANs“).

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

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

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

Configuring Layer 3 management priority

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

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

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

8.5 Flow control

8.5.1 Description of flow control

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

The example (see fig. 35) shows a graphic illustration of how the flow control works. Workstations 1, 2 and 3 want to simultaneously transmit a large amount of data to Workstation 4. The combined bandwidth of Workstations 1, 2 and 3 to the device is larger than the bandwidth of Workstation 4 to the device. This leads to an overflow of the send queue of port 4. The funnel on the left symbolizes this status.

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

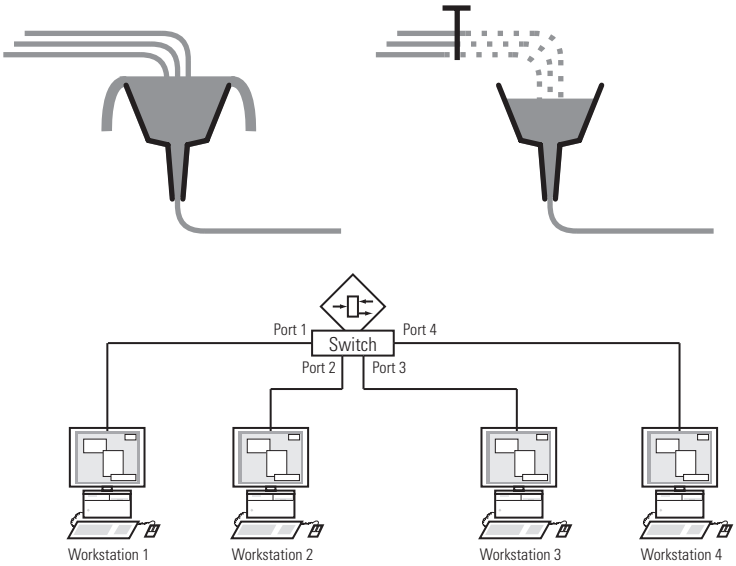


Figure 35: Example of flow control

- **Flow control with a full duplex link**
  In the example (see fig. 35) there is a full duplex link between Workstation 2 and the device.
  Before the send queue of port 2 overflows, the device sends a request to Workstation 2 to include a small break in the sending transmission.

- **Flow control with a half duplex link**
  In the example (see fig. 35) there is a half duplex link between Workstation 2 and the device.
  Before the send queue of port 2 overflows, the device sends data back so that Workstation 2 detects a collision and interrupts the sending process.

8.5.2 Setting the flow control

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

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

8.6 VLANs

8.6.1 VLAN description

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

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

The IEEE 802.1Q standard defines the VLAN function.

The most important benefits of VLANs are:

- Network load limiting
  VLANs can reduce the network load considerably as a Switch only transmits Broadcast/Multicast data packets and Unicast packets with unknown (unlearned) destination addresses within the virtual LAN. The rest of the data network is unaffected by this.

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

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

8.6.2 Examples of VLANs

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

Example 1

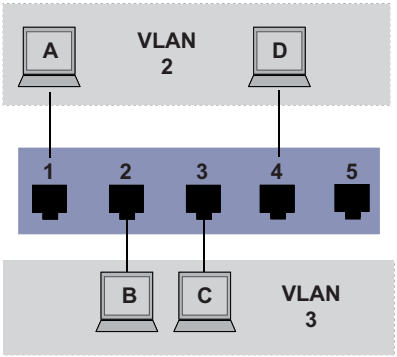


Figure 36: Example of a simple port-based VLAN

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 to which VLAN the frames sent from this port are assigned. Your entry also defines whether Ethernet frames sent from this port are to be tagged:

- T = with TAG field (T = tagged)
- U = without TAG field (U = untagged)

For the above example, the status of the TAG field of the data packets is not relevant, so you can generally 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

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

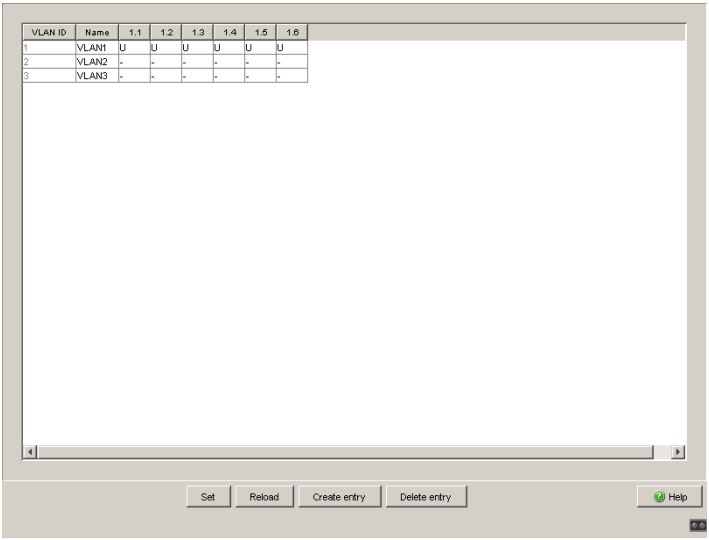


Figure 37: Creating and naming new VLANs

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

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

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

☐ Configuring the ports

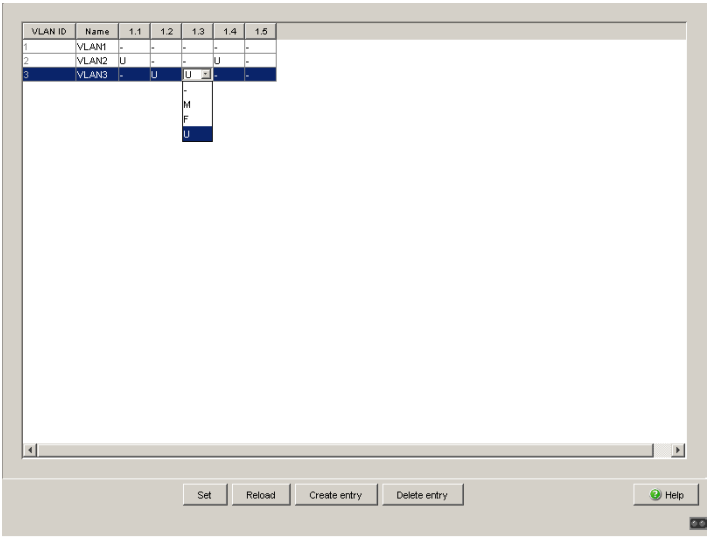


Figure 38: Defining the VLAN membership of the ports.

