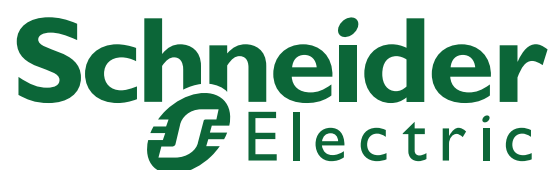


ConneXium Ethernet Cabling System

**TCSESM, TCSESM-E Managed Switch
Basic Configuration User Manual**

31007122.04

www.schneider-electric.com



Content

Safety information	9
About this Manual	11
Key	15
Introduction	17
1 Access to the user interfaces	19
1.1 System Monitor	20
1.2 Command Line Interface	22
1.3 Web-based Interface	25
2 Entering the IP Parameters	29
2.1 IP Parameter Basics	31
2.1.1 IP address (version 4)	31
2.1.2 Netmask	32
2.1.3 Classless Inter-Domain Routing	35
2.2 Entering IP parameters via CLI	37
2.3 Entering the IP Parameters via Ethernet Switch Configurator Software	40
2.4 Loading the system configuration from the EAM	43
2.5 System configuration via BOOTP	45
2.6 System Configuration via DHCP	50
2.7 System Configuration via DHCP Option 82	53
2.8 Web-based IP configuration	55
2.9 Faulty device replacement	57
3 Loading/saving settings	59
3.1 Loading settings	60
3.1.1 Loading from the local non-volatile memory	61

3.1.2	Loading from the Memory Backup Adapter	61
3.1.3	Loading from a file	62
3.1.4	Resetting the configuration to the state on delivery	64
3.2	Saving settings	65
3.2.1	Saving locally (and on the EAM)	65
3.2.2	Saving to a file on URL	66
3.2.3	Saving as a script on the PC	67
4	Loading software updates	69
4.1	Loading the software from the tftp server	70
4.2	Loading the software via file selection	72
5	Configuring the ports	73
6	Protection from unauthorized access	75
6.1	Password for SNMP access	76
6.1.1	Description of password for SNMP access	76
6.1.2	Entering the password for SNMP access	77
6.2	Telnet/Web access	80
6.2.1	Description of Web access	80
6.2.2	Enabling/disabling Telnet/Web access	80
6.3	Ethernet Switch Configurator Software settings	81
6.3.1	Description of the Ethernet Switch Configurator Software protocol	81
6.3.2	Enabling/disabling the Ethernet Switch Configurator Software function	81
6.4	Port access control	83
6.4.1	Description of the port access control	83
6.4.2	Application example for port access control	84
7	Synchronizing the System Time in the Network	87
7.1	Entering the time	88
7.2	SNTP	90
7.2.1	Description of SNTP	90
7.2.2	Preparing the SNTP coordination	91
7.2.3	Configuring SNTP	92

7.3	Precision Time Protocol	95
7.3.1	Description of PTP functions	95
8	Network load control	99
8.1	Direct packet distribution	100
8.1.1	Store-and-forward	100
8.1.2	Multi-address capability	100
8.1.3	Aging of learned addresses	101
8.1.4	Entering static address entries	102
8.1.5	Disabling the direct packet distribution	103
8.2	Multicast application	105
8.2.1	Description of the Multicast application	105
8.2.2	Example of a Multicast application	106
8.2.3	Description of IGMP Snooping	107
8.2.4	Description of GMRP	108
8.2.5	Setting up the Multicast application	109
8.3	Rate Limiter	116
8.3.1	Description of the Rate Limiter	116
8.3.2	Rate Limiter settings	116
8.4	QoS/Priority	118
8.4.1	Description of Prioritization	118
8.4.2	VLAN tagging	119
8.4.3	IP ToS / DiffServ	121
8.4.4	Management prioritization	124
8.4.5	Handling of received priority information	125
8.4.6	Handling of traffic classes	125
8.4.7	Setting prioritization	126
8.5	Flow control	130
8.5.1	Description of flow control	130
8.5.2	Setting the flow control	132
8.6	VLANs	133
8.6.1	VLAN description	133
8.6.2	Examples of VLANs	134
9	Operation diagnosis	151
9.1	Sending traps	152
9.1.1	SNMP traps during boot	152

9.1.2	Configuring traps	153
9.2	Monitoring the device status	155
9.2.1	Configuring the device status	156
9.2.2	Displaying the device status	157
9.3	Out-of-band signaling	158
9.3.1	Controlling the signal contact	158
9.3.2	Monitoring the device status via the signal contact	159
9.3.3	Monitoring the device functions via the signal contact	160
9.4	Port status indication	162
9.5	Event counter at port level	164
9.6	Topology discovery	166
9.6.1	Description of topology discovery	166
9.6.2	Displaying the topology discovery	168
9.7	Detecting IP address conflicts	171
9.7.1	Description of IP address conflicts	171
9.7.2	Configuring ACD	172
9.7.3	Displaying ACD	173
9.8	Reports	174
9.9	Monitoring port traffic (port mirroring)	175
10	EtherNet/IP	177
10.1	Integration into a Control System	179
10.2	EtherNet/IP Parameters	180
10.2.1	Identity Object	180
10.2.2	TCP/IP Interface Object	181
10.2.3	Ethernet Link Object	183
10.2.4	Ethernet Switch Agent Object	185
10.2.5	I/O Data	187
10.2.6	Mapping of the Ethernet Link Object Instances	188
10.2.7	Supported Services	189
10.3	TCSESM in a Premium System	190
10.3.1	Adding EDS Files	191
10.3.2	Adding one or more EDS files to the Device Library	192
10.3.3	Automatically Detect and Add the TCSESM Switch	194
10.3.4	Configuring the TCSESM Switch Properties	195

