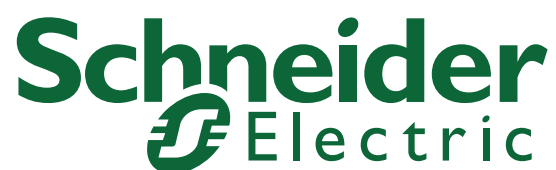


ConneXium

TCSESB Basic Managed Switch Basic Configuration User Manual

S1A78213.01

www.schneider-electric.com



Contents

	Safety Information	7
	About this Manual	9
	Key	13
	Introduction	15
1	Access to the user interfaces	17
1.1	System Monitor	18
1.2	Command Line Interface	20
1.3	Web-based Interface	22
2	Entering the IP Parameters	27
2.1	IP Parameter Basics	29
2.1.1	IP address (version 4)	29
2.1.2	Netmask	30
2.1.3	Classless Inter-Domain Routing	33
2.2	Entering IP parameters via CLI	35
2.3	Entering the IP Parameters via Ethernet Switch Configurator Software	38
2.4	Loading the system configuration from the EAM	41
2.5	System configuration via BOOTP	43
2.6	System Configuration via DHCP	48
2.7	System Configuration via DHCP Option 82	51
2.8	Web-based IP Configuration	53
2.9	Faulty Device Replacement	55
3	Loading/saving settings	57
3.1	Loading settings	58
3.1.1	Loading from the local non-volatile memory	59
3.1.2	Loading from the Memory Backup Adapter	59
3.1.3	Loading from a file	60

3.1.4	Resetting the configuration to the state on delivery	62
3.2	Saving settings	63
3.2.1	Saving locally (and on the EAM)	63
3.2.2	Saving to a file on URL	64
4	Loading Software Updates	67
4.1	Loading the software from the tftp server	68
4.2	Loading the Software via File Selection	70
5	Configuring the Ports	71
6	Protection from Unauthorized Access	73
6.1	Dealing with Unauthorized Access	74
6.2	Password for SNMP access	75
6.2.1	Description of password for SNMP access	75
6.2.2	Entering the password for SNMP access	76
6.3	Web Access	79
6.3.1	Description of Web Access	79
6.3.2	Enabling/disabling Web Access	79
6.4	Ethernet Switch Configurator Software Access	80
6.4.1	Description of the Ethernet Switch Configurator Software Protocol	80
6.4.2	Enabling/disabling the Ethernet Switch Configurator Software Function	80
7	Synchronizing the System Time in the Network	83
7.1	Entering the Time	84
7.2	SNTP	86
7.2.1	Description of SNTP	86
7.2.2	Preparing the SNTP Configuration	87
7.2.3	Configuring SNTP	88
7.3	Precision Time Protocol	91
7.3.1	Description of PTP Functions	91
8	Network Load Control	95
8.1	Direct Packet Distribution	96
8.1.1	Store-and-forward	96
8.1.2	Multi-Address Capability	96
8.1.3	Aging of Learned Addresses	97

8.1.4	Entering Static Addresses	98
8.1.5	Disabling the Direct Packet Distribution	99
8.2	Multicast Application	100
8.2.1	Description of the Multicast Application	100
8.2.2	Example of a Multicast Application	101
8.2.3	Description of IGMP Snooping	102
8.2.4	Setting up the Multicast application	103
8.3	QoS/Priority	110
8.3.1	Description of Prioritization	110
8.3.2	VLAN tagging	111
8.3.3	IP ToS / DiffServ	113
8.3.4	Handling of Received Priority Information	115
8.3.5	Handling of Traffic Classes	116
8.3.6	Setting prioritization	117
9	Operation Diagnosis	121
9.1	Sending Traps	122
9.1.1	List of SNMP Traps	123
9.1.2	SNMP Traps during Boot	123
9.1.3	Configuring Traps	124
9.2	Monitoring the Device Status	126
9.2.1	Configuring the Device Status	127
9.2.2	Displaying the Device Status	128
9.3	Out-of-band Signaling	129
9.3.1	Controlling the Signal Contact	130
9.3.2	Monitoring the Device Status via the Signal Contact	130
9.3.3	Monitoring the Device Functions via the Signal Contact	131
9.4	Port Status Indication	133
9.5	Event Counter at Port Level	135
9.6	Topology Discovery	137
9.6.1	Description of Topology Discovery	137
9.6.2	Displaying the Topology Discovery Results	139
9.7	Detecting IP Address Conflicts	142
9.7.1	Description of IP Address Conflicts	142
9.7.2	Configuring ACD	143
9.7.3	Displaying ACD	144
9.8	Reports	145
9.9	Monitoring Data Traffic at Ports (Port Mirroring)	146

A	Setting up the Configuration Environment	149
A.1	TFTP Server for Software Updates	150
A.1.1	Setting up the tftp Process	151
A.1.2	Software Access Rights	154
B	General Information	155
B.1	Abbreviations used	156
B.2	Technical Data	157
C	Index	159

Safety Information

■ Important Information

Notice: Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.



The addition of this symbol to a Danger or Warning safety label indicates that an electrical hazard exists, which will result in personal injury if the instructions are not followed.



This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

DANGER

DANGER indicates an imminently hazardous situation which, if not avoided, **will result in** death or serious injury.

WARNING

WARNING indicates a potentially hazardous situation which, if not avoided, **can result in** death or serious injury.

CAUTION

CAUTION indicates a potentially hazardous situation which, if not avoided, **can result in** minor or moderate injury.

PLEASE NOTE: Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

© 2011 Schneider Electric. All Rights Reserved.

About this Manual

Validity Note

The data and illustrations found in this book are not binding. We reserve the right to modify our products in line with our policy of continuous product development. The information in this document is subject to change without notice and should not be construed as a commitment by Schneider Electric.

Product Related Information

Schneider Electric assumes no responsibility for any errors that may appear in this document. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

No part of this document may be reproduced in any form or by any means, electronic or mechanical, including photocopying, without express written permission of Schneider Electric.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to ensure compliance with documented system data, only the manufacturer should perform repairs to components.

When devices are used for applications with technical safety requirements, please follow the relevant instructions.

Failure to use Schneider Electric software or approved software with our hardware products may result in improper operating results.

Failure to observe this product related warning can result in injury or equipment damage.

User Comments

We welcome your comments about this document. You can reach us by e-mail at techpub@schneider-electric.com

Related Documents

Title of Documentation	Reference-Number
ConneXium TCSESB Basic Managed Switch Redundancy Configuration User Manual	S1A78418
ConneXium TCSESB Managed Switch Basic Configuration User Manual	S1A78213
ConneXium TCSESB Basic Managed Switch Command Line Interface Reference Manual	S1A78426
ConneXium TCSESB Basic Managed Switch Web-based Interface Reference Manual	S1A78429
ConneXium TCSESB Basic Managed Switch Installation Manual	S1A78204

Note: The Glossary is located in the Reference Manual “Command Line Interface”.

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

The following thematic sequence has proven itself in practice:

- ▶ Set up device access for operation by entering the IP parameters
- ▶ Check the status of the software and update it if necessary
- ▶ If a configuration already exists, load/store it
- ▶ 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
- ▶ Store the newly created configuration to nonvolatile memory

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





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

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.

Key

The designations used in this manual have the following meanings:

	List
<input type="checkbox"/>	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.
<i>Courier</i>	ASCII representation in user interface
	Execution in the Web-based Interface user interface
	Execution in the Command Line Interface user interface

Symbols used:

	WLAN access point
	Router with firewall
	Switch with firewall
	Router
	Switch

Key



Bridge



Hub



A random computer



Configuration Computer



Server



PLC -
Programmable logic
controller



I/O -
Robot

Introduction

The device has been developed for 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.

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

1 Access to the user interfaces

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

- ▶ System monitor via the V.24 interface (out-of-band)
- ▶ Command Line Interface (CLI) via the V.24 connection (out-of-band)
- ▶ 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.

```
< Device Name (Boot) Release: 1.00 Build: 2005-09-17 15:36 >
Press <1> to enter System Monitor 1 ...
1
```

Figure 1: Screen display during the boot process

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

```
System Monitor 1
(Selected OS: L2S-05.2.02-K05 (2010-09-09 16:02))
1  Select Boot Operating System
2  Update Operating System
3  Start Selected Operating System
4  End (reset and reboot)
5  Erase main configuration file
6  Show Bootcode information

sysMon1>
```

Figure 2: System monitor - screen display

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

1.2 Command Line Interface

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

The Command Line Interface provides IT specialists with a familiar environment for configuring IT devices.

The script compatibility of the Command Line Interface enables you, among other things, to feed multiple devices with the same configuration data, to create and apply partial configurations or to compare 2 configuration by comparing the script files.

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

You can access the Command Line Interface via

- ▶ the V.24 port (out-of-band)

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.
A window for entering the user name appears on the screen.

```
Copyright (c) 2004-2010 Schneider Electric

All rights reserved

TCSESB Release L2S-05.2.02-K04

(Build date 2010-08-04 18:14)

System Name: TCSESB083F2CU0
Mgmt-IP      : 10.0.1.221
Base-MAC     : 00:80:63:51:74:00
System Time: 2010-08-11 13:14:15

User:
```

Figure 3: Logging in to the Command Line Interface program

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

The start screen appears.

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

```
(Schneider Electric TCSESB) >
```

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 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 Java software 6 (“Java™ Runtime Environment Version 1.6.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 do not have access to the internet, cancel the installation. Install the software from the enclosed CD-ROM. To do this, browse the directory of this CD under "ConneXium", then open the "Java" folder. Start the installation program.

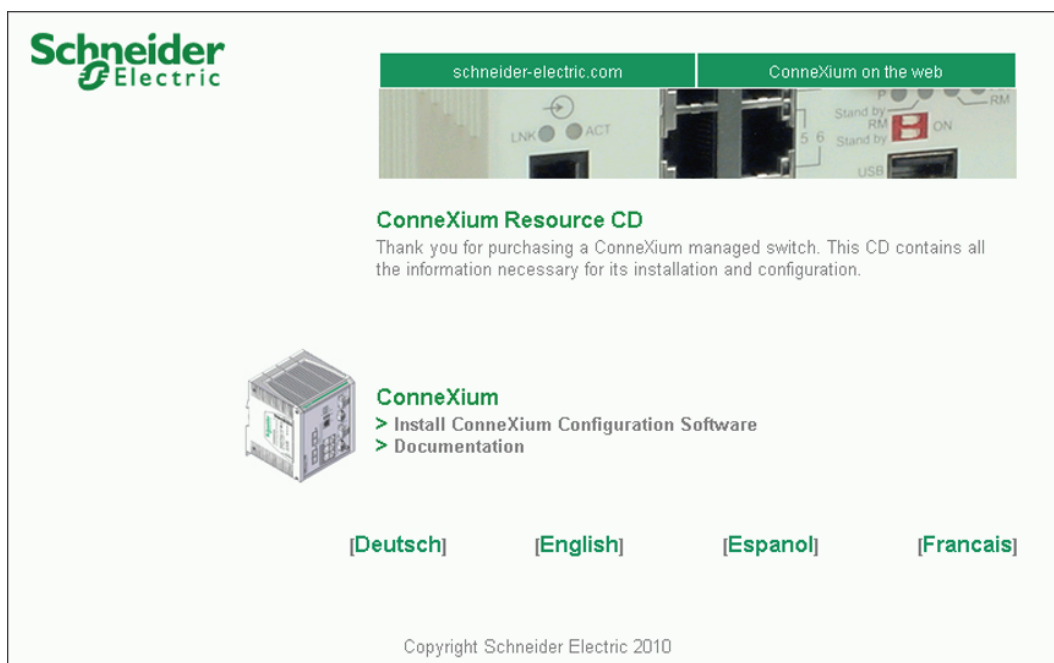


Figure 5: Installing Java

- 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 "Set". Click "Reload" to update the display.

Note: If you enter an incorrect configuration, you may block the access to your device.

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.

Note: The following Memory Backup Adapter is used for the ConneXium Basic managed switches: TCSEAM0200.