☐ 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 do not interpret data packets with a tag, you select the `U` setting here.

☐ Click on “Set” to temporarily save the entry in the configuration.

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

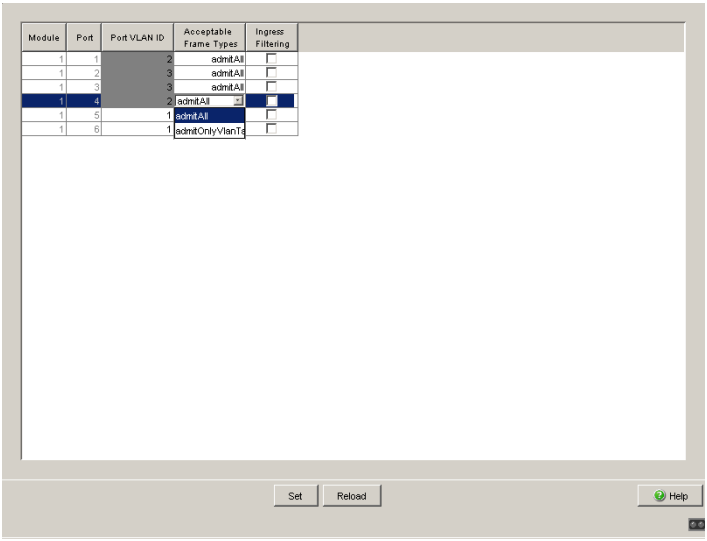


Figure 39: Assign and save Port VLAN ID, Acceptable Frame Types and Ingress Filtering

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

`enable`	Switch to the Privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`interface 1/1`	Switch to the Interface Configuration mode of interface 1/1.
`vlan participation include 2`	Port 1/1 becomes member untagged in VLAN 2.
`vlan pvid 2`	Port 1/1 is assigned the port VLAN ID 2.
`exit`	Switch to the Configuration mode.
`interface 1/2`	Switch to the interface configuration mode of 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 3`	Show details for VLAN 3.

```
VLAN ID           : 3
VLAN Name         : VLAN3
VLAN Type         : Static
VLAN Creation Time: 0 days, 02:52:26 (System Uptime)
Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1         Exclude   Autodetect   Tagged
1/2         Include   Include      Untagged
1/3         Include   Include      Untagged
1/4         Exclude   Autodetect   Tagged
1/5         Exclude   Autodetect   Tagged
```

Example 2

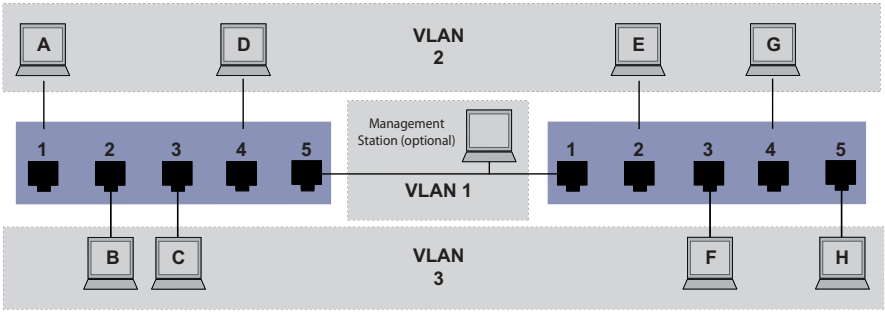


Figure 40: Example of a more complex VLAN constellation

The second example shows a more complex constellation with 3 VLANs (1 to 3). Along with the Switch from example 1, a second Switch (on the right in the example) is now used.
The terminal devices of the individual VLANs (A to H) are spread over two transmission devices (Switches). Such VLANs are therefore known as distributed VLANs. An optional Management Station is also shown, which enables access to all network components if it is configured correctly.

Note: In this case, VLAN 1 has no significance for the terminal device communication, but it is required to maintain 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 two transmission devices (uplink), the ports transport packets for both VLANs. To differentiate these, “VLAN tagging” is used, which prepares the packets accordingly (see on page 119 „VLAN tagging“). This ensures that the assignments to the respective VLANs is maintained.

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 to which VLAN the frames sent from this port are assigned. Your entry also defines whether Ethernet frames sent from this port are to be tagged:

- T = with TAG field (T = tagged)
- U = without TAG field (U = untagged)

In this example, tagged frames are used in the communication between the transmission devices (uplink), as frames for different VLANs are differentiated at these ports.

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
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 at ports 1 and 4 of the left device and terminal devices at ports 2 and 4 of the right device are members of VLAN 2 and can thus communicate with each other. The behavior is the same for the terminal devices at ports 2 and 3 of the left device and the terminal devices at ports 3 and 5 of the right device. These belong to VLAN 3.
The terminal devices “see” their respective part of the network and cannot reach any other participant outside their VLAN. Broadcast and Multicast data packets, and Unicast packets with unknown (unlearned) target addresses as also only sent within a VLAN.

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

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

Proceed as follows to perform the example configuration:

☐ Configure VLAN

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

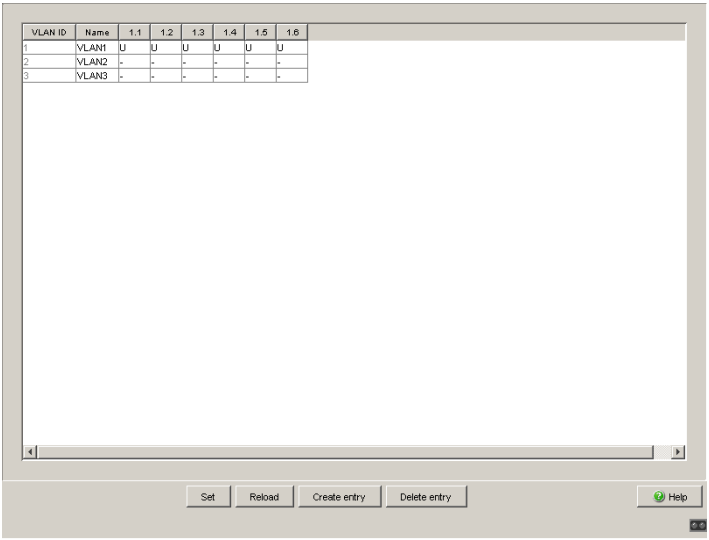


Figure 41: Creating and naming new VLANs

☐ Click on “Create Entry” to open a window for entering the VLAN ID.