10.3.5	Viewing the TCSESM Switch Data	198
10.3.6	SEND_REQ Example-Get_Attributes_Single	200
10.4	TCSESM in a Quantum System	206
10.4.1	Adding EDS Files	207
10.4.2	Adding one or more EDS files to the Device Library	208
10.4.3	Automatically Detect and Add the TCSESM Switch	210
10.4.4	Configuring the TCSESM Switch Properties	211
10.4.5	Viewing the TCSESM Switch Data	214
10.4.6	MPB_MSTR Example-Get_Attributes_Single	216
A	Setting up the Configuration Environment	223
A.1	TFTP Server for Software Updates	224
A.1.1	Setting up the tftp process	225
A.1.2	Software access rights	228
B	General Information	229
B.1	Abbreviations used	230
B.2	Technical Data	231
C	Index	233

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.

© 2010 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 Ethernet Cabling System Managed Switch User Manual Redundancy Configuration	31007126.03
ConneXium Ethernet Cabling System Managed Switch User Manual Basic Configuration	31007122.04
ConneXium Ethernet Cabling System Managed Switch Reference Manual Command Line Interface	31007130.03
ConneXium Ethernet Cabling System Managed Switch Reference Manual Web-based Interface	EIO0000000482.01
ConneXium Ethernet Cabling System Managed Switch Installation Manual TCSESM	31007118.05
ConneXium Ethernet Cabling System Managed Switch Installation Manual TCSESM-E	EIO0000000529.01

Note: The Glossary you will find 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 before you begin with the configuration of the device.





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

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






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

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:

	Router with firewall
	Switch with firewall
	Router
	Switch
	Bridge

Key



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 three user interfaces, which you can access via different interfaces:

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

1.1 System Monitor

The system monitor enables you to

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

■ Opening the system monitor

- Use the terminal cable (see accessories) to connect
 - the V.24 socket (RJ11) to
 - a terminal or a COM port of a PC with terminal emulation based on VT100(for the physical connection, see the "Installation" user manual).

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

Table 1: Data transfer parameters

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

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

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

Figure 1: Screen display during the boot process

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

```
System Monitor
(Selected OS: L3P-01.0.00-K16 (2005-10-31 19:32))
1  Select Boot Operating System
2  Update Operating System
3  Start Selected Operating System
4  End (reset and reboot)
5  Erase main configuration file

sysMon1>
```

Figure 2: System monitor 1 screen display

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

1.2 Command Line Interface

The Command Line Interface enables you to use 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) or
- ▶ Telnet (in-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 ([see on page 20 "Opening the system monitor"](#)) or call up the Command Line Interface via Telnet. A window for entering the user name appears on the screen. Up to five users can access the Command Line Interface.

```
Copyright (c) 2004-2009 Schneider Electric
All rights reserved
```

```
TCSESM-E Release L2S-05.0.00
```

```
(Build date 2009-05-11 19:32)
```

```
System Name: TCSESM063F2CU1
Mgmt-IP      : 10.0.1.105
1.Router-IP: 0.0.0.0
Base-MAC     : 00:80:63:51:74:00
System Time: 2009-05-21 16:00:59
```

User:

Figure 3: Logging in to the Command Line Interface program

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

The start screen appears.

Note: For a TCSESM switch, the default CLI prompt is (Schneider Electric TCSESM) >, for a TCSESM-E switch, it is (Schneider Electric TCSESM-E) >.

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

(Schneider Electric TCSESM) >

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 the Java software version 5 or later ("Java™ Runtime Environment Version 1.5.x or 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.



schneider-electric.com

ConneXium im web

ConneXview im web



ConneXium Resource CD
 Haben Sie vielen Dank für den Kauf eines ConneXium verwalteten Schalters. Diese CD enthält sämtliche benötigten Informationen für seine Installation and Konfigurierung. Sie enthält außerdem eine Demonstration der ConneXview-Industrie-Ethernet Diagnose-Software, ein neues Tool, das Ihnen erlaubt, Ihr Netzwerk zu überwachen, Fehler zu diagnostizieren und Stillstandzeiten zu reduzieren.



ConneXium

- > Installieren der ConneXium-Konfigurierungs-Software
- > Durchblättern des Inhaltsverzeichnisses dieser CD
- > Dokumentation
- > Sehen Sie sich ein Demo-Video an



ConneXview Industrie-Ethernet Diagnose-Software

- > Installieren Sie eine 21-Tage-Versuchsversion von ConneXview
- > Installieren des ConneXview Service Pack

[Deutsch]
[Espanol]
[English]
[Francais]

Copyright Schneider Electric 2009

Figure 5: Installing Java

- Start your Web browser.
- Check that you have activated JavaScript and Java in your browser settings.
- 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.