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 35 “Entering IP parameters via CLI”).
- ▶ Entry using the Ethernet Switch Configurator Software 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 38 “Entering the IP Parameters via Ethernet Switch Configurator Software”).
- ▶ Configuration using the Memory Backup Adapter (EAM).
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 EAM (see page 59 “Loading from the Memory Backup Adapter”).
- ▶ 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 43 “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 48 “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 51 “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-Saharan Africa
- ▶ LACNIC (Regional Latin-American and Caribbean IP Address Registry) – Latin America and some Caribbean Islands
- ▶ RIPE NCC (Réseaux IP Européens) - Europe and Surrounding Regions

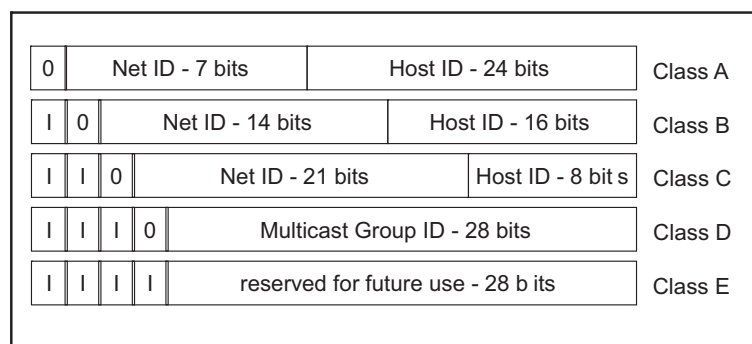


Figure 7: Bit representation of the IP address

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:

Decimal notation

255.255.192.0

Binary notation

11111111.11111111.11000000.00000000



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

Decimal notation

129.218.65.17



Binary notation

1000001.11011010.01000001.00010001



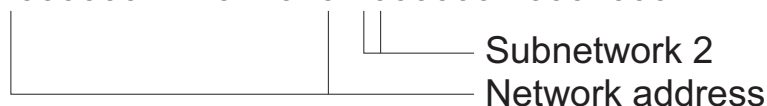
Decimal notation

129.218.129.17



Binary notation

1000001.11011010.10000001.00010001



■ Example of how the network mask is used

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

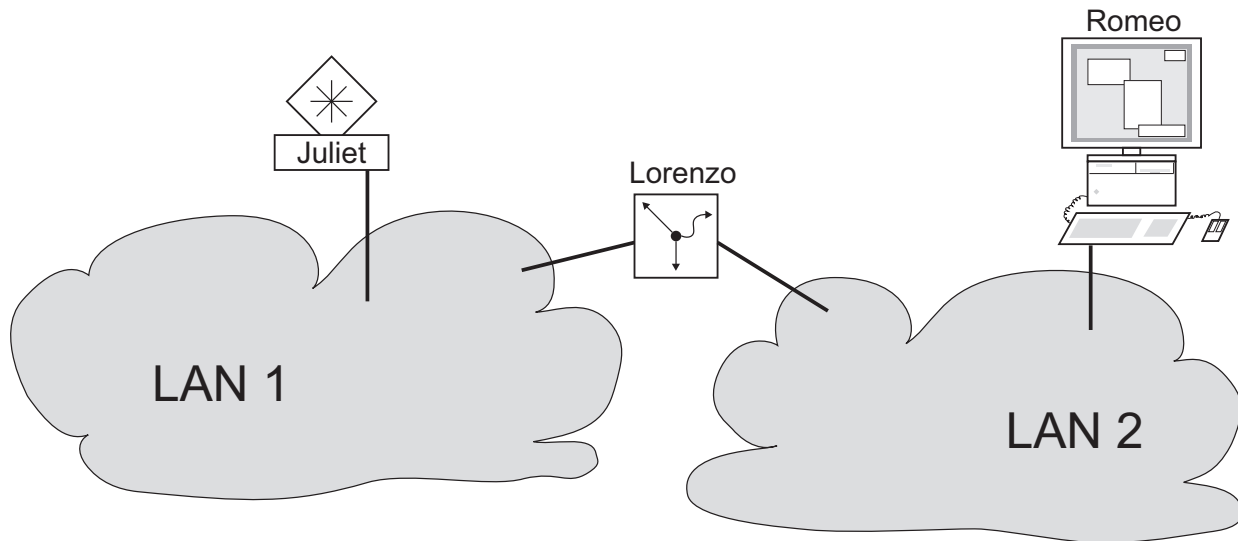


Figure 8: Management agent that is separated from its management station by a router

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

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

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

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

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

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

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

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

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

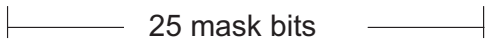

2.1.3 Classless Inter-Domain Routing

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
		
CIDR notation: 149.218.112.0/25		
		

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

2.2 Entering IP parameters via CLI

If you do not configure the system via BOOTP/DHCP, DHCP Option 82, the Ethernet Switch Configurator Software protocol or the Memory Backup Adapter EAM, then you perform the configuration via the V.24 interface using the CLI.

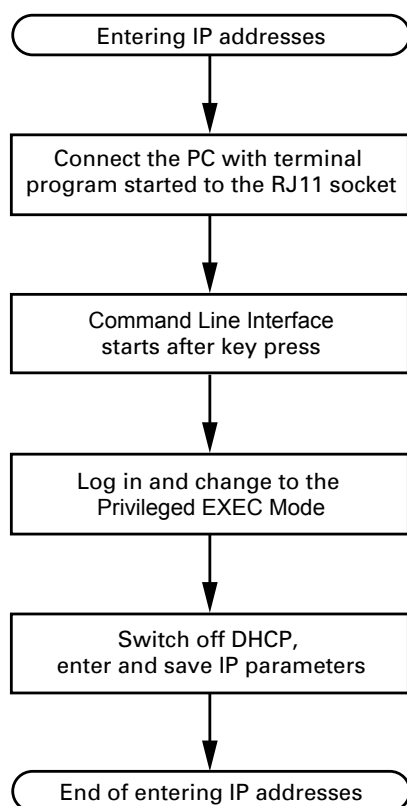


Figure 9: Flow chart for entering IP addresses

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 20 “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' command forms of that particular mode. For a list of valid 'no' command forms for that mode, enter the help command 'no ?'. For the syntax of a particular command form, please consult documentation.

(Schneider Electric TCSESB) >

- 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 32 “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
network protocol none
network parms 10.0.1.23
                255.255.255.0

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

Switch to the Privileged EXEC mode.

Deactivate DHCP.

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

Save the current configuration to the non-volatile memory.

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

2.3 Entering the IP Parameters via Ethernet Switch Configurator Software

The Ethernet Switch Configurator Software 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 Ethernet Switch Configurator Software on your PC. The software is on the CD supplied with the device.

- To install it, you start the installation program on the CD.
- Start the Ethernet Switch Configurator Software program.

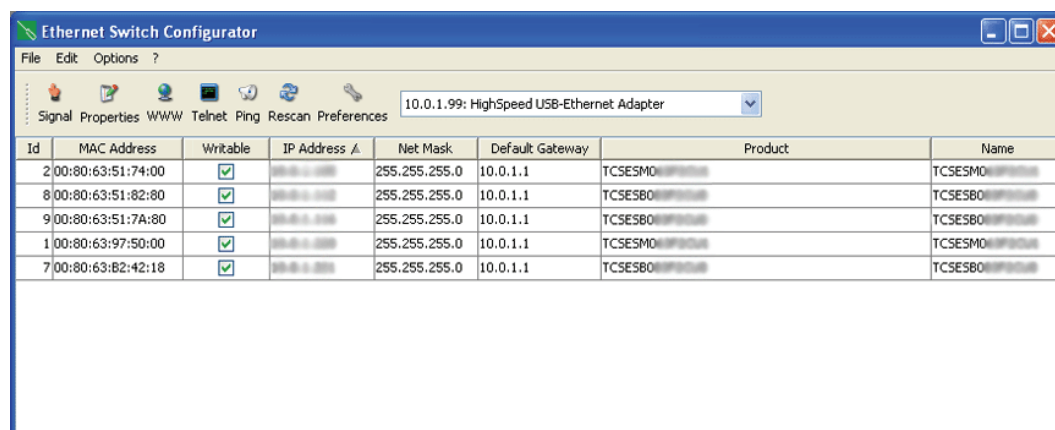


Figure 10: Ethernet Switch Configurator Software

When Ethernet Switch Configurator Software is started, it automatically searches the network for those devices which support the Ethernet Switch Configurator Software protocol.

Ethernet Switch Configurator Software uses the first PC network card found. If your computer has several network cards, you can select these in Ethernet Switch Configurator Software on the toolbar.

Ethernet Switch Configurator Software displays a line for every device which reacts to the Ethernet Switch Configurator Software protocol.

Ethernet Switch Configurator Software enables you to identify the devices displayed.

- Select a device line.
- Click on the signal symbol in the tool bar to set the LEDs for the selected device flashing. To switch off the flashing, click on the symbol again.
- By double-clicking a line, you open a window in which you can enter the device name and the IP parameters.

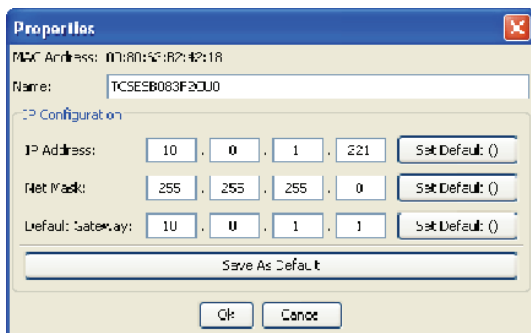


Figure 11: Ethernet Switch Configurator Software - assigning IP parameters

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

Note: For security reasons, switch off the Ethernet Switch Configurator Software function for the device in the Web-based interface, after you have assigned the IP parameters to the device (see on page 53 “Web-based IP Configuration”).

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

2.4 Loading the system configuration from the EAM

The Memory Backup Adapter (EAM) is a device for

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

In the case of a device becoming inoperative, the EAM 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 EAM. If it finds an EAM with a valid password and valid software, the device loads the configuration data from the EAM.

The password is valid if

- ▶ the password in the device matches the password in the EAM or
- ▶ the preset password is entered in the device.

To save the configuration data on the EAM, see [“Saving locally \(and on the EAM\)”](#) on [page 63](#).

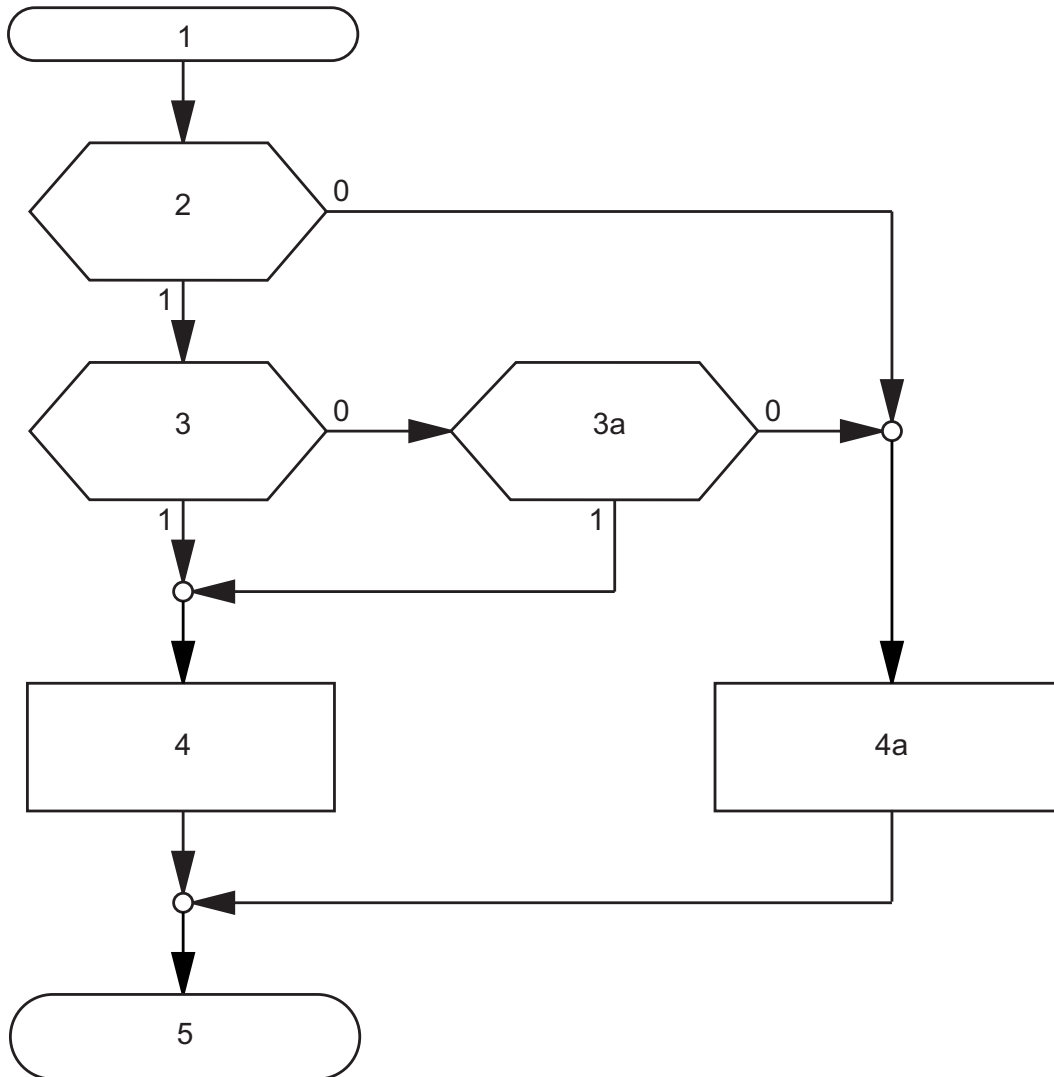


Figure 12: Flow chart of loading configuration data from the EAM

- 1 – Device start-up
- 2 – EAM plugged-in?
- 3 – Password in device and EAM identical?
- 3a – Default password in device?
- 4 – Load configuration from EAM, EAM LEDs flashing synchronously
- 4a – Load configuration from local memory, EAM LEDs flashing alternately
- 5 – Configuration data loaded

2.5 System configuration via BOOTP

When it is started up via BOOTP (bootstrap protocol), a device receives its configuration data in accordance with the “BOOTP process” flow chart (see 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 53 “Web-based IP Configuration”), or see the CLI:

Note: When you change the protocol for setting the IP address (`none`, `dhcp` or `bootp`), the device activates the new mode immediately after the command is entered.

<code>enable</code>	Switch to the Privileged EXEC mode.
<code>network protocol bootp</code>	Activate BOOTP.
<code>copy system:running-config nvram:startup-config</code>	Activate BOOTP.
<code>y</code>	Confirm save.