☐ Assign VLAN ID 2 to the VLAN.

☐ You give this VLAN the name VLAN2 by clicking on the mask and entering the name. Also change the name for VLAN 1 from “Default” to “VLAN1”.

☐ Repeat the previous steps and create another VLAN with the VLAN ID 3 and the name “VLAN3”.

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

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

☐ Configuring the ports

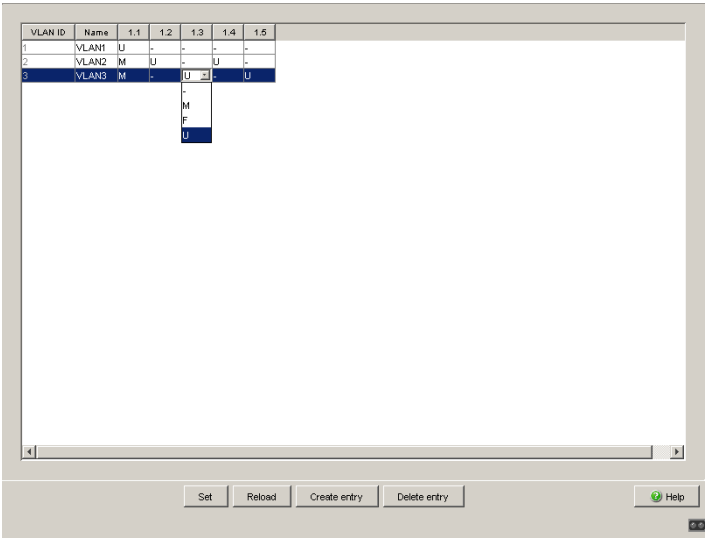


Figure 42: Defining the VLAN membership of the ports.

☐ 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 do not interpret data packets with a tag, you select the `U` setting. You only select the `T` setting at the uplink port at which the VLANs communicate with each other.

☐ Select “Write” to save your settings temporarily.

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

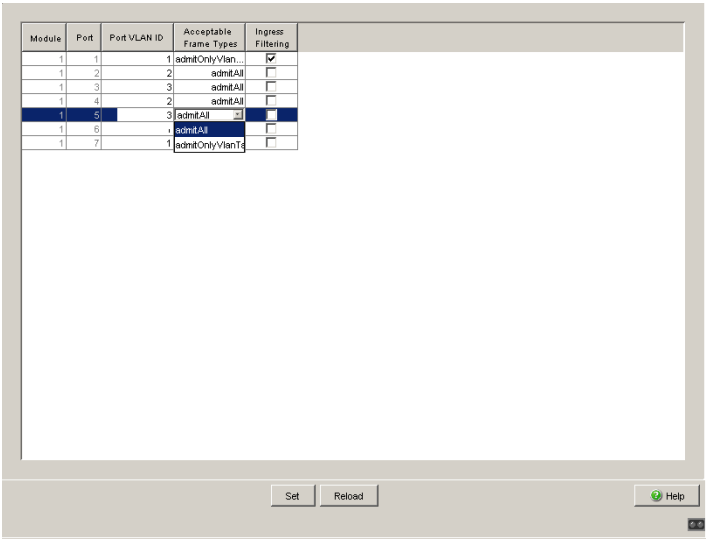


Figure 43: Assign and save Port VLAN ID, Acceptable Frame Types and Ingress Filtering

- ☐ Assign the ID of the related VLANs (1 to 3) to the individual ports.
- ☐ Because terminal devices usually do not send data packets with a tag, you select the `admitAll` setting for the terminal device ports. Configure the uplink port with `admit only VLAN tags`.
- ☐ Activate `Ingress Filtering` at the uplink port so that the VLAN tag is evaluated at this port.
- ☐ Click on “Write” to accept the new settings temporarily.
- ☐ Select the dialog `Basic Settings:Load/Save` to save the example configuration permanently.

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

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

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

9 Operation diagnosis

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

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

9.1 Sending traps

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

Examples of such events are:

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

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

9.1.1 SNMP trap listing

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

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

Table 18: Possible traps

9.1.2 SNMP traps when booting

The device sends the ColdStart trap during every booting.

9.1.3 Configuring traps

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

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

☐ Select "Create entry".

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

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

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

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

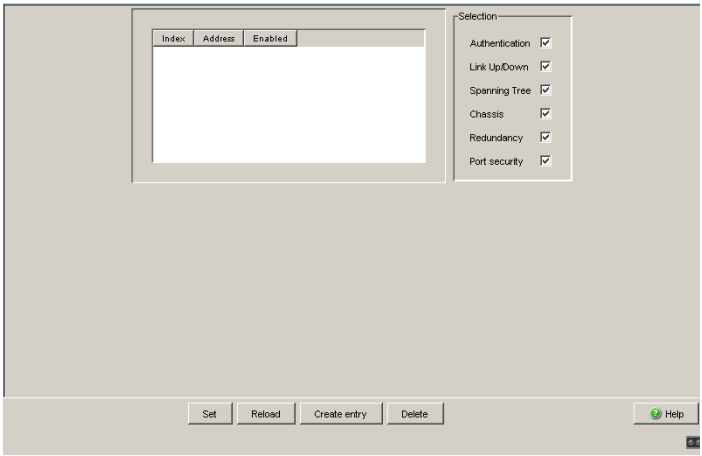


Figure 44: Alarms dialog

The events which can be selected are:

Name	Meaning
Authentication	The device has rejected an unauthorized access attempt (see the `Access for IP Addresses and Port Security` dialog).
Link Up/Down	At one port of the device, the link to a device connected there has been established/interrupted.
Spanning Tree	The topology of the Rapid Spanning Tree has changed.
Chassis	Summarizes the following events: – The status of a supply voltage has changed (see the System dialog). – The status of the signal contact has changed. To take this event into account, you activate “Create trap when status changes” in the `Diagnostics:Signal Contact 1/2` dialog. – A media module was added or removed. – The AutoConfiguration AdapterACA was added or removed. – The temperature threshold was exceeded/not reached. – The receiver power status of a port with an SFP module has changed (see dialog `Dialog:Ports:SFP Modules`).
Redundancy	The redundancy status of the ring redundancy (redundant line active/inactive) or the redundant Ring/Network coupling (redundancy exists) has changed.
Port security	On one port a data packet has been received from an unauthorized terminal device (see the `Port Security` dialog).