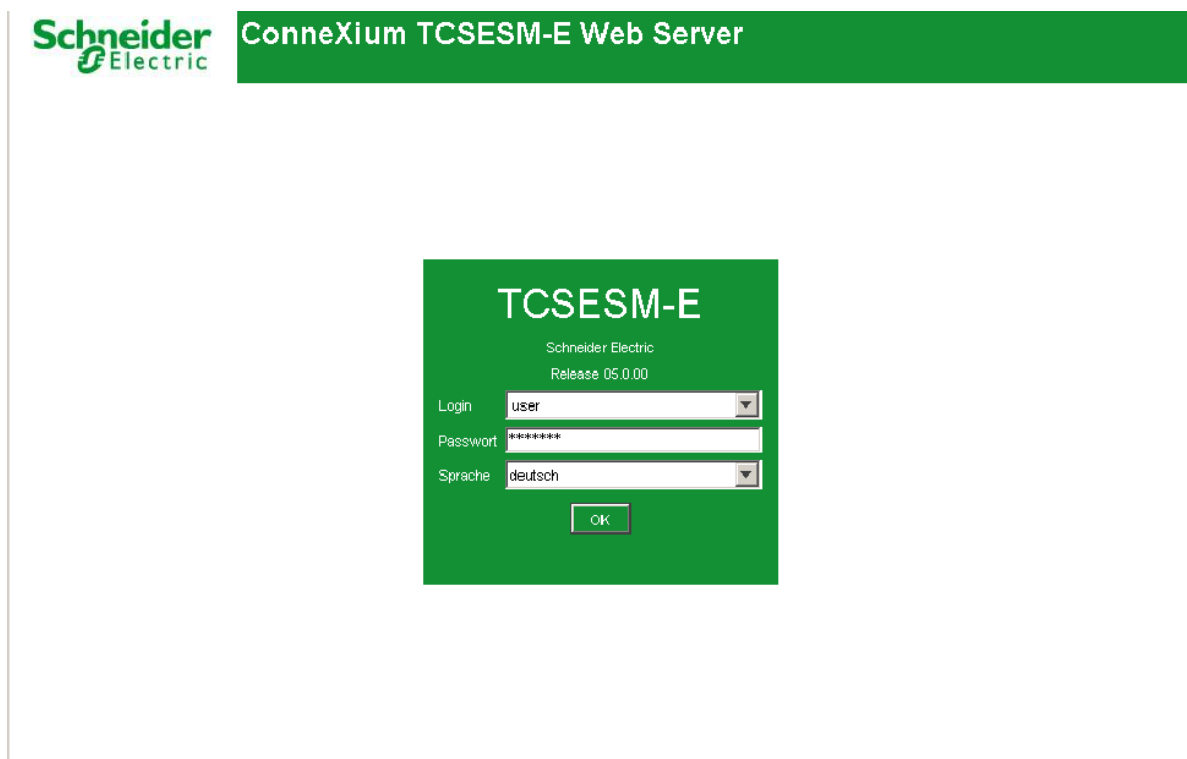


Figure 6: Login window

- 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: You can block your access to the device by entering an incorrect configuration.

Activating the function "Cancel configuration change" in the "Load/Save" dialog enables you to return automatically to the last configuration after a set time period has elapsed. This gives you back your access to the device.

2 Entering the IP Parameters

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

The device provides 7 options for entering the IP parameters during the first installation:

- ▶ Entry using the Command Line Interface (CLI).
You choose this “out of band” method if
 - ▶ you preconfigure your device outside its operating environment
 - ▶ you do not have network access (“in-band”) to the device
(see page 37 “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 40 “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 43 “Loading the system configuration from the EAM”).
- ▶ 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 45 “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 50 “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 53 “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

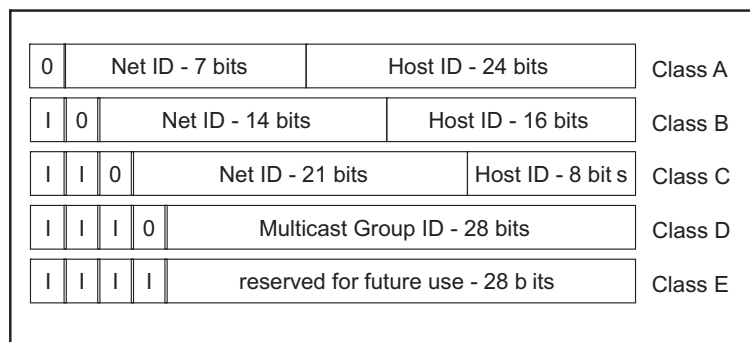


Figure 7: Bit representation of the IP address

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.

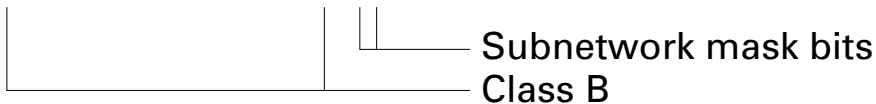
The division into subnetworks with the aid of the netmask is performed in much the same way as the division of the network addresses (net id) into classes A to C.

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:

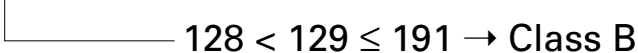
Decimal notation
255.255.192.0

Binary notation
11111111.11111111.11000000.00000000

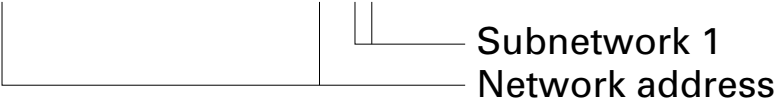


Example of IP addresses with subnetwork assignment when the above sub-
net mask is applied:

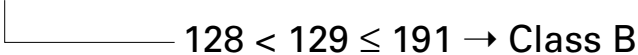
Decimal notation
129.218.65.17



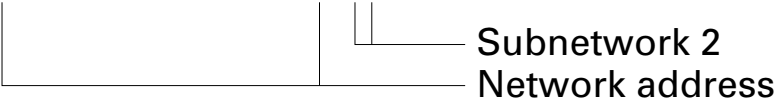
binary notation
10000001.11011010.01000001.00010001



Decimal notation
129.218.129.17



binary notation
10000001.11011010.10000001.00010001



■ 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?