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

```
# /etc/bootptab for BOOTP-daemon bootpd
#
# gw -- gateway
# ha -- hardware address
# ht -- hardware type
# ip -- IP address
```

```
# sm -- subnet mask
# tc -- template

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

switch_01:ht=ethernet:ha=008063086501:ip=10.1.112.83:tc=.global:
switch_02:ht=ethernet:ha=008063086502:ip=10.1.112.84:tc=.global:
.
.
```

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

The lines under ".global:" make the configuration of several devices easier. With the template (tc) you allocate the global configuration data (tc=.global:) to each device.

The direct allocation of hardware address and IP address is performed in the device lines (switch-0...).

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

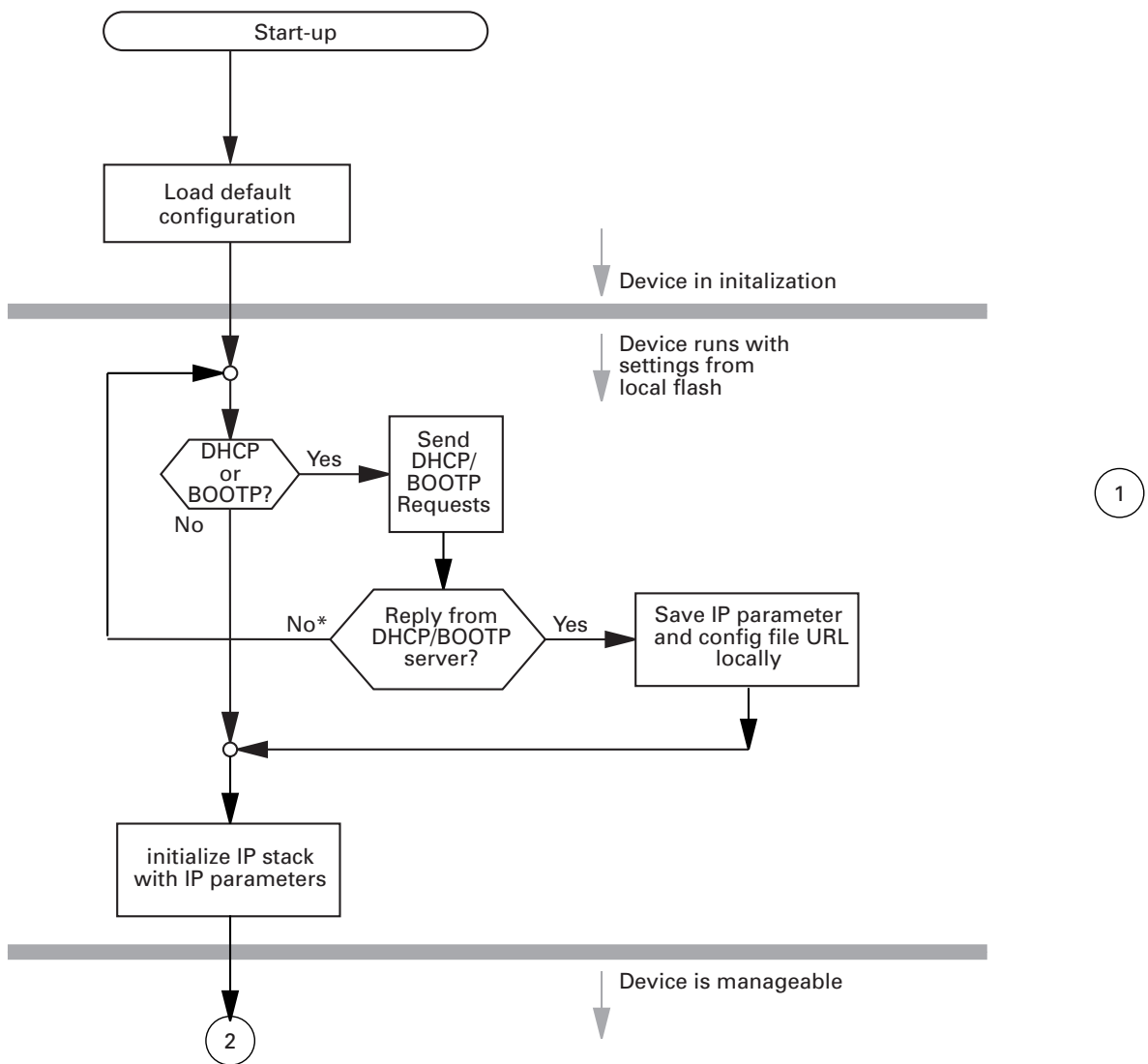


Figure 13: Flow chart for the BOOTP/DHCP process, part 1
 * see fig. 14

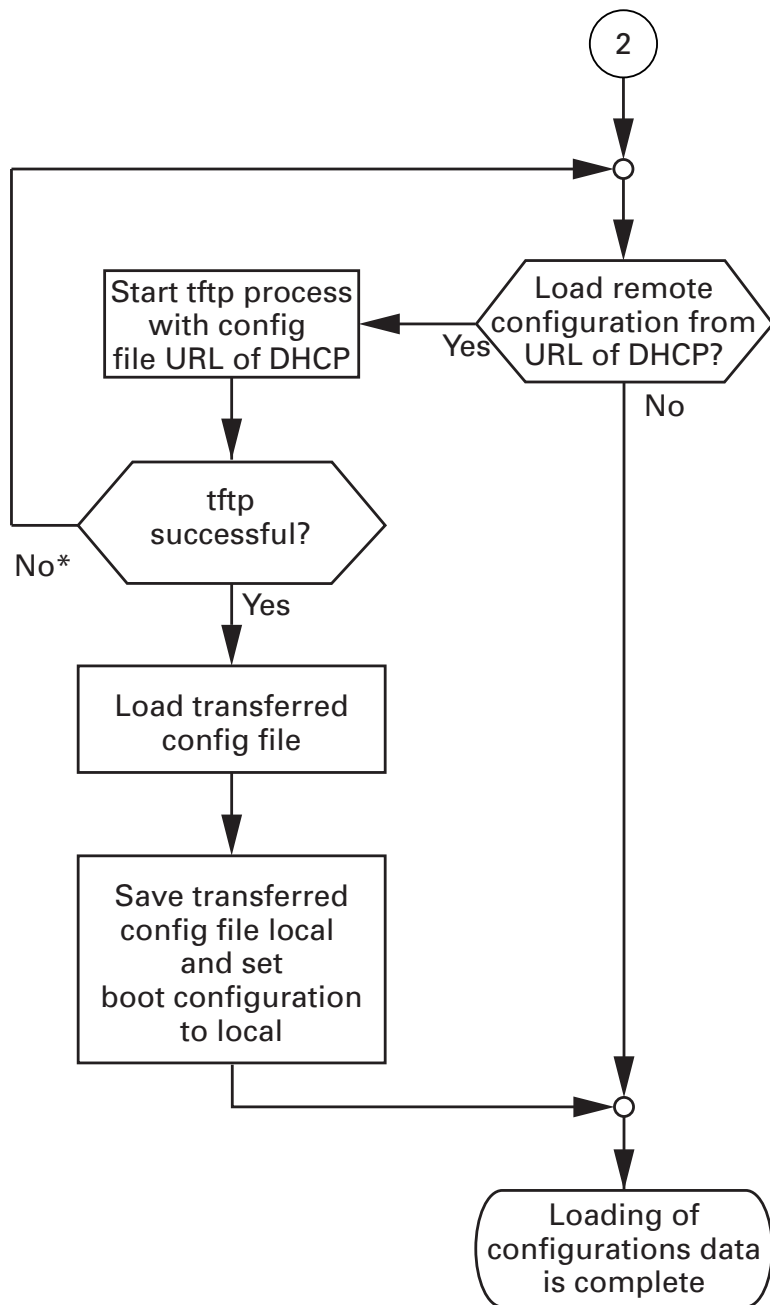


Figure 14: Flow chart for the BOOTP/DHCP process, part 2

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

2.6 System Configuration via DHCP

The DHCP (Dynamic Host Configuration Protocol) is a further development of BOOTP, which it has replaced. The DHCP additionally allows the configuration of a DHCP client via a name instead of via the MAC address. For the DHCP, this name is known as the “client identifier” in accordance with rfc 2131.

The device uses the name entered under sysName in the system group of the MIB II as the client identifier. You can enter this system name directly via SNMP, the Web-based management (see system dialog), or the Command Line Interface.

During startup operation, a device receives its configuration data according to the “DHCP process” flowchart ([see 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 netmask
- the default gateway (if available)
- the tftp URL of the configuration file (if available).

The device accepts this data as configuration parameters ([see on page 53 “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
17	Root Path
42	NTP server
61	Client Identifier
66	TFTP Server Name
67	Bootfile Name

Table 3: DHCP options which the device requests

The advantage of using DHCP instead of BOOTP is that the DHCP server can restrict the validity of the configuration parameters (“Lease”) to a specific time period (known as dynamic address allocation). Before this period (“Lease Duration”) elapses, the DHCP client can attempt to renew this lease. Alternatively, the client can negotiate a new lease. The DHCP server then allocates a random free address.

To avoid this, most DHCP servers provide the explicit configuration option of always assigning a specific client the same IP address based on a unique hardware ID (known as static address allocation).

On delivery, DHCP is activated.

As long as DHCP is activated, the device attempts to obtain an IP address. If it cannot find a DHCP server after restarting, it will not have an IP address.

To activate/deactivate DHCP ([see on page 53 “Web-based IP Configuration”](#)).

Example of a DHCP configuration file:

```
# /etc/dhcpd.conf for DHCP Daemon
#
subnet 10.1.112.0 netmask 255.255.240.0 {
option subnet-mask 255.255.240.0;
option routers 10.1.112.96;
}
#
# Host berta requests IP configuration
# with her MAC address
```

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

Lines that 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

On the device's front panel you will find the following safety note.



WARNING

UNINTENDED OPERATION

Do not change cable positions if DHCP Option 82 is enabled. Check the Basic Configuration user manual before servicing (refer to DHCP OPTION 82 topic).

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

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 classic DHCP protocol on the device being configured ([see on page 48 “System Configuration via DHCP”](#)), Option 82 is based on the network topology. This procedure gives you the option of always assigning the same IP address to any device which is connected to a particular location (port of a device) on the LAN.

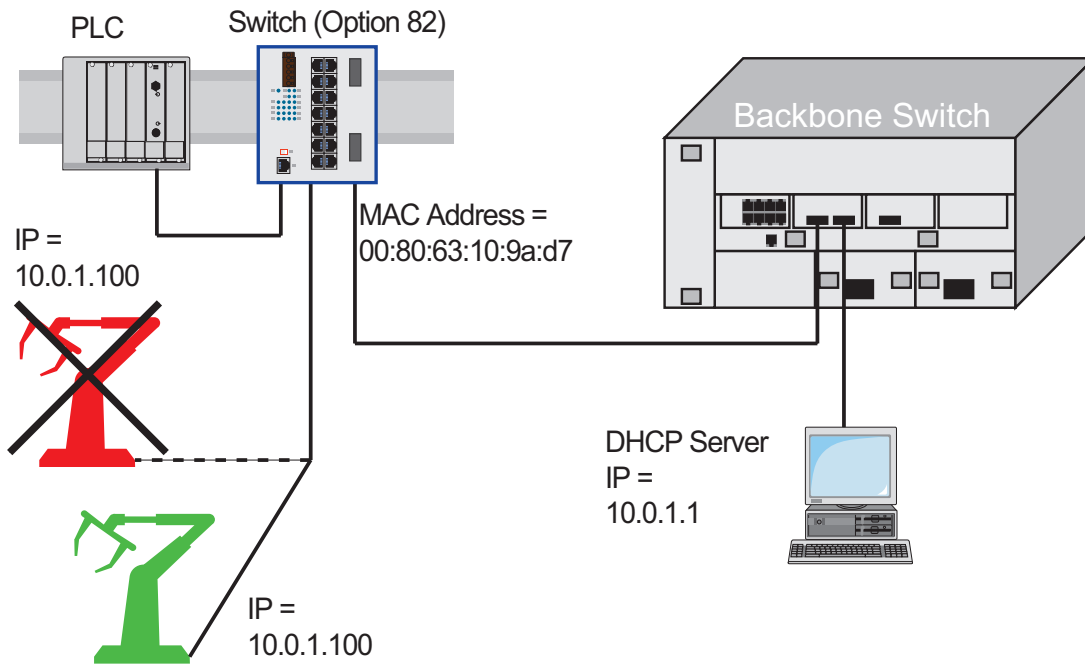


Figure 15: Application example of using Option 82

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 configure the Ethernet Switch Configurator Protocol access.

The screenshot shows a web-based configuration interface for network parameters. On the left, under the heading "Mode", there are three radio buttons: "BOOTP", "DHCP", and "Local". The "Local" radio button is selected. To the right, there are several input fields and sections. The "BOOTP / DHCP" section has a "MAC Address" field containing "00:80:63:B2:42:18". The "DHCP" section has a "System Name" field containing "TCSES8083F2CU0". The "Local" section has three fields: "IP Address" (10.0.1.221), "Netmask" (255.255.255.0), and "Gateway address" (10.0.1.1). Below these is the "Ethernet Switch Configurator Protocol" section, which includes an "Operation" field with "On" selected and "Off" as an option, and an "Access" dropdown menu set to "read-write". At the bottom of the dialog, there are "Set", "Reload", and "Help" buttons.

Figure 16: Network parameters dialog

- Under “Mode”, you enter where the device gets its IP parameters:
 - ▶ In the BOOTP mode, the configuration is via a BOOTP or DHCP server on the basis of the MAC address of the device.
 - ▶ In the DHCP mode, the configuration is via a DHCP server on the basis of the MAC address or the name of the device.
 - ▶ In the “local” mode the net parameters in the device memory are used.