Table 19: Trap categories

9.2 Monitoring the device status

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

- signal the device status out-of-band via a signal contact (see on page 161 „Monitoring the device status via the signal contact“)
- signal the device status by sending a trap when the device status changes
- detect the device status in the Web-based interface on the system side.
- query the device status in the Command Line Interface.

The device status of the device includes:

- Incorrect supply voltage,
  the failure of at least one of the two supply voltages,
  a permanent fault in the device (internal supply voltage).
- The temperature threshold has been exceeded or has not been reached.
- The removal of a module (for modular devices).
- The removal of the SCA.
- The interruption of the connection at at least one port. In the `Basic Settings:Port Configuration` menu, you define which ports the device signals if the connection is down (see on page 72 „Displaying connection error messages“). On delivery, there is no link monitoring.
- Event in the ring redundancy:
  Failure of the redundancy (in ring manager mode). On delivery, there is no ring redundancy monitoring.
- Event in the ring/network coupling:
  Failure of the redundancy. On delivery, there is no ring redundancy monitoring.
  The following conditions are also reported by the device in standby mode:
  – Defective link status of the control line
  – Partner device is in standby mode

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

Note: With non-redundant voltage supply, the device reports the absence of a supply voltage. You can prevent this message by feeding the supply voltage over both inputs, or by switching off the monitoring (see on page 162 „Monitoring the device functions via the signal contact“).

9.2.1 Configuring the device status

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

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

Note: The above CLI commands activate the monitoring and the trapping respectively for all the supported components. If you want to activate or deactivate monitoring only for individual components, you will find the corresponding syntax in the CLI manual or in the help (Input ?) of the CLI console.

9.2.2 Displaying the device status

☐ Select the `Basics:System` dialog.

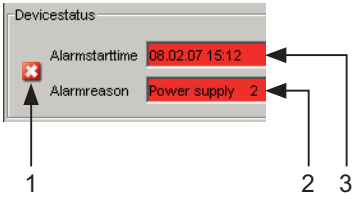


Figure 45: Device status and alarm display
1 - The symbol displays the device status
2 - Cause of the oldest existing alarm
3 - Start of the oldest existing alarm

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

9.3 Out-of-band signaling

The signal contact is used to control external devices and monitor the operation of the device. Function monitoring enables you to perform remote diagnostics.
The device reports the operating status via a break in the potential-free signal contact (relay contact, closed circuit):

- Incorrect supply voltage,
  the failure of at least one of the two supply voltages,
  a permanent fault in the device (internal supply voltage).
- The temperature threshold has been exceeded or has not been reached.
- The removal of a module (for modular devices).
- The removal of the SCA.
- The interruption of the connection at at least one port. In the `Basic Settings:Port Configuration` menu, you define which ports the device signals if the connection is down (see on page 72 „Displaying connection error messages“). On delivery, there is no link monitoring.
- Event in the ring redundancy:
  Failure of the redundancy (in ring manager mode). On delivery, there is no ring redundancy monitoring.
- Event in the ring/network coupling:
  Failure of the redundancy. On delivery, there is no ring redundancy monitoring.
  The following conditions are also reported by the device in standby mode:
  – Defective link status of the control line
  – Partner device is in standby mode

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

Note: With non-redundant voltage supply, the device reports the absence of a supply voltage. You can prevent this message by feeding the supply voltage over both inputs, or by switching off the monitoring (see on page 162 „Monitoring the device functions via the signal contact“).

9.3.1 Controlling the signal contact

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

Application options:

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

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

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

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

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

`enable`	Switch to the 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.

9.3.2 Monitoring the device status via the signal contact

The "Device Status" option enables you, like in the operation monitoring, to monitor the device state (see on page 157 „Monitoring the device status“) via the signal contact.

9.3.3 Monitoring the device functions via the signal contact

Configuring the operation monitoring

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

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

Displaying the signal contact

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

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

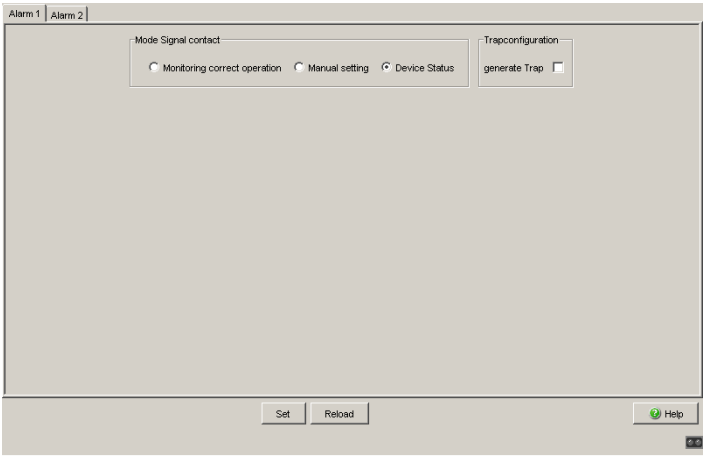


Figure 46: Signal Contact dialog

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

9.4 Port status indication

☐ Select the `Basics:System` dialog.
The device view shows the device with the current configuration. The symbols underneath the device view represent the status of the individual ports.

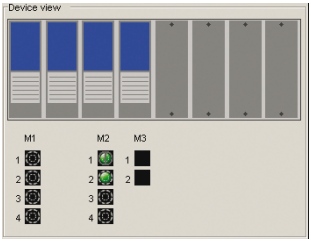


Figure 47: Device view

Meaning of the symbols:


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


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


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


The port is in autonegotiation mode.


The port is in HDX mode.