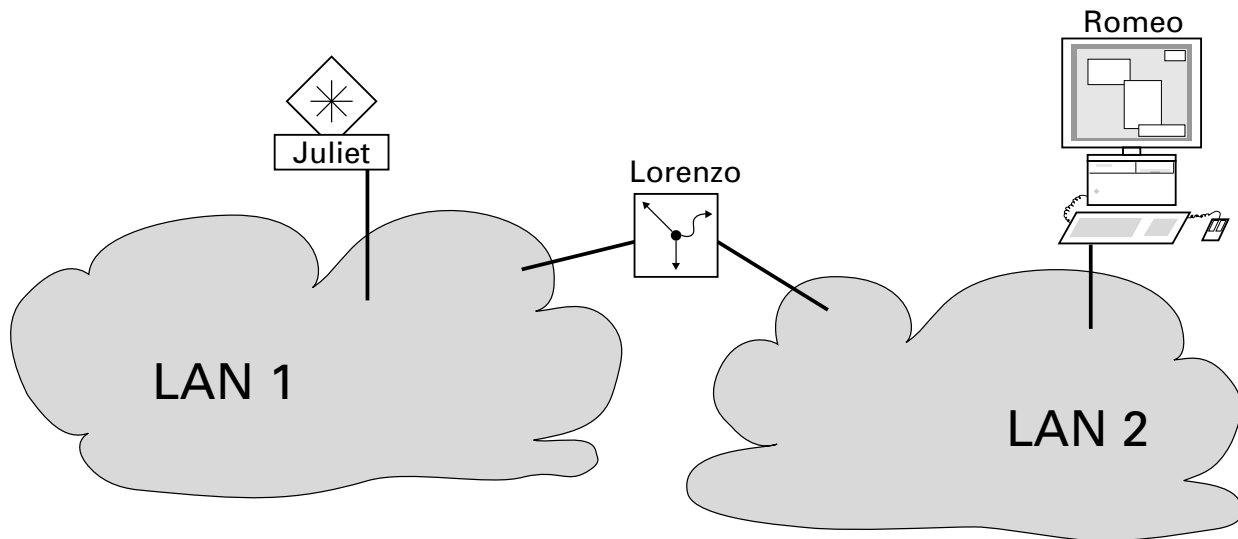


Figure 8: Management agent that is separated from its management station by a router

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 ISO/OSI layer model.

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

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

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

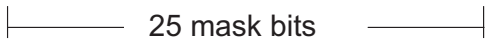

2.1.3 Classless Inter-Domain Routing

Class C with a maximum of 254 addresses was too small, and class B with a maximum of 65534 addresses was too large for most users, as they would never require so many addresses. This resulted in ineffective usage of the class B addresses available.

Class D contains reserved multicast addresses. Class E is reserved for experimental purposes. A gateway not participating in these experiments ignores datagrams with these destination addresses.

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

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

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

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

2.2 Entering IP parameters via CLI

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

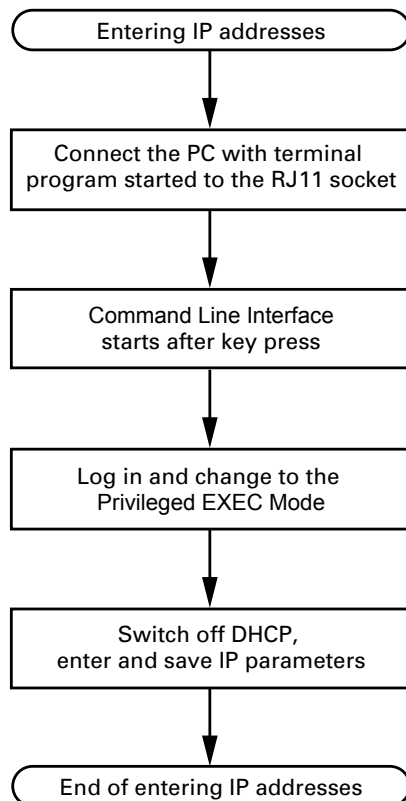


Figure 9: Flow chart for entering IP addresses

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

- Set up a connection to the device ([see on page 22 “Opening the Command Line Interface”](#)).

The start screen appears.

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

(Schneider Electric TCSESM-E) >

- 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 34 “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 Configu- rator 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 software on your PC. The software is on the CD supplied with the device.

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

Note: The installation of Ethernet Switch Configurator Software involves installing the WinPcap Version 3.1 software package.

If an earlier version of WinPcap is already installed on the PC, then follow the suggestion to uninstall it in the setup.

A newer version remains intact when you install Ethernet Switch Configurator Software. However, this cannot be guaranteed for all future versions of WinPcap. In the event that the installation of Ethernet Switch Configurator Software has overwritten a newer version of WinPcap, you uninstall WinPcap 3.1 and then re-install the new version.

- Start the Ethernet Switch Configurator Software program.