Note: When you change the network mode from "Local" to "BOOTP" or "DHCP", the server will assign a new IP address to the device. If the server does not respond, the IP address will be set to 0.0.0.0, and the BOOTP/DHCP process will try to obtain an IP address again.

- 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 Ethernet Switch Configurator Software protocol allows you to allocate an IP address to the device on the basis of its MAC address. Activate the Ethernet Switch Configurator Software protocol if you want to allocate an IP address to the device from your PC with the enclosed Ethernet Switch Configurator Software (state on delivery: operation "on", access "read-write").

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

2.9 Faulty Device Replacement

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

- ▶ Configuring the new device using an Memory Backup Adapter ([see on page 59 “Loading from the Memory Backup Adapter”](#)) or
- ▶ configuration via DHCP Option 82.

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

3 Loading/saving settings

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

The device enables you to

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

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

3.1 Loading settings

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

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

- ▶ the local non-volatile memory
- ▶ from the Memory Backup Adapter. If an EAM is connected to the device, the device automatically loads its configuration from the EAM during the boot procedure.
- ▶ a file in the connected network (setting on delivery)
- ▶ a binary file and
- ▶ the firmware (restoration of the configuration on delivery).

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

Note: Loading a configuration deactivates the ports while the configuration is being set up. Afterwards, the Switch sets the port status according to the new configuration.

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 EAM is connected to the device.

- Select the `Basics: Load/Save` dialog.
- In the "Load" frame, click "from Device".
- Click "Restore".

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

Switch to the Privileged EXEC mode.

The device loads the configuration data from the local non-volatile memory.

3.1.2 Loading from the Memory Backup Adapter

If a EAM is connected to the device, the device automatically loads its configuration from the EAM during the boot procedure.

The chapter [“Saving locally \(and on the EAM\)”](#) on [page 63](#) describes how to save a configuration file on an EAM.

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 Memory Backup 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 "Restore".

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

Example of loading from a tftp server

- Before downloading a file from the tftp server, you have to save the configuration file in the corresponding path of the tftp servers with the file name, e.g. `switch/switch_01.cfg` (see on page 64 "Saving to a file on URL")
- In the "URL" line, enter the path of the tftp server, e.g. `tftp://10.1.112.214/switch/switch_01.cfg`.

Figure 17: Load/Save dialog

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

Switch to the Privileged EXEC mode.
The device loads the configuration data from a tftp server in the connected network.

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

3.1.4 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 * .c f g.
- 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 EAM)

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

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

```
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 EAM is connected, also on the EAM

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

3.2.2 Saving to 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.

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

- Click "Save".


```
enable
copy nvram:startup-config
  tftp://10.1.112.159/
  switch/config.dat
copy nvram:script
  tftp://10.0.1.159/switch/
  config.txt
```

Switch to the Privileged EXEC mode.

The device saves the configuration data in a binary file on a tftp server in the connected network

The device saves the configuration data in a script file on a tftp server in the connected network.

4 Loading Software Updates

■ Checking the installed software release

- 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..... TCSESB083F2CU0_
  ConneXium Ethernet Managed Switch
System Name..... TCSESB083F2CU0
System Location..... Schneider TCSESB
System Contact.....
  www.schneider-electric.com
System Up Time..... 0 days 0 hrs 45 mins
  57 secs
System Date and Time (local time zone)..... 2010-02-03 05:06:07
System IP Address..... 10.0.1.13
Boot Software Release..... L2S-05.0.00
Boot Software Build Date..... 2010-07-15 07:30
OS Software Release..... L2S-05.2.02-K01
OS Software Build Date..... 2010-08-04 18:14
Backplane Hardware Revision..... 1.02 / 17 / 0101
Backplane Hardware Description..... TCSESB083F2CU0
Serial Number..... 942014002000101279
Base MAC Address..... 00:80:63:1F:10:54
Number of MAC Addresses..... 18 (0x12)

```

■ Loading the software

The device gives you 2 options for loading the software:

- ▶ via TFTP from a tftp server (in-band) and
- ▶ via a file selection dialog from your PC.

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

4.1 Loading the software 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 150 “TFTP Server for Software Updates”).

- Select the `Basics:Software` dialog.

The URL identifies the path to the software stored on the tftp server. The URL is in the format

`tftp://IP address of the tftp server/path name/file name`
(e.g. `tftp://192.168.1.1/device/device.bin`).

- Enter the path of the device software.
- Click on "Update" to load the software from the tftp server to the device.

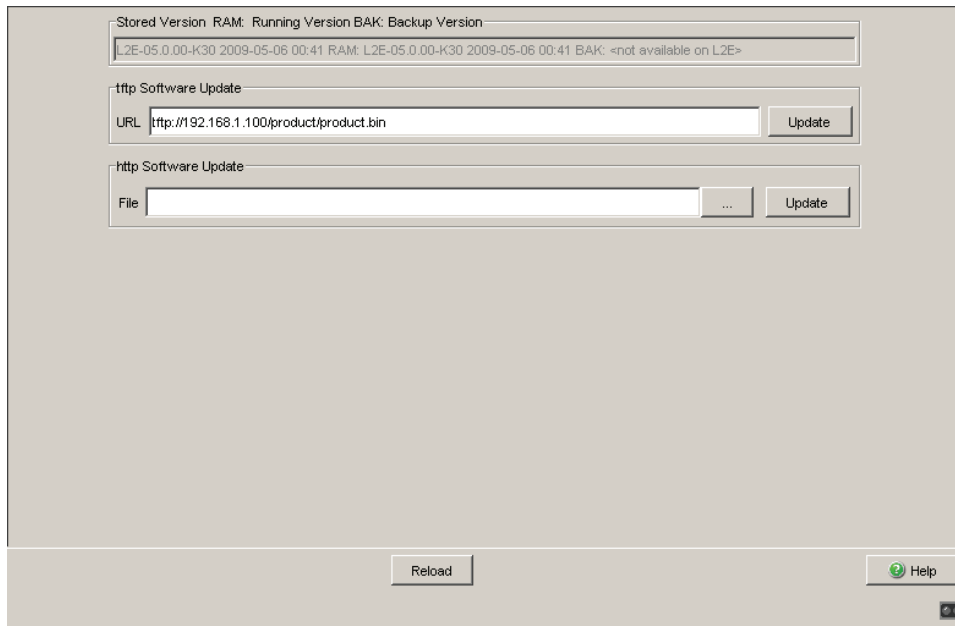


Figure 18: Software update dialog

- After successfully loading it, you activate the new software: Select the dialog `Basic Settings:Restart` and perform a cold start. In a cold start, the device reloads the software from the non-volatile memory, restarts, and performs a self-test.
- After booting the device, click "Reload" in your browser to access the device again.

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

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

4.2 Loading the Software via File Selection

For an HTTP software update (via a file selection window), the device software must be on a data carrier that you can access from your workstation.

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

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

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

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

■ 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 "Propagate connection error" column, select the ports for which you want to have link monitoring.

6 Protection from Unauthorized Access

The device provides you with the following functions to help you protect it against unauthorized access.

- ▶ Password for SNMP access
- ▶ Web access disabling
- ▶ Ethernet Switch Configurator Software function disabling

6.1 Dealing with Unauthorized Access

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

- Deactivate SNMPv1 and SNMPv2 and select a password for SNMPv3 access other than the standard password ([see on page 76 “Entering the password for SNMP access”](#)).
- Deactivate web access ([see on page 79 “Enabling/disabling Web Access”](#)) after you have downloaded the applet for the web-based interface onto your management station. You can start the web-based interface as an independent program and thus have SNMPv3 access to the device.
- Deactivate Ethernet Switch Configurator Software access.

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

6.2 Password for SNMP access

6.2.1 Description of password for SNMP access

A network management station communicates with the device via the Simple Network Management Protocol (SNMP).

Every SNMP packet contains the IP address of the sending computer and the password with which the sender of the packet wants to access the device MIB.

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

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

To help protect your device from unwanted access:

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

6.2.2 Entering the password for SNMP access

- Select the `Security:Password/SNMP Access` dialog.

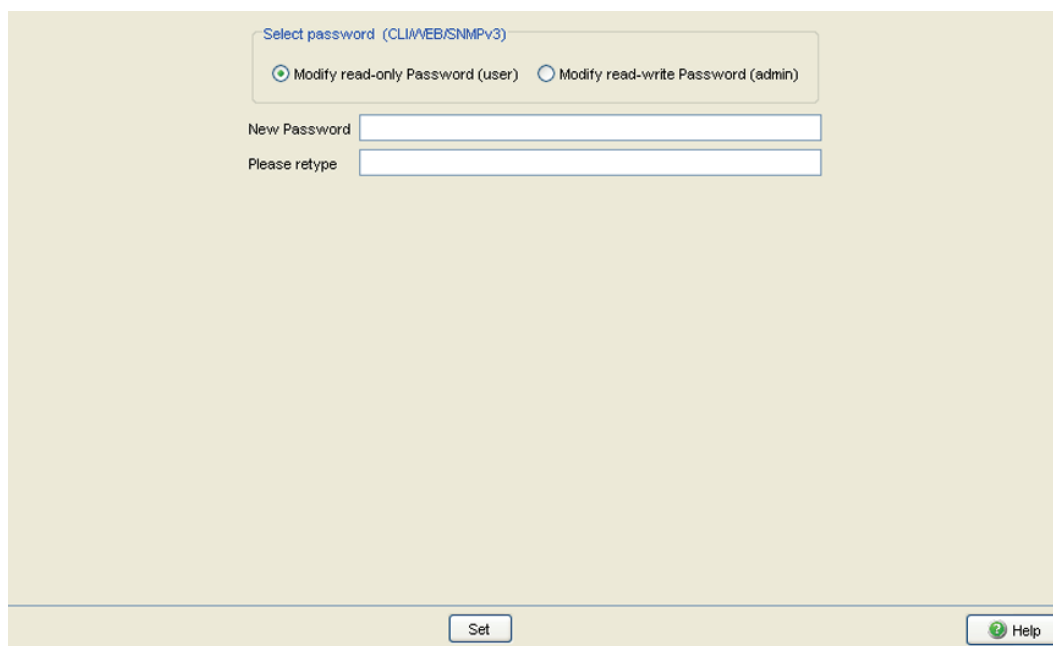
This dialog gives you the option of changing the read and read/write passwords for access to the device via the Web-based interface, via the CLI, and via SNMPv3 (SNMP version 3). Please note that passwords are case-sensitive.

Set different passwords for the read password and the read/write password so that a user that only has read access (user name “user”) does not know, or cannot guess, the password for read/write access (user name “admin”).

If you set identical passwords, when you attempt to write this data the device reports a general error.

The Web-based interface and the user interface (CLI) use the same passwords as SNMPv3 for the users “admin” and “user”.

- 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.



Select password (CLI/WEB/SNMPv3)

Modify read-only Password (user) Modify read-write Password (admin)

New Password

Please retype

Figure 19: Dialog Password/SNMP Access

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

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

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

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

- Select the `Security:SNMPv1/v2 access` dialog. With this dialog you can select the access via SNMPv1 or SNMPv2. In the state on delivery, both protocols are activated. You can thus 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.

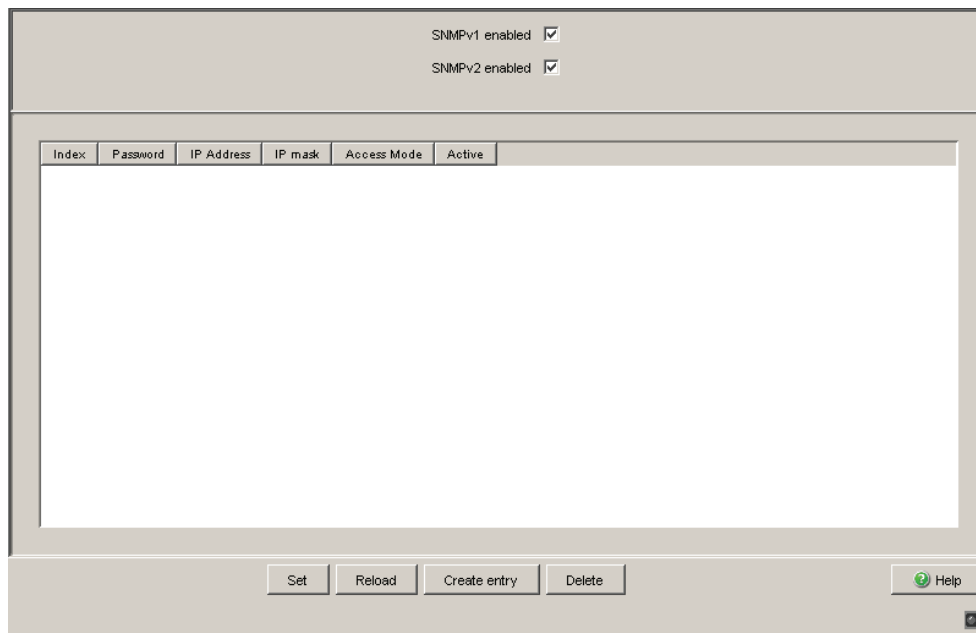


Figure 20: SNMPv1/v2 access dialog

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

6.3 Web Access

6.3.1 Description of Web Access

The Web server of the device allows you to configure the device by using the Web-based interface. Deactivate the Web server if you do not want the device to be accessed from the Web.

On delivery, the server is activated.