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


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

9.5 Event counter at port level

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

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

Table 20: Examples indicating possible problems

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

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

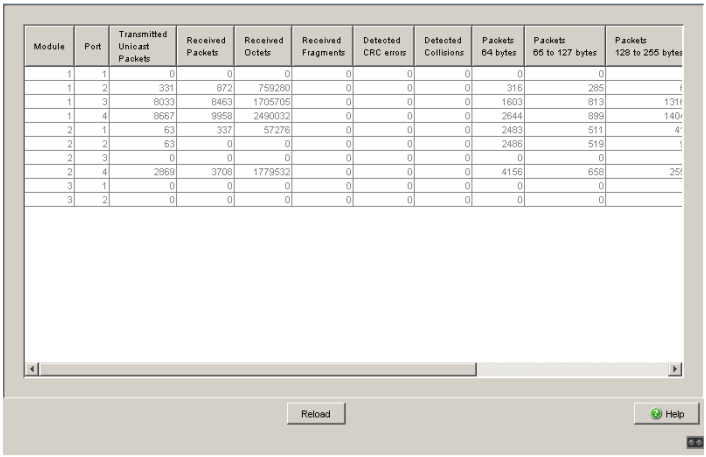


Figure 48: Port Statistics dialog

9.6 Displaying the SFP status

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

- module type
- support provided in media module
- Temperature in º C
- Tx Power in mW
- Receive power in mW

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

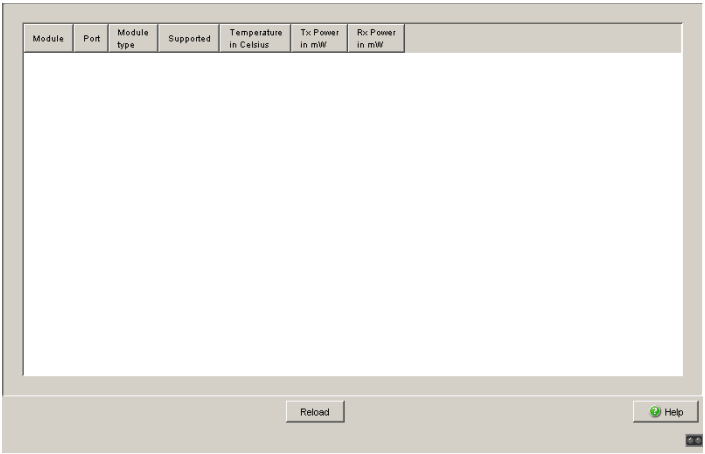


Figure 49: SFP Modules dialog

9.7 Topology discovery

9.7.1 Description of topology discovery

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

A device with active LLDP

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

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

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

- Information about the VLANs of which the port is a member (VLAN ID and VLAN name).

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

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

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

9.7.2 Displaying the topology discovery

☐ Select the `Diagnostics:Topology Discovery` dialog.

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

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

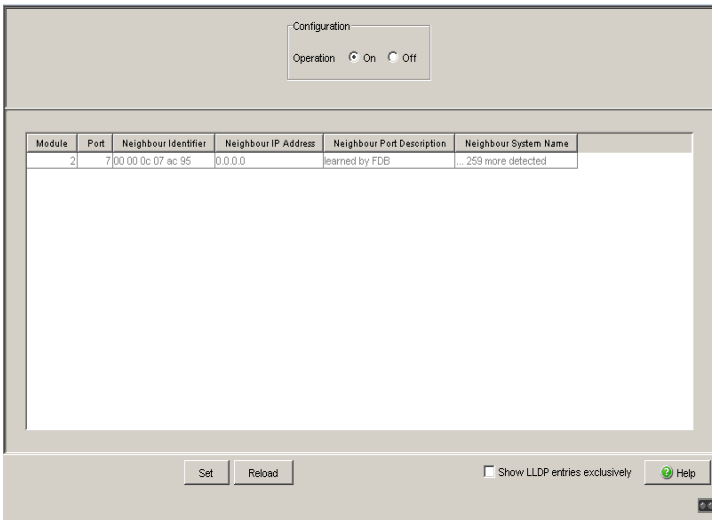


Figure 50: Topology discovery

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

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

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

If
- only devices without active topology discovery are connected to a port, the table will contain one line for this port to represent all devices. This line contains the number of connected devices.
MAC addresses of devices that the topology table hides for the sake of clarity, are located in the address table (FDB) . (see page 104 „Entering static address entries“).

9.8 Detecting IP address conflicts

9.8.1 Description of IP address conflicts

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

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

Table 21: Possible address conflict operation modes

9.8.2 Configuring ACD

☐ Select the Diagnostics:IP Address Conflict Detection dialog.
☐ With "Status" you enable/disable the IP address conflict detection or select the operating mode (see table 21).

9.8.3 Displaying ACD

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

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

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

☐ You can delete this table by restarting the device.

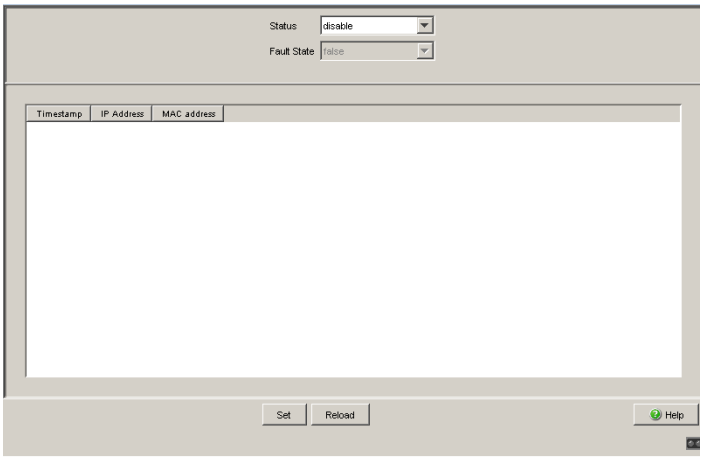


Figure 51: IP Address Conflict Detection dialog

9.9 Reports

The following reports are available for the diagnostics:

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

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

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

☐ Select the `Diagnostics:Report` dialog.