No	MAC Address	Writable	IP Address	Subnet Mask	Default Gateway	Product	Name
1	00:80:63:51:74:00	<input checked="" type="checkbox"/>	10.0.1.105	255.255.255.0	10.0.1.200		
2	00:80:63:1B:2F:CE	<input checked="" type="checkbox"/>	10.0.1.100	255.255.255.0	10.0.1.200		
3	00:80:63:1F:10:54	<input checked="" type="checkbox"/>	10.0.1.13	255.255.255.0	0.0.0.0		
4	00:80:63:57:4C:67	<input checked="" type="checkbox"/>	10.0.1.203	255.255.255.0	0.0.0.0		
5	00:80:63:70:E8:70	<input checked="" type="checkbox"/>	10.0.1.14	255.255.255.0	10.0.1.200		
6	00:80:63:0F:1D:B0	<input checked="" type="checkbox"/>	10.0.1.5	255.255.255.0	0.0.0.0		
7	00:80:63:74:02:5E	<input checked="" type="checkbox"/>	10.0.1.17	255.255.255.0	0.0.0.0		
8	00:80:63:51:7A:80	<input checked="" type="checkbox"/>	10.0.1.116	255.255.255.0	0.0.0.0		
9	00:80:63:51:82:80	<input checked="" type="checkbox"/>	10.0.1.112	255.255.255.0	0.0.0.0		
10	00:80:63:10:9A:D7	<input checked="" type="checkbox"/>	10.0.1.53	255.255.255.0	0.0.0.0		
11	00:80:63:17:2B:79	<input checked="" type="checkbox"/>	10.0.1.4	255.255.255.0	0.0.0.0		
12	00:80:63:FD:3B:A1	<input checked="" type="checkbox"/>	10.0.1.6	255.255.255.0	0.0.0.0		
13	00:80:63:4A:A7:B3	<input checked="" type="checkbox"/>	10.0.1.10	255.255.255.0	0.0.0.0		
14	00:80:63:2F:FB:B8	<input checked="" type="checkbox"/>	10.0.1.2	255.255.255.0	10.0.1.200		
15	00:80:63:74:67:C8	<input checked="" type="checkbox"/>	10.0.1.15	255.255.255.0	0.0.0.0		

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.

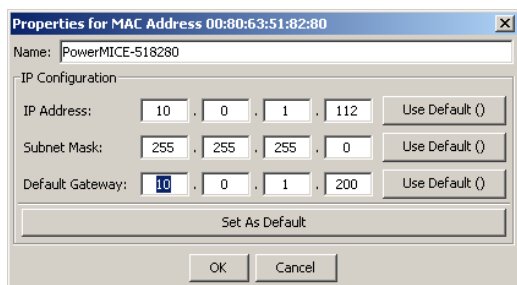


Figure 11: Ethernet Switch Configurator Software - assigning IP parameters

Note: When the IP address is entered, the device copies the local configuration settings (see on page 59 “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 55 “Web-based IP configuration”).

Note: Save the settings so that you will still have the entries after a restart (see on page 59 “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 in the EAM, see [“Saving locally \(and on the EAM\)”](#) on [page 65](#).