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

6.3.2 Enabling/disabling Web Access

- Select the `Security:Web Access` dialog.
- Disable the server to which you want to refuse access.

```
enable
configure
lineconfig
exit
exit
ip http server
no ip http server
```

Switch to the Privileged EXEC mode.
Switch to the Configuration mode.
Switch to the configuration mode for CLI.
Switch to the Configuration mode.
Switch to the privileged EXEC mode.
Enable Web server.
Disable Web server.

6.4 Ethernet Switch Configurator Software Access

6.4.1 Description of the Ethernet Switch Configurator Software Protocol

The Ethernet Switch Configurator Software protocol allows you to allocate an IP address to the device on the basis of its MAC address ([see on page 27 “Entering the IP Parameters”](#)). Ethernet Switch Configurator Software is a Layer 2 protocol.

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

6.4.2 Enabling/disabling the Ethernet Switch Configurator Software Function

- Select the `Basics:Network` dialog.
- Disable the Ethernet Switch Configurator Software function in the "Ethernet Switch Configurator Software Protocol" frame or limit the access to "read-only".


```
enable
network protocol
  ethernet-switch-conf off
network protocol
  ethernet-switch-conf
  read-only
network protocol
  ethernet-switch-conf
  read-write
```

Switch to the Privileged EXEC mode.

Disable the Ethernet Switch Configurator Software function.

Enable the Ethernet Switch Configurator Software function with "read-only" access

Enable the Ethernet Switch Configurator Software function with "read-write" access

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.

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.

Examples of application areas include:

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

Select the method (SNMP or PTP) that best suits your requirements. If necessary, you can also use both methods simultaneously.

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 88](#) “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. Possible sources are: `local` and `sntp`. The source is initially `local`. If SNTP is activated and if the device receives a valid SNTP packet, the device sets its time source to `sntp`.

- With "Set time from PC", the device takes the PC time as the system time and calculates the IEEE 1588 / SNTP time using the local time difference.
"IEEE 1588 / SNTP time" = "System time" - "Local offset"
- The "Local Offset" is for displaying/entering the time difference between the local time and the "IEEE 1588 / SNTP time".

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

```
enable
configure
ntp time <YYYY-MM-DD
HH:MM:SS>
ntp client offset <-1000 to
1000>
```

Switch to the Privileged EXEC mode.

Switch to the Configuration mode.

Set the system time of the device.

Enter the time difference between the local time and the "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 client and the SNTP server function.

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

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

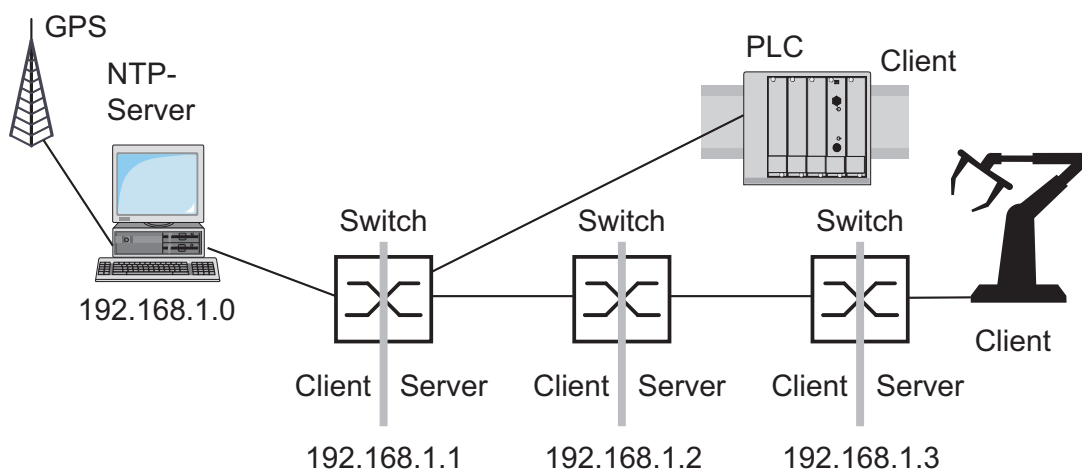


Figure 21: SNTP cascade

7.2.2 Preparing the SNTP Configuration

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

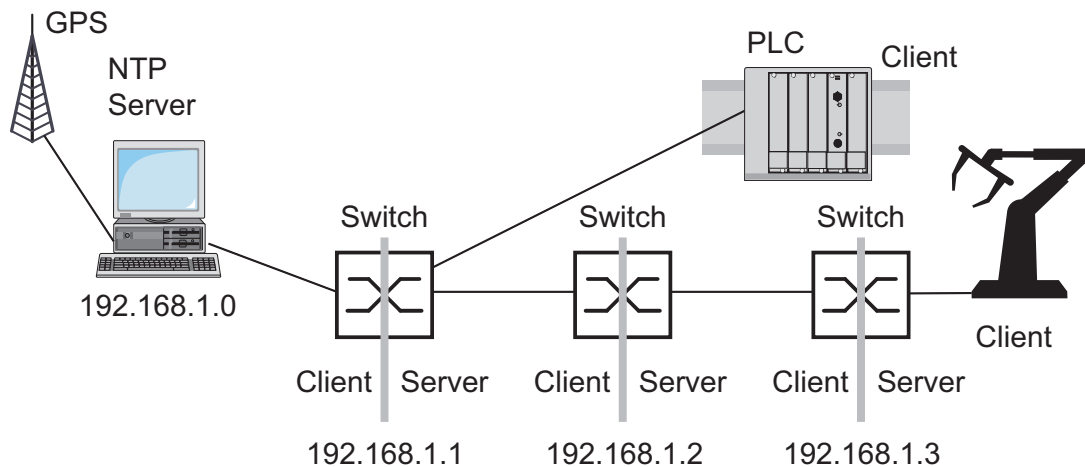


Figure 22: Example of SNTP cascade

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

7.2.3 Configuring SNTP

- Select the `Time:SNTP` dialog.
- ▶ Configuration SNTP Client and Server
 - In this frame you switch the SNTP function on/off globally.
- ▶ SNTP Status
 - The “Status message” displays statuses of the SNTP client as one or more test messages, e.g. `Server 2 not responding`.
- ▶ Configuration SNTP Server
 - In “Server status” you switch the SNTP server of the device on/off.
 - In “Anycast destination address” you enter the IP address to which the SNTP server of the device sends its SNTP packets (see table 4).
 - In “Anycast send interval” you specify the interval at which the device sends SNTP packets (valid entries: 1 s to 3,600 s, on delivery: 120 s).
 - With “Disable Server at local time source” the device disables the SNTP server function if the source of the time is `local` (see `Time` dialog).

IP destination address	Send SNTP 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 - 3,600 s, on delivery: 30 s).
- With “Accept SNTP Broadcasts” the device takes the system time from SNTP Broadcast/Multicast packets that it receives.

Configuration SNTP Client and Server

Operation On Off

Configuration SNTP Server

Anycast Destination Address 0.0.0.0

Anycast Send Interval [s] 120

Disable Server at local Time Source

SNTP Status

Configuration SNTP Client

External Server Address 0.0.0.0

Redundant Server Address 0.0.0.0

Server Request Interval [s] 30

Accept SNTP Broadcasts

Threshold for obtaining the UTC [ms] 0

Disable Client after successful Synchronization

Set Reload Help

Figure 23: 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. 22)

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 a LAN.

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

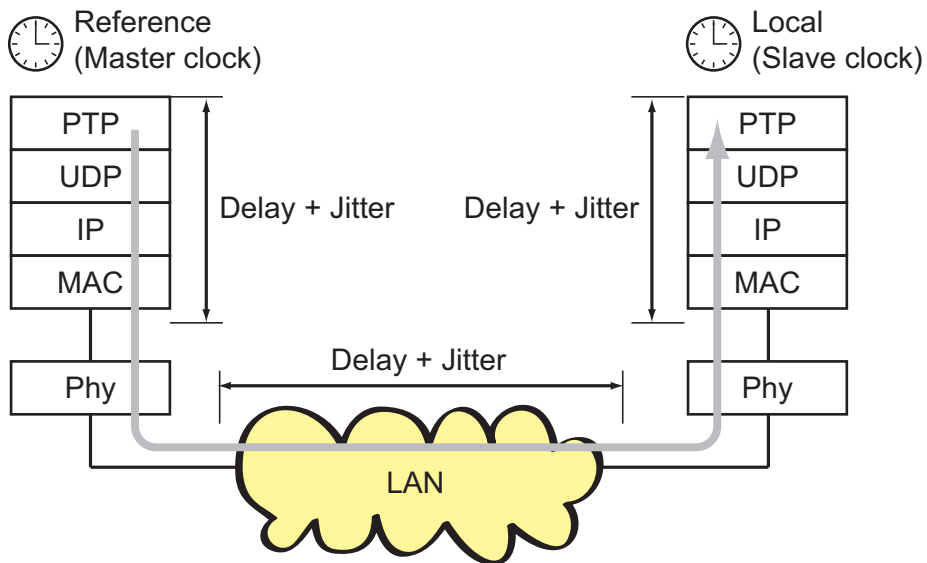
Factors influencing precision are:

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

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

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
- ▶ Prioritization - QoS

8.1 Direct Packet Distribution

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

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

8.1.1 Store-and-forward

All data received by the device is stored, and its validity is checked. Invalid and defective data packets (> 1502 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 destination addresses
- ▶ these destination addresses or
- ▶ a multi/broadcast destination address

in the destination address field are sent to this port. The device enters learned source addresses in its filter table ([see on page 98 “Entering Static Addresses”](#)).

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 particular age - the aging time - are deleted by the device from its address table.

Data packets with an unknown destination address are sent by the device to all ports.

Data packets with known destination addresses are selectively transmitted by the device.

Note: A reboot deletes the learned address entries.

- Select the `Switching:Global` dialog.
- Enter the aging time for all dynamic entries in the range from 10 to 630 seconds (unit: 1 second; default setting: 30).

8.1.4 Entering Static Addresses

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

The following are valid filter criteria:

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

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

- ▶ The management administrator describes the static part of the filter table (`dot1qStaticTable`).
- ▶ During operation, the device is capable of learning which of its ports receive data packets from which source address ([see on page 96 “Multi-Address Capability”](#)). This information is written to a dynamic part (`dot1qTpFdbTable`).

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 filter entries for Multicast addresses.

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

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

- ▶ `learned`: The filter was created automatically by the device.
- ▶ `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 63 "Saving settings").
- ▶ `igmp`: The filter was created by IGMP Snooping.

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

8.1.5 Disabling the Direct Packet Distribution

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

- Select the `Switching:Global` dialog.

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

8.2 Multicast Application

8.2.1 Description of the Multicast Application

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

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

In the case of a Multicast address, the device forwards all data packets with a Multicast address to all ports. This leads to an increased bandwidth requirement.

Procedures such as IGMP Snooping enable the device to exchange information via the direct transmission of Multicast data packets. The bandwidth requirement can be reduced by distributing the Multicast data packets only to those ports to which recipients of these Multicast packets are connected.

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

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

8.2.2 Example of a Multicast Application

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

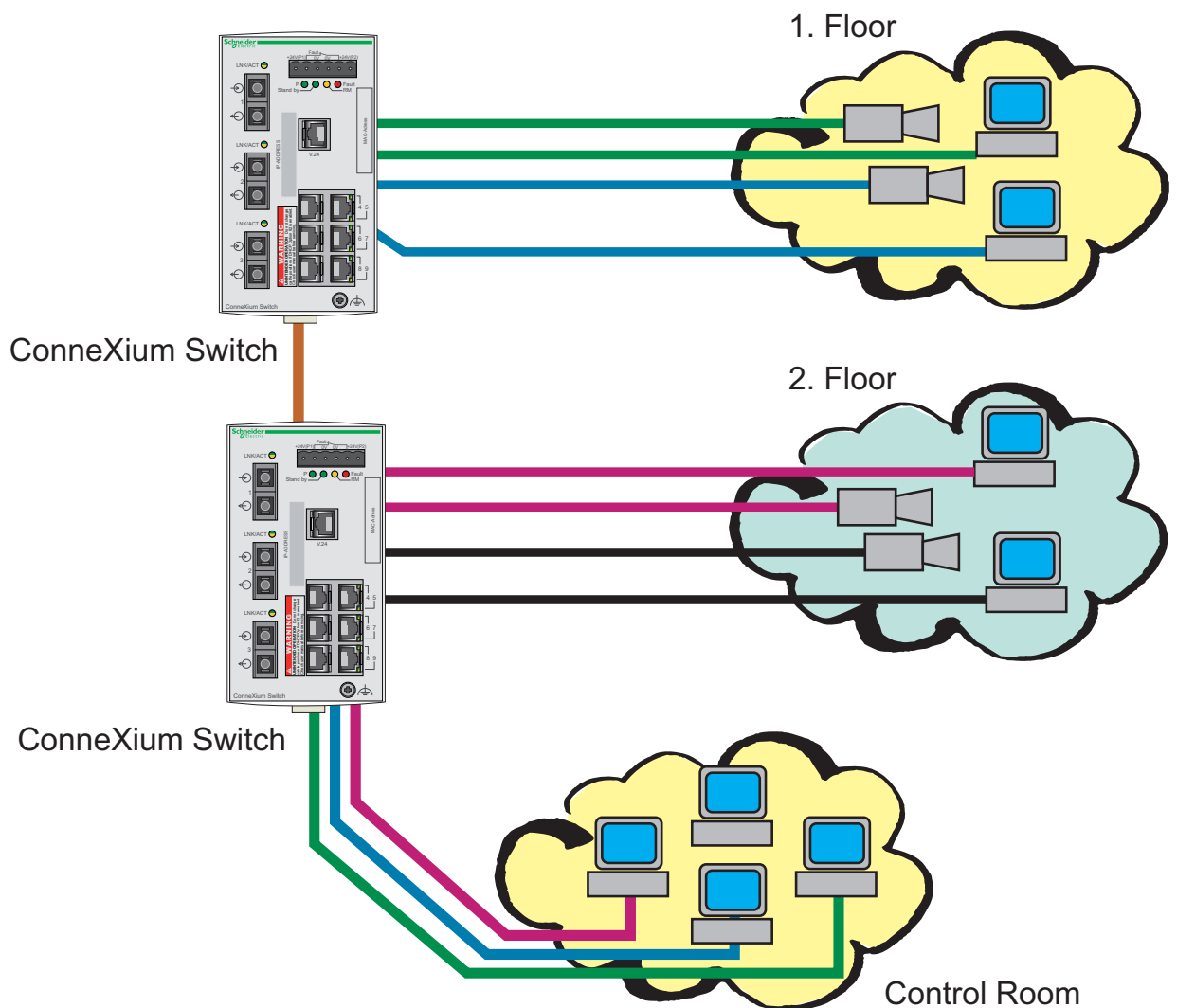


Figure 25: Example: Video surveillance in machine rooms

8.2.3 Description of IGMP Snooping

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

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

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

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

A Switch that connects a Multicast receiver with a router can evaluate the IGMP information 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, which are obtained via IGMP Snooping from the IP addresses, in the static address table. The Switch thus transmits these Multicast packets exclusively at the ports at which Multicast receivers are connected. The other ports are not affected by these packets.