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

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

9.10 Monitoring port traffic (port mirroring)

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

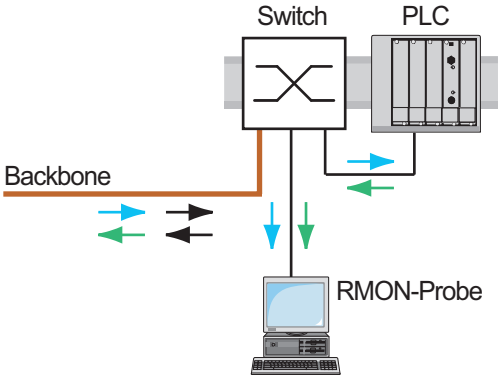


Figure 52: Port mirroring

☐ Select the `Diagnostics:Port Mirroring` dialog.

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

☐ Select the source port whose data traffic you want to observe.

☐ Select the destination port to which you have connected your management tool.

☐ Select "enabled" to switch on the function.

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

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

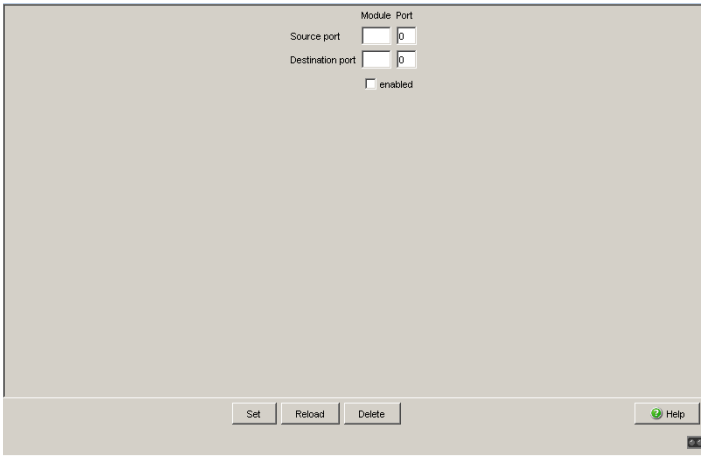


Figure 53: Port Mirroring dialog

A Setting up configuration environment

A.1 Setting up DHCP/BOOTP server

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

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

☐ Start the `DHCP Server` program.

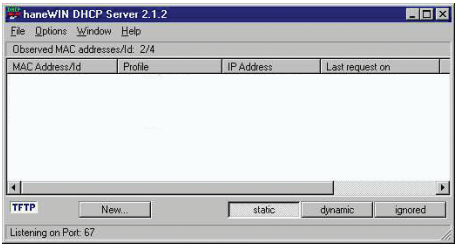


Figure 54: Start window of the DHCP server

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

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

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

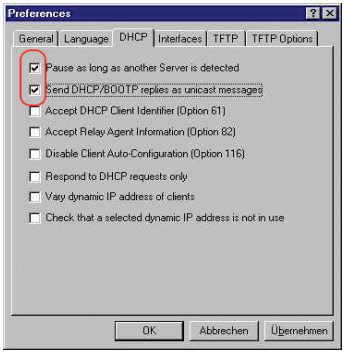


Figure 55: DHCP setting

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

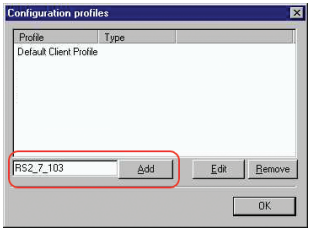


Figure 56: Adding configuration profiles

☐ Enter the network mask and click `Accept`.

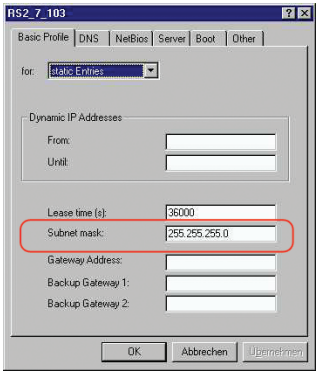


Figure 57: Network mask in the configuration profile

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

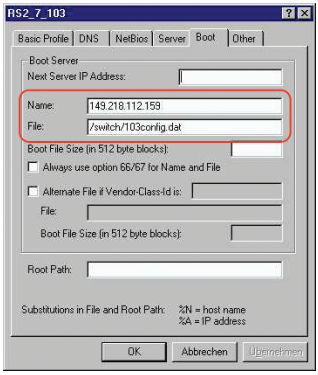


Figure 58: Configuration file on the tftp server

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

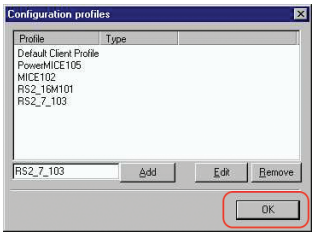


Figure 59: Managing configuration profiles

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

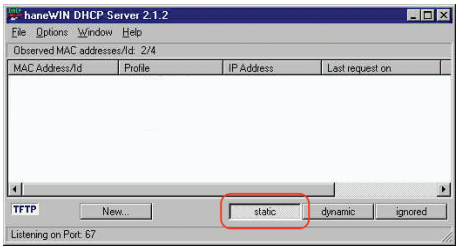


Figure 60: Static address input

☐ Click `New`.

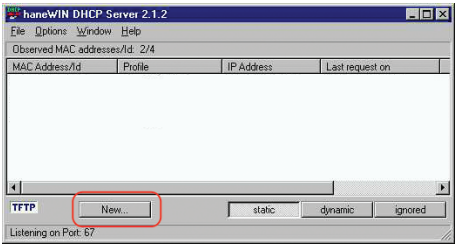


Figure 61: Adding static addresses

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

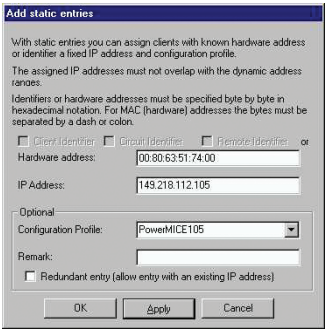


Figure 62: Entries for static addresses

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

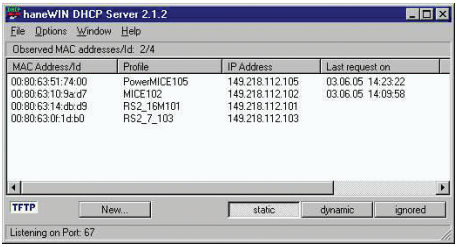


Figure 63: DHCP server with entries

A.2 Setting up DHCP Server Option 82

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

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

☐ Start the `DHCP Server` program.