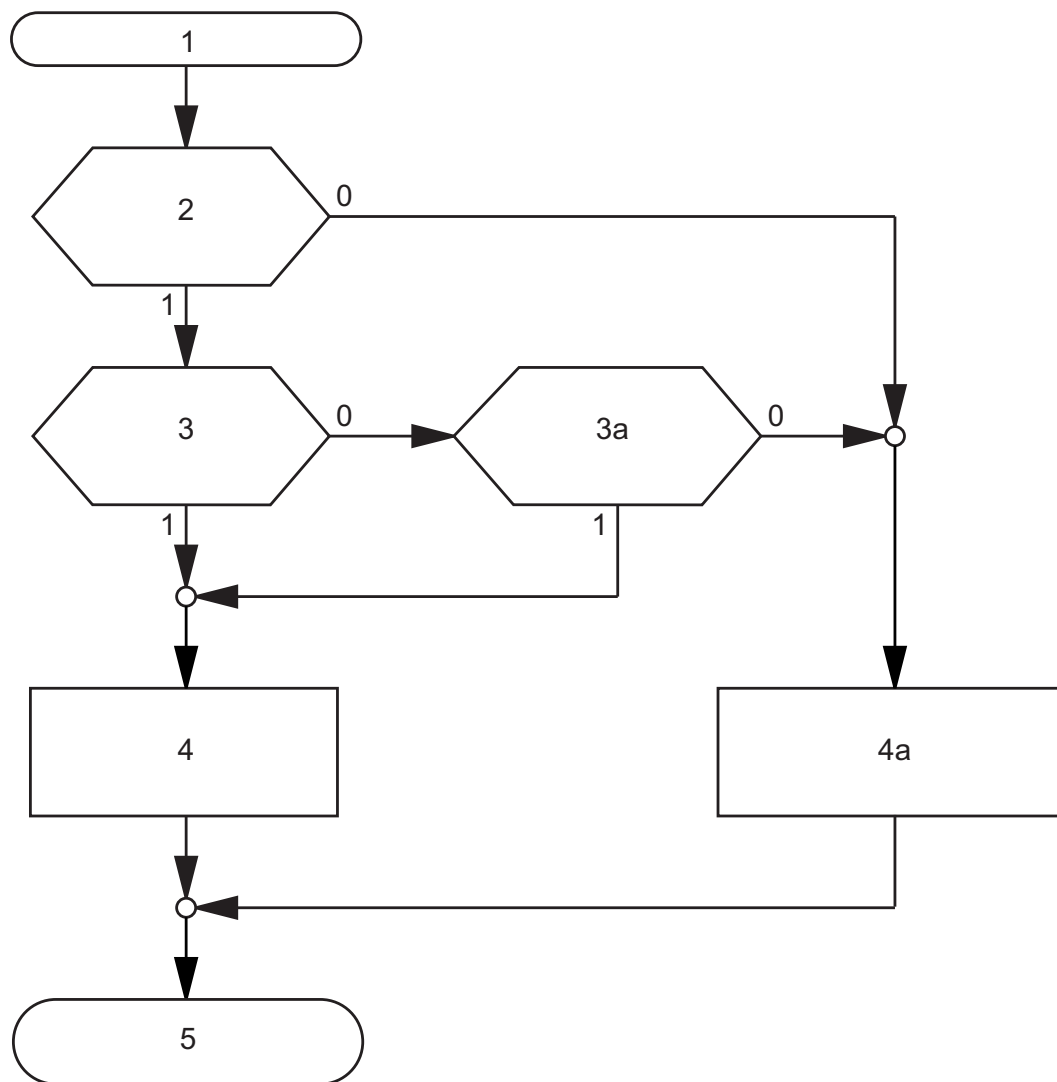


Figure 12: Flow chart of loading configuration data from the EAM

- 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 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 55 "Web-based IP configuration"](#)) or see in the CLI:

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

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

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

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

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

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

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

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

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

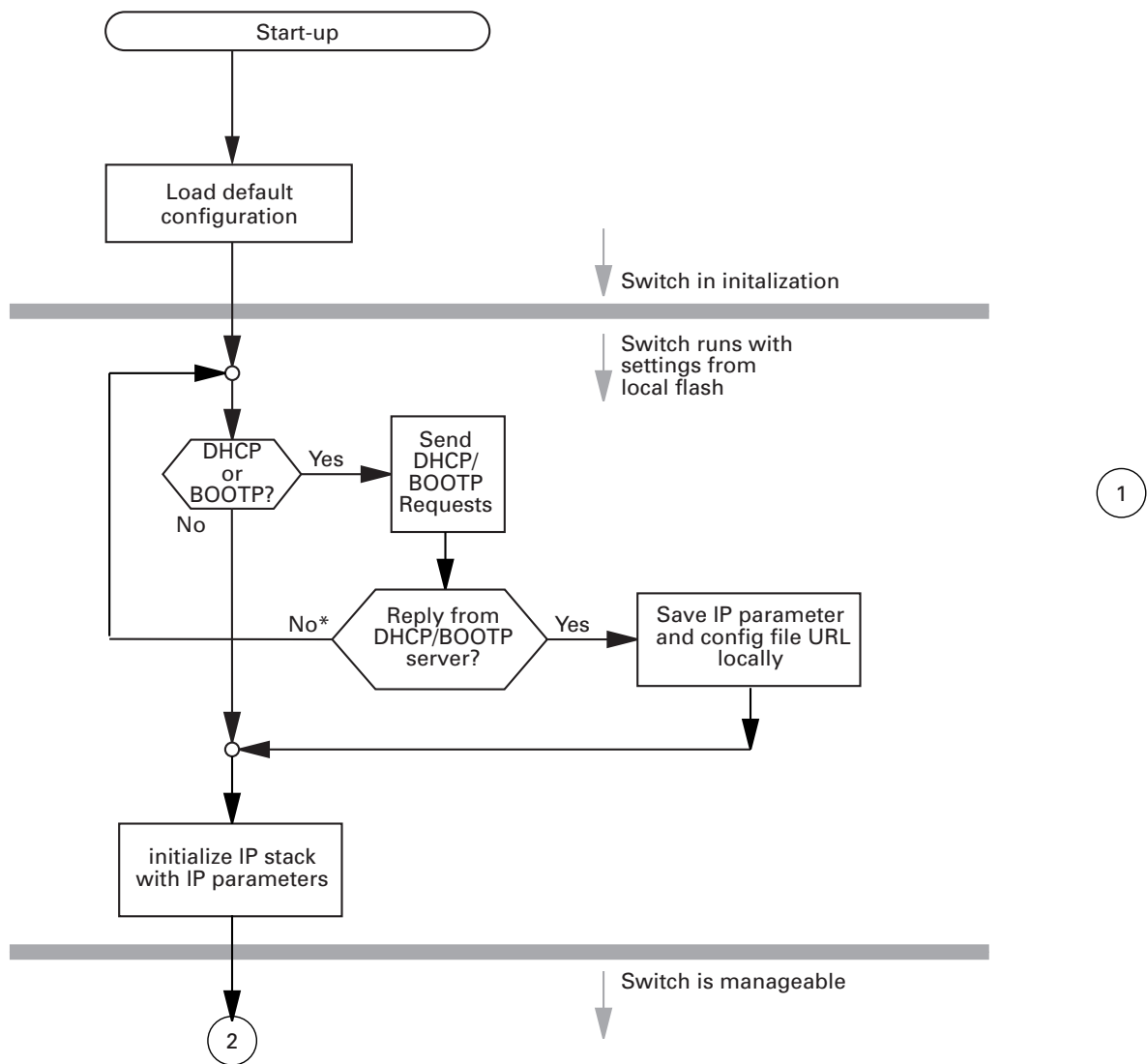


Figure 13: Flow chart for the BOOTP/DHCP process, part 1
 * see note [fig. 14](#)