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

Default setting: "Off".

8.2.4 Setting up the Multicast application

- Select the `Switching:Multicasts` dialog.

■ Global Configuration

The “Global Configuration” frame allows you to enable/disable IGMP Snooping globally for the entire device.

If IGMP Snooping is disabled, then

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

■ Settings for IGMP Querier and IGMP

With these frames you can enter global settings for the IGMP settings and the IGMP Querier function.

Prerequisite: The IGMP Snooping function is activated globally.

IGMP Querier

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

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

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

Note the connection between the parameters Max. Response Time, Send Interval and Group Membership Interval ([see on page 105 “Parameter Values”](#)).

IGMP-capable terminal devices respond to a query with a report message, thus generating a network load.

Select large sending intervals if you want to reduce the load on your network and can accept the resulting longer switching times.

Select small sending intervals if you require short switching times and can accept the resulting network load.

IGMP Settings

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

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

Note the connection between the parameters Max. Response Time, Send Interval and Group Membership Interval ([see on page 105 “Parameter Values”](#)).

The Multicast group members select a random value within the maximum response time for their response, to prevent all the Multicast group members responding to the query at the same time.

Select a large value if you want to reduce the load on your network and can accept the resulting longer switching times.

Select a small value if you require short switching times and can accept the resulting network load.

In “Group Membership Interval” you specify the period for which a dynamic Multicast group remains entered in the device if it does not receive any report messages (valid values: 3-3,600 s, default setting: 260 s).

Note the connection between the parameters Max. Response Time, Send Interval and Group Membership Interval ([see on page 105 “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 1-3,598 seconds	10 seconds
Send Interval	1, 2, 3	2-3,599 seconds	125 seconds
Group Membership Interval	1, 2, 3	3-3,600 seconds	260 seconds

Table 7: Value range for

- *Max. Response Time*
- *Send Interval*
- *Group Membership Interval*

■ Unknown Multicasts

Unknown Multicasts

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

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

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

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

■ Known Multicasts

Known Multicasts

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

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

■ Settings per Port (Table)

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

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

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

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

- ▶ “IGMP Automatic Query Port”
This table column shows you which ports the device has learned as query ports, if “automatic” is selected in “Static Query Port”.
- ▶ “Static Query Port”
The device sends IGMP report messages to the ports 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 connected Schneider Electric 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, you can obtain quick reconfiguration of the network for data packets with registered Multicast destination addresses with the following settings:

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

The screenshot shows the 'Multicasts dialog' configuration interface. It is divided into several sections:

- Global Configuration:** Includes radio buttons for 'IGMP Snooping' (disabled) and 'disabled'.
- IGMP Querier:** Includes a checkbox for 'IGMP Querier active', 'Protocol Version' (radio buttons for 1, 2, 3), and 'Transmit Interval [s]' (input field with value 125).
- IGMP Settings:** Includes input fields for 'Current Querier IP Address' (0.0.0.0), 'Max Response Time [s]' (10), and 'Group Membership Interval [s]' (260).
- Unknown Multicasts:** Includes radio buttons for 'Send To Query Ports', 'Send To All Ports' (selected), and 'Discard'.
- Known Multicasts:** Includes radio buttons for 'Send to Query and registered Ports' and 'Send to registered Ports' (selected).

Below these sections is a table with the following columns: Module, Port, IGMP enabled, IGMP Form. All, IGMP Automatic Query Port, Static Query Port, and Learned Query Port. The table contains 8 rows, all with '1' in the Module column and '1' through '8' in the Port column. The 'IGMP enabled' column is checked for all rows. The 'IGMP Form. All' column is checked for all rows. The 'IGMP Automatic Query Port' column is checked for all rows. The 'Static Query Port' and 'Learned Query Port' columns are set to 'disabled' for all rows.

At the bottom of the dialog are 'Set' and 'Reload' buttons, and a 'Help' button in the bottom right corner.

Figure 26: Multicasts dialog

8.3 QoS/Priority

8.3.1 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, this provides optimal data flow for time-critical data traffic.

The device supports 4 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)

8.3.2 VLAN tagging

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

For data packets with a VLAN tag, the device evaluates:

- ▶ the priority information.

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 traffic classes

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

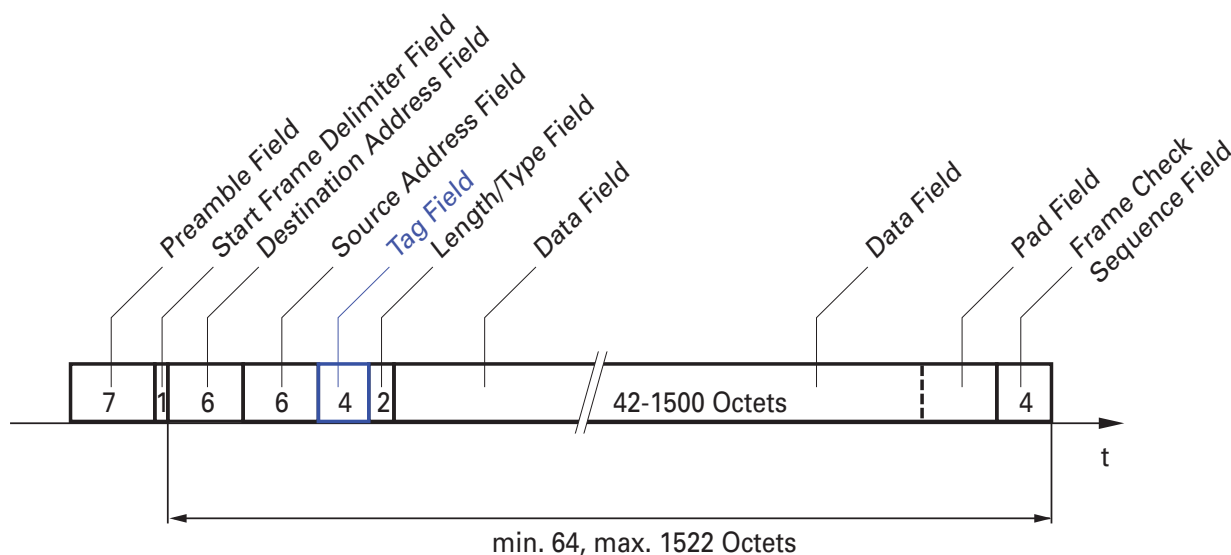


Figure 27: Ethernet data packet with tag

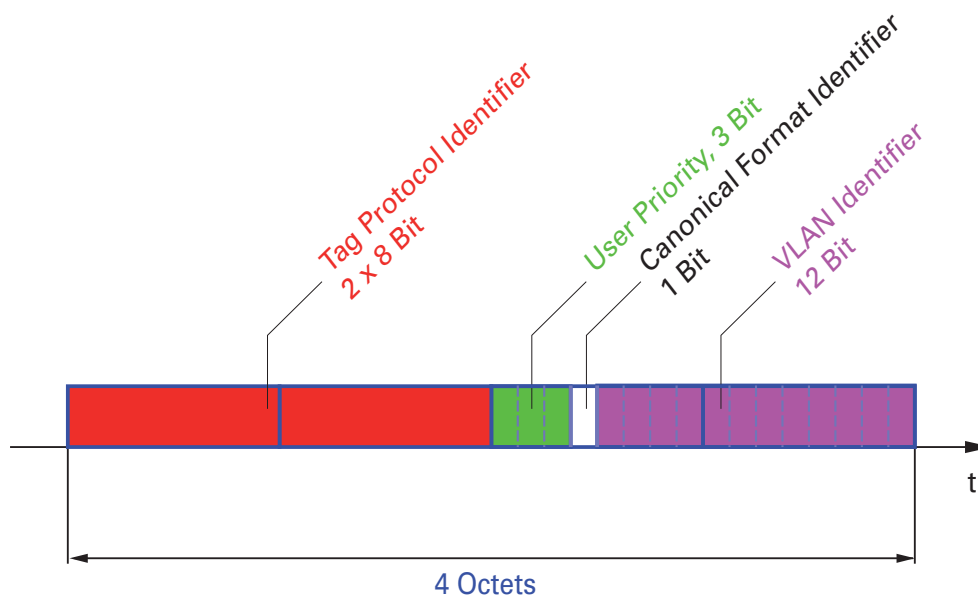


Figure 28: Tag format

When using VLAN prioritizing, note the following special features:

- ▶ End-to-end prioritizing requires the VLAN tags to be transmitted to the entire network, which means that all network components must be VLAN-capable.

- ▶ Routers cannot receive or send packets with VLAN tags via port-based router interfaces.

8.3.3 IP ToS / DiffServ

■ Differentiated Services

The newly defined Differentiated Services field in the IP header (see fig. 29) - often known as the DiffServ code point or DSCP, replaces the ToS field and is used to mark the individual packets with a DSCP. Here the packets are divided into different quality classes. The first 3 bits of the DSCP are used to divide the packets into classes. The next 3 bits are used to further divide the classes on the basis of different criteria. In contrast to the ToS byte, DiffServ uses six bits for the division into classes. This results in up to 64 different service classes.

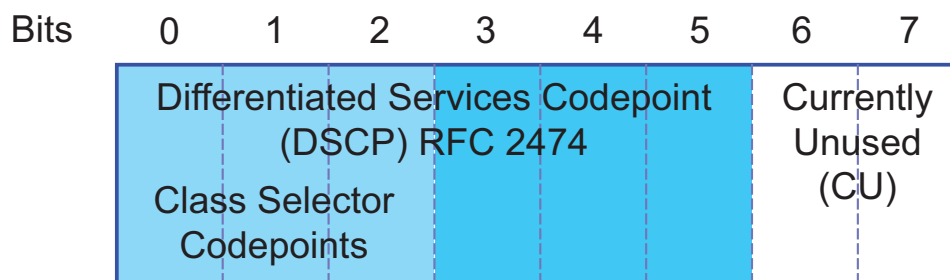


Figure 29: Differentiated Services field in the IP header

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

- ▶ Class Selector (CS0-CS7): For reasons of compatibility to TOS/IP Precedence
- ▶ Expedited Forwarding (EF): Premium service. Reduced delay, jitter + packet loss (RFC2598)
- ▶ Assured Forwarding (AF): Provides a differentiated schema for handling different data traffic (RFC2597).

- 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 9: 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 10: Mapping the DSCP values onto the traffic classes

■ TYPE of Service

The Type of Service (ToS) field in the IP header (see table 11) 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 11: ToS field in the IP header

8.3.4 Handling of Received Priority Information

The device provides 3 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 111 “VLAN tagging”](#)). You can modify this assignment. The device assigns the port priority to packets that it receives without a tag.
- ▶ **untrusted**
The device ignores the priority information in the packet and always assigns the packets the port priority of the receiving port.
- ▶ **trust ip-dscp**
The device assigns the IP packets to the different traffic classes according to the DSCP value in the IP header, even if the packet was also VLAN-tagged. The assignment is based on the pre-defined values ([see table 10](#)). You can modify this assignment.
The device prioritizes non-IP packets according to the port priority.

8.3.5 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, packets with lower traffic classes cannot be sent when there is a high level of data traffic.

When Strict Priority is set, the high-priority data in applications that are time- or latency-critical, such as VoIP or video, is sent immediately.

8.3.6 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.

```
enable
configure
interface 1/1

vlan priority 3
exit
```

Switch to the Privileged EXEC mode.
 Switch to the Configuration mode.
 Switch to the Interface Configuration mode of interface 1/1.
 Assign port priority 3 to interface 1/1.
 Switch to the Configuration mode.

■ Assigning the VLAN Priority to the Traffic Classes

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

```
enable
configure
classofservice dot1p-
mapping 0 2
classofservice dot1p-
mapping 1 2
exit
show classofservice dot1p-
mapping
```

Switch to the Privileged EXEC mode.
 Switch to the Configuration mode.
 Assign traffic class 2 to VLAN priority 0.

 Also assign traffic class 2 to VLAN priority 1.

 Switch to the privileged EXEC mode.
 Display the assignment.