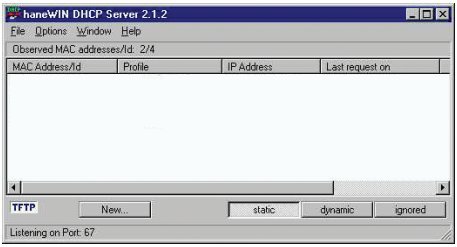


Figure 64: Start window of the DHCP server

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

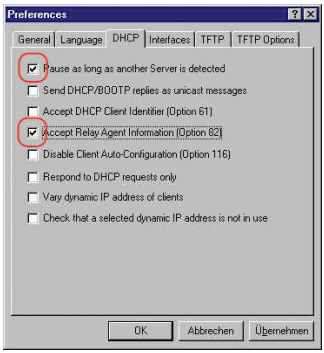


Figure 65: DHCP setting

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

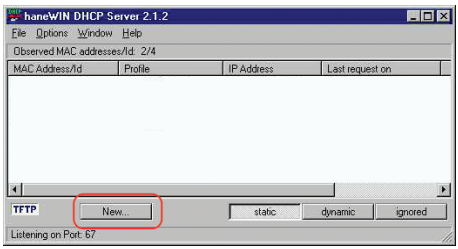


Figure 66: Adding static addresses

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

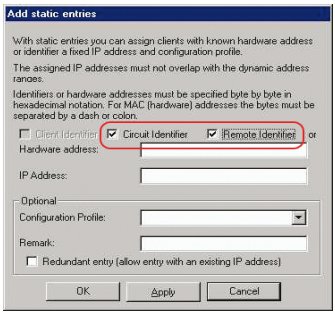


Figure 67: Default setting for the fixed address assignment

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

The hardware address is in the following form:

ciclhhvvvvssmmpprirlxxxxxxxxxxxx

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

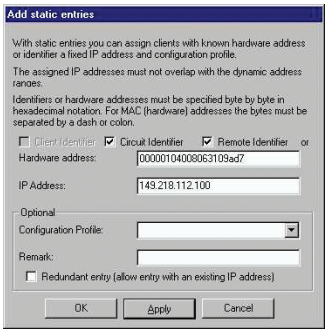


Figure 68: Entering the addresses

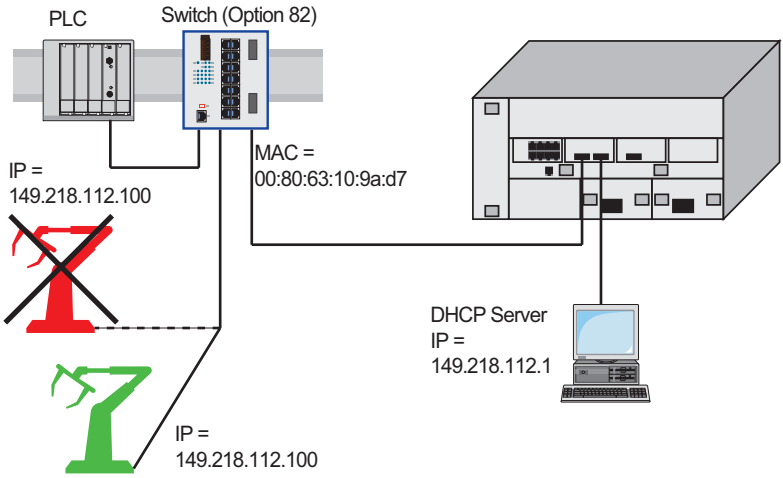


Figure 69: Application example of using Option 82

A.3 tftp server for software updates

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

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

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

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

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

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

A.3.1 Setting up the tftp process

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

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

SunOS and HP

☐ First check whether the tftp daemon (background process) is running, i.e. whether the file /etc/inetd.conf contains the following line (see fig. 70) and whether the status of this process is "IW":

SunOS

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

HP

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

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

SunOS

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

HP

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

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

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

Special steps for HP workstations:

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

For example:

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

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

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

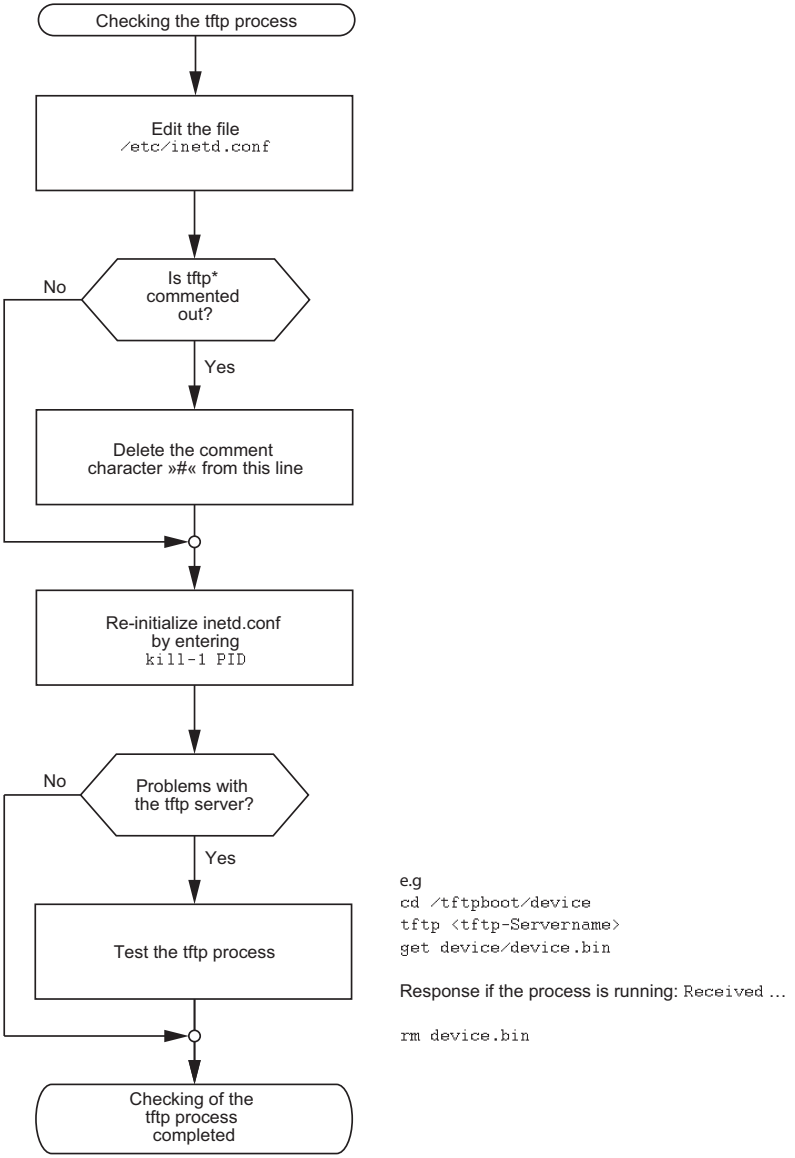


Figure 70: Flow chart for setting up tftp server with SunOS and HP

A.3.2 Software access rights

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

Example of a UNIX tftp server

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

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

Table 22: Directory structure of the software

l = link; d = directory; r = read; w = write; x = execute
1st position denotes the file type (- = normal file),
2nd to 4th positions designate user access rights,
5th to 7th positions designate access rights for users from other groups,
8th to 10th positions designate access rights of all other users.

B General information

B.1 Management Information Base (MIB)

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

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

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

Definition of the syntax terms used:	
Integer	An integer in the range -2^{31} - 2^{31}-1
IP Address	xxx.xxx.xxx.xxx (xxx = integer in the range 0-255)
MAC Address	12-digit hexadecimal number in accordance with ISO/IEC 8802-3
Object identifier	x.x.x.x… (e.g. 1.3.6.1.1.4.1.248…)
Octet string	ASCII character string
PSID	Power supply identifier (number of the power supply unit)
TimeTicks	Stopwatch, Elapsed time (in seconds) = numerical value / 100 Numerical value = integer in range 0-2^{32}-1
Timeout	Time value in hundredths of a second Time value = integer in range 0-2^{32}-1
Type field	4-digit hexadecimal number in accordance with ISO/IEC 8802-3
Counter	Integer (0-2^{32-1}), whose value is increased by 1 when certain events occur.

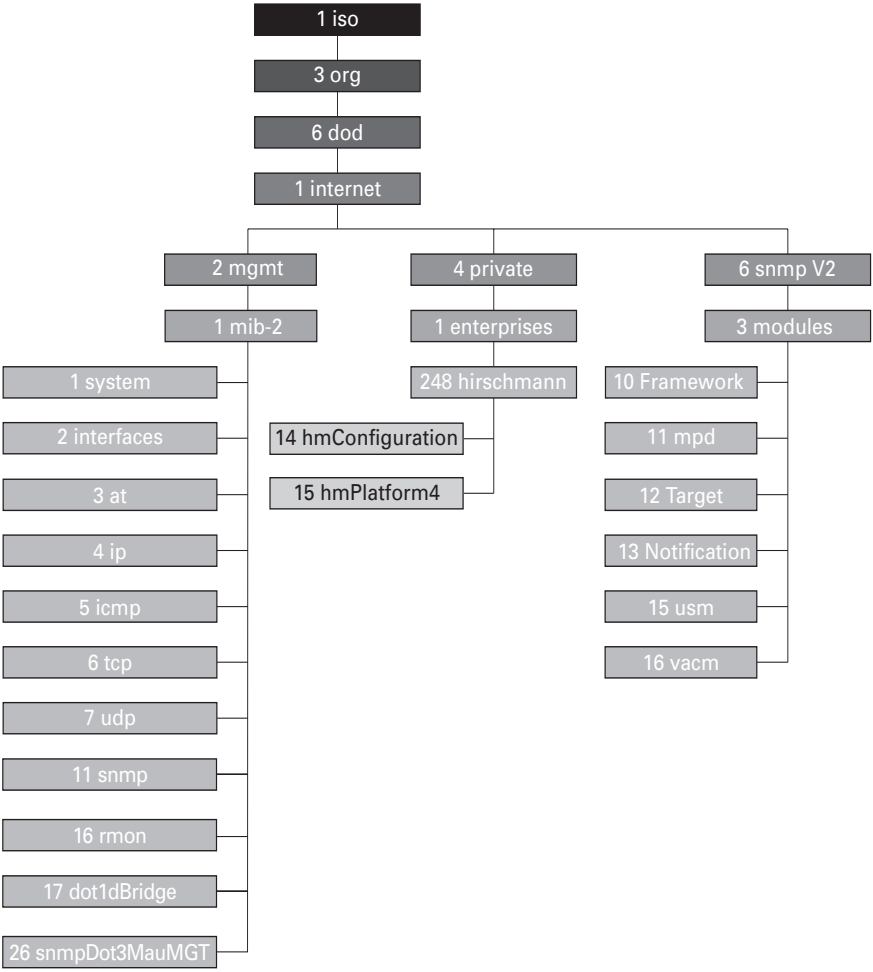


Figure 71: Tree structure of the Pilz MIB

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

B.2 Abbreviations used

SCA	AutoConfiguration Adapter
ACL	Access Control List
BOOTP	Bootstrap Protocol
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
FDB	Forwarding Database
GARP	General Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocoll
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocol
F/O	Optical Fiber
MAC	Media Access Control
NTP	Network Time Protocol
PC	Personal Computer
PTP	Precision Time Protocol
QoS	Quality of Service
RFC	Request For Comment
RM	Redundancy Manager
RS	Rail Switch
RSTP	Rapid Spanning Tree Protocol
SFP	Small Form-factor Pluggable
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
TCP	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
Reference-Handbook Web-based Interface

C Index

T

U

V

W

22753 – EN- 01, 2010-03 Printed in Germany

60
1948–2008
AUTOMATION

...
In many countries we are represented by our subsidiaries and sales partners.

Please refer to our homepage for further details or contact our headquarters.

www
www.pilz.com

Technical support
+49 711 3409-444

PROFIBUS
PROFINET

DAT - I - 010/05

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern, Germany
Telephone: +49 711 3409-0
Telefax: +49 711 3409-133
E-Mail: pilz.gmbh@pilz.de

pilz