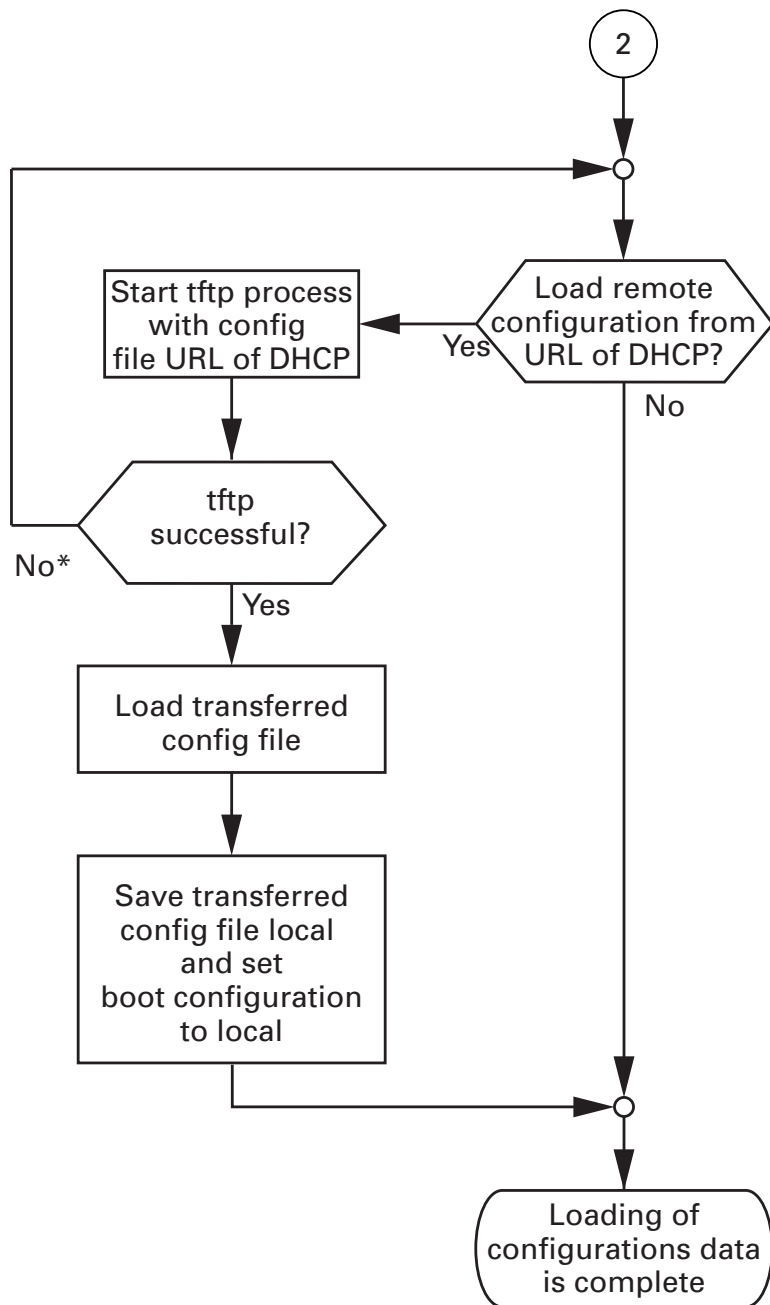


Figure 14: Flow chart for the BOOTP/DHCP process, part 2
 * see note

Note: The loading process started by DHCP/BOOTP ([see on page 45 “System configuration via BOOTP”](#)) shows the selection of "from URL & save locally" in the "Load" frame. If you get an error message when saving a configuration, this could be due to an active loading process. DHCP/BOOTP only finishes a loading process when a valid configuration has been loaded. If DHCP/BOOTP does not find a valid configuration, then finish the loading process by loading the local configuration in the "Load" frame.

2.6 System Configuration via DHCP

The DHCP (dynamic host configuration protocol) responds similarly to the BOOTP and additionally offers the configuration of a DHCP client via a name instead of via the MAC address.

For the DHCP, this name is known as the “client identifier” in accordance with rfc 2131.

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

During startup operation, a device receives its configuration data according to the “DHCP process” flowchart ([see fig. 13](#)).

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

In addition to the IP address, the DHCP server sends

- the tftp server name (if available),
- the name of the configuration file (if available).

The device accepts this data as configuration parameters ([see on page 55 “Web-based IP configuration”](#)).

If an IP address was assigned by a DHCP server, it will be permanently saved locally.

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

Table 3: DHCP options which the device requests

The special feature of DHCP in contrast to BOOTP is that the DHCP server can only provide the configuration parameters for a certain period of time (“lease”).

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

On delivery, DHCP is activated.

As long as DHCP is activated, the device attempts to obtain an IP address. If it cannot find a DHCP server after restarting, it will not have an IP address. To activate/deactivate DHCP ([see on page 55 “Web-based IP configuration”](#)).

Example of a DHCP configuration file:

```
# /etc/dhcpd.conf for DHCP Daemon
#
subnet 149.218.112.0 netmask 255.255.240.0 {
option subnet-mask 255.255.240.0;
option routers 149.218.112.96;
}
#
# Host berta requests IP configuration
# with her MAC address
#
```

```
host berta {
hardware ethernet 00:80:63:08:65:42;
fixed-address 149.218.112.82;
}
#
# Host hugo requests IP configuration
# with his client identifier.
#
host hugo {
#
option dhcp-client-identifier "hugo";
option dhcp-client-identifier 00:68:75:67:6f;
fixed-address 149.218.112.83;
server-name "149.218.112.11";
filename "/agent/config.dat";
}
```

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

The lines preceding the individually listed devices refer to settings that apply to all the following devices.