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

■ Assigning the traffic class to a DSCP

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

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

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

■ **Always assign the DSCP priority to received IP data packets globally**

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

<code>enable</code>	Switch to the Privileged EXEC mode.
<code>configure</code>	Switch to the Configuration mode.
<code>classofservice trust ip-</code>	Assign the "trust ip-dscp" mode globally.
<code>dscp</code>	
<code>exit</code>	Switch to the Configuration mode.
<code>exit</code>	Switch to the privileged EXEC mode.
<code>show classofservice trust</code>	Display the trust mode.
Class of Service Trust Mode: IP DSCP	

9 Operation Diagnosis

The device provides you with the following diagnostic tools:

- ▶ Sending traps
- ▶ Monitoring device status
- ▶ Out-of-band signaling via signal contact
- ▶ Port status indication
- ▶ Event counter at port level
- ▶ Topology discovery
- ▶ Detecting IP address conflicts
- ▶ 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 List of SNMP Traps

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 the agent without permission.
coldStart	is sent for both cold and warm starts during the boot process after successful management initialization.
saBackUpConfigAdapterTrap	is sent when Memory Backup Adapter EAM is removed or plugged in.
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.
saPowerSupply	is sent if the status of the voltage supply changes.
saSigConRelayChange	is sent if the status of the signal contact changes during the operation monitoring.
newRoot	is sent if the sending agent becomes the 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.
saRingRedReconfig	is sent if the configuration of the HIPER-Ring changes.
saSNTPTrap	is sent if errors occur in connection with the SNTP (e.g. server cannot be reached).
saRelayDuplicateTrap	is sent if a duplicate IP address is detected in connection with DHCP Option 82.
lldpRemTablesChangeTrap	is sent if an entry in the topology remote table is changed.

Table 12: Possible traps

9.1.2 SNMP Traps during Boot

The device sends the ColdStart trap every time it boots.

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 “IP Address” column, enter the IP address of the recipient to whom the traps should be sent.
- In the “Enabled” column, you select 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.

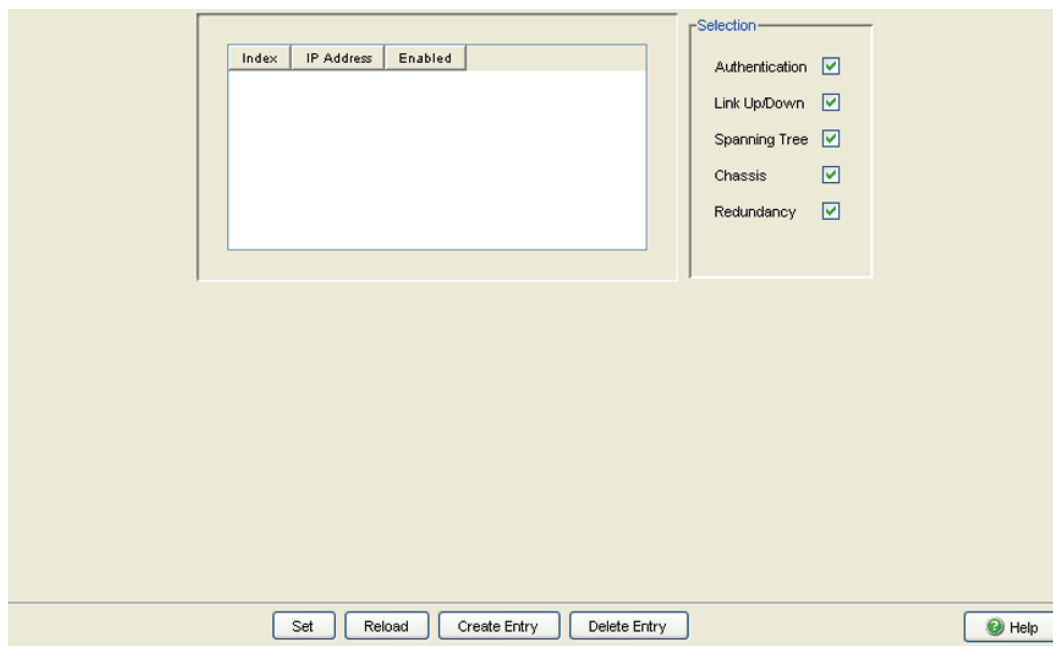


Figure 30: Alarms (Traps) Dialog

The events which can be selected are:

Name	Meaning
Authentication	The device has rejected an unauthorized access attempt (see on page 74 “Dealing with Unauthorized Access”).
Link Up/Down	At one port of the device, the link to another device has been established/interrupted.
Spanning Tree	The topology of the Rapid Spanning Tree has changed.
Chassis	Summarizes the following events: <ul style="list-style-type: none"> – The status of a supply voltage has changed (see the <code>System</code> dialog). – The status of the signal contact has changed. To take this event into account, you activate “Create trap when status changes” in the <code>Diagnostics:Signal Contact 1/2</code> dialog. <ul style="list-style-type: none"> – A media module has been added or removed (only for modular devices). – The Memory Backup Adapter (EAM) has been added or removed.
Redundancy	The redundancy status of the ring redundancy (redundant line active/inactive) or (for devices that support redundant ring/network coupling) the redundant ring/network coupling (redundancy exists) has changed.

Table 13: 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 130 “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, at least one of the two supply voltages is inoperative, the internal supply voltage is inoperative.
- ▶ The removal of the Memory Backup Adapter.
- ▶ 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.

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

Note: With a non-redundant voltage supply, the device reports the absence of a supply voltage. If you do not want this message to be displayed, feed the supply voltage over both inputs or switch off the monitoring (see on page 130 “Monitoring the Device Status 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.

```
enable
configure
device-status monitor all
error
device-status trap enable
```

Switch to the Privileged EXEC mode.

Switch to the Configuration mode.

Include all the possible events in the device status determination.

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.

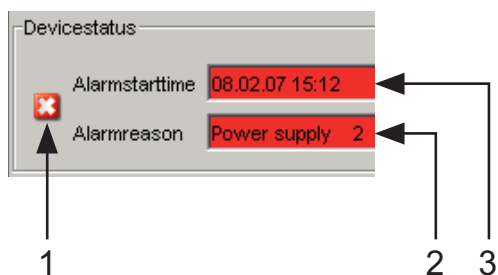


Figure 31: Device status and alarm display

- 1 - The symbol displays the device status*
- 2 - Cause of the oldest existing alarm*
- 3 - Start of the oldest existing alarm*

```
exit
```

```
show device-status
```

Switch to the privileged EXEC mode.

Display the device status and the setting for the device status determination.

9.3 Out-of-band Signaling

The signal contact is used to control external devices and monitor the operation of the device. Function monitoring enables you to perform remote diagnostics.

The device reports the operating status via a break in the potential-free signal contact (relay contact, closed circuit):

- ▶ Incorrect supply voltage, at least one of the two supply voltages is inoperative, the internal supply voltage is inoperative.
- ▶ 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.

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

Note: With a non-redundant voltage supply, the device reports the absence of a supply voltage. If you do not want this message to be displayed, feed the supply voltage over both inputs or switch off the monitoring ([see on page 130 “Monitoring the Device Status 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 as an input for process control monitoring equipment.
- ▶ 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.

<code>enable</code>	Switch to the Privileged EXEC mode.
<code>configure</code>	Switch to the Configuration mode.
<code>signal-contact 1 mode manual</code>	Select the manual setting mode for signal contact 1.
<code>signal-contact 1 state open</code>	Open signal contact 1.
<code>signal-contact 1 state closed</code>	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 126 "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.

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

■ Displaying the signal contact's status

The device gives you 3 additional options for displaying the status of the signal contact:

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

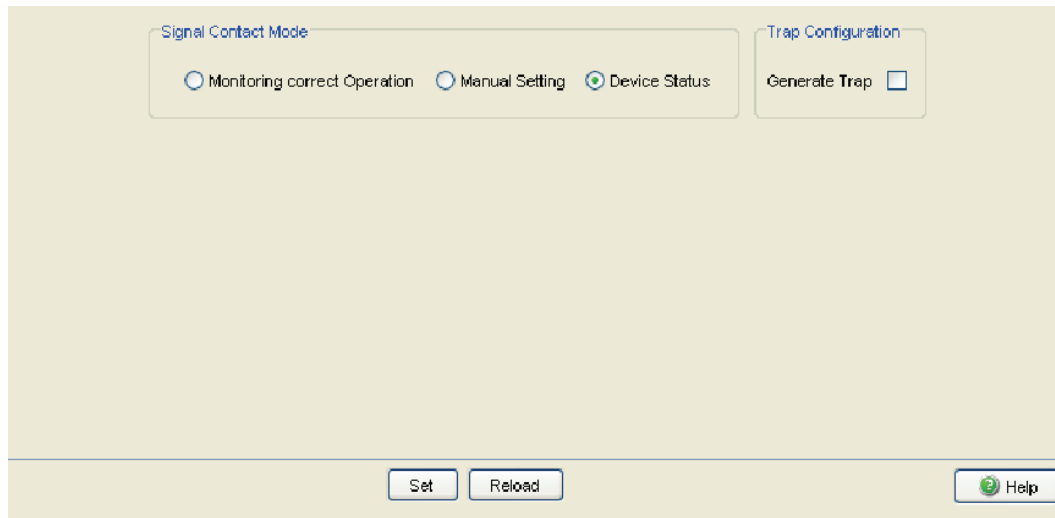


Figure 32: Signal Contact Dialog

```
exit  
show signal-contact 1
```

Switch to the privileged EXEC mode.
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.

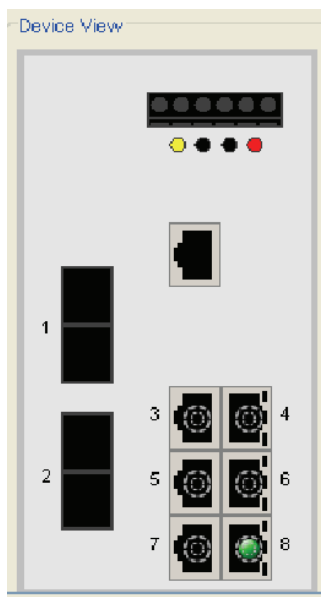








Figure 33: Device View

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).

9.5 Event Counter at Port Level

The port statistics table enables experienced network administrators to identify possible detected problems in the network.

This table shows you the contents of various event counters. In the Restart menu item, you can reset 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 detected problem
Received fragments	<ul style="list-style-type: none">– The controller of the connected device is inoperable– Electromagnetic interference in the transmission medium
CRC error	<ul style="list-style-type: none">– The controller of the connected device is inoperable– Electromagnetic interference in the transmission medium– Defective component in the network
Collisions	<ul style="list-style-type: none">– The controller of the connected device is inoperable– Network overextended/lines too long– Collision of a fault with a data packet

Table 14: Examples indicating possible detected problems

- Select the `Diagnostics:Ports:Statistics` dialog.
- To reset the counters, click on "Reset port counters" in the `Basic Settings:Restart` dialog.

Module	Port	Transmitted Packets	Transmitted Unicast Packets	Transmitted Non Unicast Packets	Received Packets	Received Octets	Received Fragments	Detected CRC errors	Detected Collisions	Detected Late Collisions	Packets 64 bytes	Packets 65 to 127 bytes
1	1	0	0	0	0	0	0	0	0	0	0	0
1	2	0	0	0	0	0	0	0	0	0	0	0
1	3	0	0	0	0	0	0	0	0	0	0	0
1	4	0	0	0	0	0	0	0	0	0	0	0
1	5	0	0	0	0	0	0	0	0	0	0	0
1	6	0	0	0	0	0	0	0	0	0	0	0
1	7	0	0	0	0	0	0	0	0	0	0	0
1	8	57532	50879	6653	311313	18863795	0	0	0	0	131671	7971

Figure 34: Port Statistics dialog

9.6 Topology Discovery

9.6.1 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. This can be evaluated there 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 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
- ▶ Currently activated system capabilities
- ▶ Interface ID of the management address
- ▶ 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 (for example, RSTP, HIPER-Ring, MRP).

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 2 LLDP-capable devices prevents LLDP information exchange between these two devices.

To get around this, Schneider Electric devices send and receive additional LLDP packets with the Schneider Electric Multicast MAC address 01:80:63:2F:FF:0B. Schneider Electric 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 device holds the LLDP information in the LLDP MIB.

9.6.2 Displaying the Topology Discovery Results

-  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.

Configuration

Operation On Off

Module	Port	Neighbor Identifier	Neighbor IP Address	Neighbor Port Description	Neighbor System Name
1	8	00:80:63:97:50:00	10.0.1.220	Module: 1 Port: 7 - 10/100 ...	TCSESM063F2CU1

Set Reload Show LLDP entries exclusively Help

Figure 35: Topology Discovery dialog

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 on page 98 “Entering Static Addresses”](#)).

9.7 Detecting IP Address Conflicts

9.7.1 Description of IP Address Conflicts

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

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

Table 15: Possible address conflict operation modes

9.7.2 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 15](#)).

9.7.3 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.

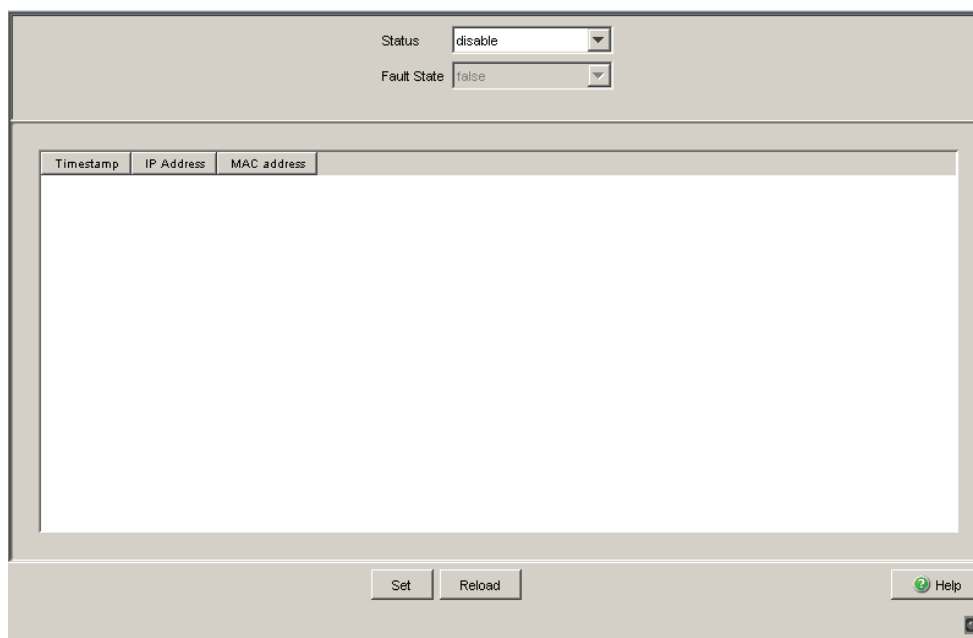


Figure 36: IP Address Conflict Detection dialog

9.8 Reports

The following reports are available for the diagnostics:

- ▶ Log file
The log file is an HTML file to which the device writes important device-internal events
- ▶ System information.
The system information is an HTML file containing system-relevant data.

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.

9.9 Monitoring Data Traffic at Ports (Port Mirroring)

The port mirroring function enables you to review the data traffic at a device port for diagnostic purposes. The device additionally forwards (mirrors) this data to another port. This process is also called port mirroring.

The port to be observed is called the source port. The port to which the data to be observed is copied is called the destination port.

In port mirroring, the device copies valid incoming **and** outgoing data packets of the source port to 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 data traffic of the source port. Set the destination port as a member in all VLANs.

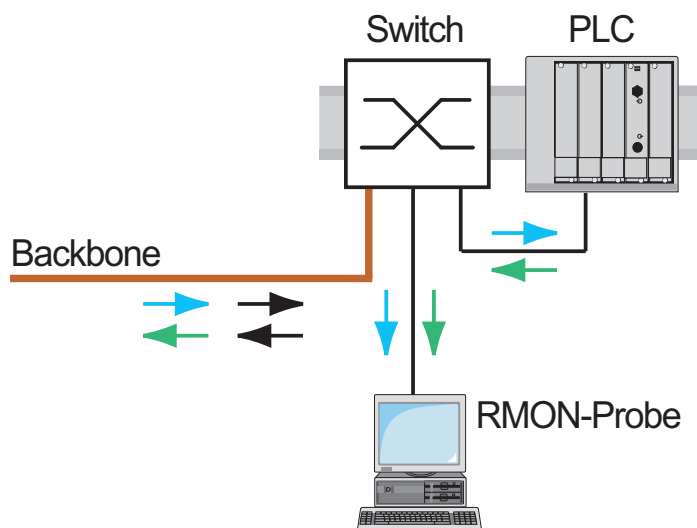


Figure 37: Port mirroring

- 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.

	Module	Port
Source port	1	0
Destination port	1	0

enabled

Buttons: Set, Reload, Delete, Help

Figure 38: Portmirroring dialog

A Setting up the Configuration Environment

A.1 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.1.1 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. 39](#)) and whether the status of this process is "IW":

SunOS

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

HP

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

If the process is not entered or only entered as a comment line (`#`), modify `/etc/inetd.conf` accordingly and then re-initialize the INET daemon. This is performed with the command "kill -1 PID", where PID is the process number of inetd.

This re-initialization can be executed automatically by entering the following UNIX commands:

SunOS

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

HP

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

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

Note: The command "ps" does not 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 /etc/passwd file.

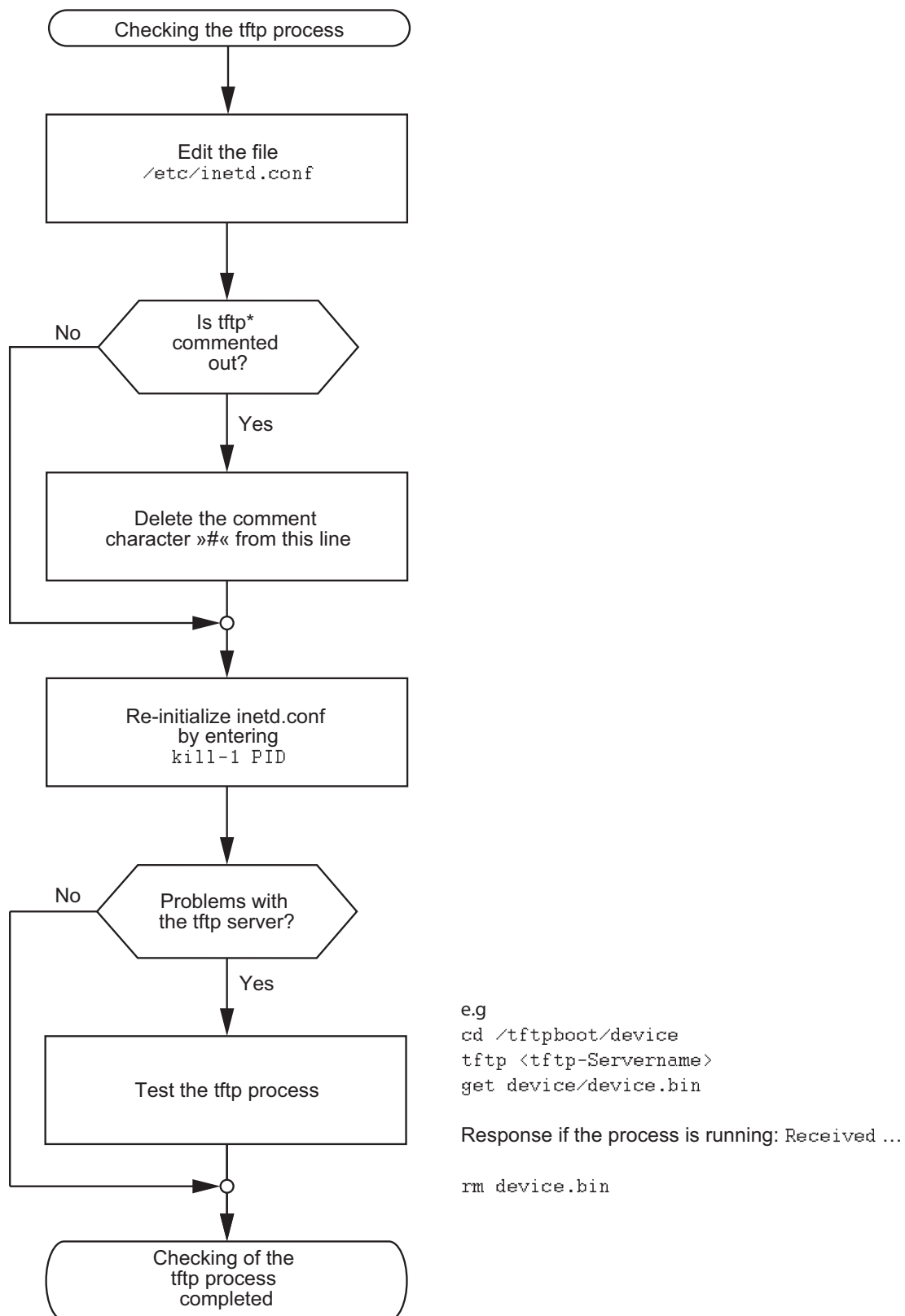
For example:

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

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

- Test the tftp process with, for example:

```
cd /tftpboot/device  
tftp <tftp-Servername>  
get device/device.bin  
rm device.bin
```

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

Figure 39: Flow chart for setting up tftp server with SunOS and HP

A.1.2 Software Access Rights

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

■ Example of a UNIX tftp Server

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

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

Table 16: 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 Abbreviations used

EAM	Memory Backup 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
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocol
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocol
F/O	Optical Fiber
MAC	Media Access Control
NTP	Network Time Protocol
PC	Personal Computer
PTP	Precision Time Protocol
QoS	Quality of Service
RFC	Request For Comment
RM	Redundancy Manager
RS	Rail Switch
RSTP	Rapid Spanning Tree Protocol
SFP	Small Form-factor Pluggable
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TP	Twisted Pair
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network

B.2 Technical Data

You will find the technical data in the document “Web-based Interface Reference Manual”.

C Index

A		Data transfer parameter	18
ACD	142	Destination address	98, 98, 99
AF	113	Destination address field	97
APNIC	29	Destination table	122
ARIN	29	Device Status	126, 126, 129
ARP	33	Device status	126
Access rights	75	DiffServ	110
Access security	71	DiffServ-Codepoint	113
Access with Web-based interface, password	76	Differentiated Services	113
		Dynamic	98
Address Conflict Detection	142	E	
Address conflict	142	EAM	41, 58, 125
Address table	97	EF	113
Aging Time	97, 97	Ethernet Switch Configurator Software	38, 80, 80
Aging time	102, 102	Expedited Forwarding	113
Alarm	124	F	
Alarm messages	122	FDB	98
Assured Forwarding	113	Faulty device replacement	55
Automatic configuration	71	Filter	98
B		Filter table	98
BOOTP	27, 48, 58	First installation	27
Bandwidth	100	Flash memory	62
Booting	18	Forwarding database	98
Broadcast	89, 96, 98, 100	G	
Browser	22	Gateway	30, 36
		Grandmaster	91
C		H	
CIDR	34	HIPER-Ring	11
CLI access, password	76	HIPER-Ring (source for alarms)	125
Class Selector	113	Hardware address	44
Classless Inter-Domain Routing	33, 34	Hardware reset	122
Clock	91	Host address	30
Clock synchronization	93	I	
Closed circuit	129	IANA	29
Command Line Interface	20	IEEE 1588 time	84
Configuration	62	IEEE 802.1 Q	111
Configuration changes	122	IEEE MAC address	138
Configuration data	43, 51, 60, 63	IGMP	102
Configuration file	48, 59	IGMP Querier	104
Connection error	72	IGMP Snooping	100, 102, 102
D		IP Address	48
DHCP	28, 48, 48, 51, 58	IP Parameter	27
DHCP Client	48	IP address	29, 36, 44, 142
DHCP Option 82	51		
DHCP client	48		
DHCP server	84		
DSCP	113, 116, 118, 119		

IP header	110, 115	Priority queues	110
IP- Header	113	Priority tagged frames	111
ISO/OSI layer model	33		
Internet Assigned Numbers Authority	29	Q	
Internet service provider	29	QoS	110
		Query	102
J		Query function	104
Java Runtime Environment	22	Queue	116
JavaScript	23		
		R	
L		RIPE NCC	29
LACNIC	29	RMON-Probe	146
Leave	102, 102	Read access	24
Link monitoring	126, 129	Real time	83, 110
Local clock	92	Receiving port	99
Login	23	Redundancy	11
		Reference clock	84, 87, 91
M		Relay contact	129
MAC destination address	33	Remote diagnostics	129
MRP	11	Report	102, 145
Media module (for modular devices), source		Request interval (SNTP)	89
for alarms	125	Ring manager	98
Memory Backup Adapter	41	Ring/Network Coupling	11
Message	122	Ring/Network coupling (source for alarms)	125
Multicast	89, 98, 100, 102	Router	30
N		S	
NTP	86, 88	SNMP	22, 75, 122
Netmask	30, 36	SNMPv3 access, password	76
Network address	29	SNTP	83, 86, 88
Network topology	51	SNTP client	86, 88
		SNTP server	86
O		Segmentation	122
Operating mode	71	Service	145
Operation monitoring	129	Service provider	29
Option 82	28, 51	Signal contact	72, 129
Out-of-band	20	Signal contact (source for alarm)	125
		Signal runtime	87
P		Simple Network Time Protocol	83
PHB	113	Software	154
PTP	83, 84, 91	Software release	67
Password	21, 24, 64, 77	Source address	96
Password for CLI access	76	State on deliver	62
Password for SNMPv3 access	76	State on delivery	62, 75
Password for access with Web-based interface	76	Static	98
Polling	122	Strict Priority	116, 116
Port configuration	71	Subnetwork	36, 97
Port mirroring	147	Summer time	84
Port priority	116	Supply voltage	125
Port-Mirroring	146	Symbol	13
Precedence	113	System Monitor	18, 18
Precision Time Protocol	83, 91	System Name	48
Priority	111, 116	System name	48

System time 87, 89

T

TCP/IP stack 151
TFTP 150
TFTP Update 69
Time difference 84
Time management 91
Time zone 84
ToS 110, 113, 115
Topology 51
Traffic class 116, 117, 118
Traffic classes 110
Transmission reliability 122
Trap 122, 124
Trap Destination Table 122
Trivial File Transfer Protocol 150
Trust dot1p 116
Trust ip-dscp 116
Type Field 111
Type of Service 115

U

UTC 84
Unicast 100
Untrusted 116
Update 18
User name 21

V

V.24 20
VLAN 111, 116
VLAN Tag 111
VLAN priority 117
VLAN tag 111
VLAN-ID (device network parameters) 53
Video 116
VoIP 116

W

Web-based Interface 22
Web-based interface 22
Web-based management 23
Website 24
Winter time 84
Write access 24