The fixed-address line assigns a permanent IP address to the device.

For further information, please refer to the DHCP server manual.

2.7 System Configuration via DHCP Option 82

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 classical DHCP protocol ([see on page 50 "System Configuration via DHCP"](#)) on the device being configured, Option 82 is based on the network topology. This procedure gives you the option of always assigning the same IP address to any device which is connected to a particular location (port of a device) on the LAN.

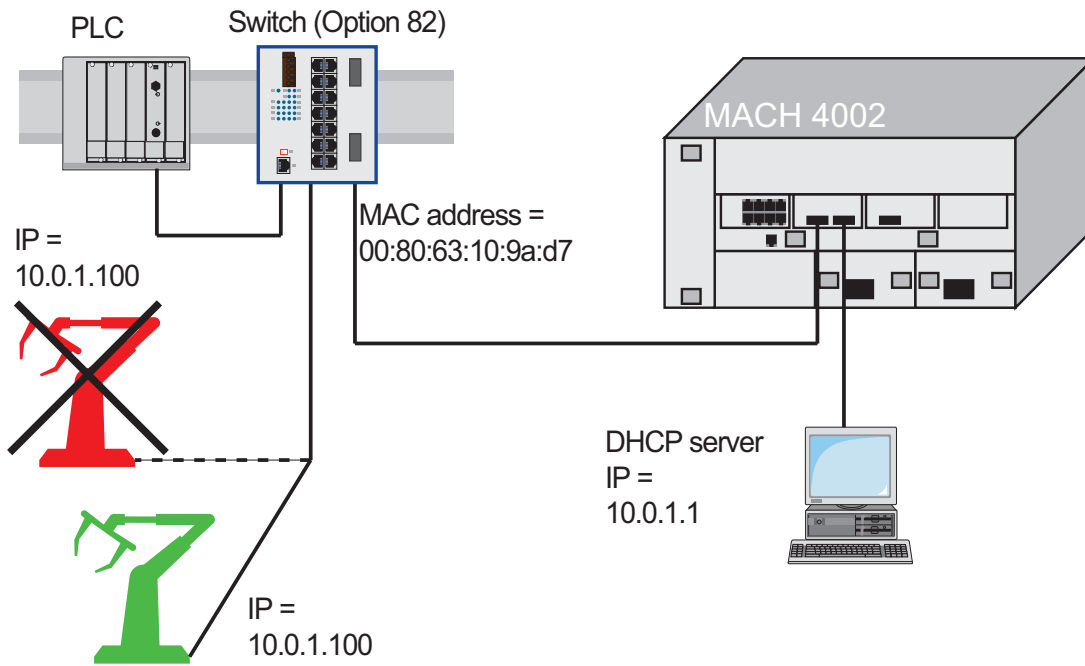


Figure 15: Application example of using Option 82

2.8 Web-based IP configuration

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

The screenshot shows a web-based configuration interface for network parameters. It features a sidebar on the left with a 'Mode' section containing three radio buttons: 'BOOTP', 'DHCP', and 'Local', with 'Local' selected. Below this is a 'VLAN' section with an 'ID' field containing the number '1'. The main content area is divided into several sections: 'BOOTP / DHCP' with a 'MAC Address' field containing '00:80:63:67:33:94'; 'DHCP' with a 'System Name' field containing 'TCSESM103F2LG0'; 'Local' with three fields: 'IP Address' (10.0.1.56), 'Netmask' (255.255.254.0), and 'Gateway address' (10.0.1.1); and 'Ethernet Switch Configurator Protocol' with an 'Operation' section containing 'On' and 'Off' radio buttons (with 'On' selected) and an 'Access' dropdown menu set to 'read-write'. At the bottom of the dialog are buttons for 'Set', 'Reload', and 'Help'.

Figure 16: Network parameters dialog

- Under "Mode", enter where the device is to obtain its IP parameters:
 - ▶ In the BOOTP mode, the configuration is via a BOOTP or DHCP server on the basis of the MAC address of the device.
 - ▶ 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.
- 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 assign an IP address to the device on the basis of its MAC address. Activate the Ethernet Switch Configurator Software protocol if you want to assign an IP address to the device from your PC with the enclosed Ethernet Switch Configurator Software software (setting on delivery: active).

Note: Save the settings so that you will still have the entries after a restart (see page 59 [“Loading/saving settings”](#)).

2.9 Faulty device replacement

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

- ▶ Configuring the new device via an Memory Backup Adapter ([see on page 43 “Loading the system configuration from the EAM”](#)) 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.

Note: If you replace a device with DIP switches, use identical switch settings on the replacement device.

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 load/save symbol in the menu area changes from a disk symbol into a yellow triangle. After saving the configuration, the load/save symbol changes back into the disk symbol.

3.1 Loading settings

When it is restarted, the device loads its configuration data from the local non-volatile memory, if you have deactivated BOOTP/DHCP and if 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
- ▶ the Memory Backup Adapter. If an EAM is connected to the device, the device always loads its configuration from the EAM.
- ▶ a file in the connected network¹
- ▶ the firmware (restoring the configuration in the state of 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: When loading a configuration, all ports are turned off while applying the new configuration. Afterwards, the switch sets the port's state according to the new configuration.

1. This source is the default in the state of delivery

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 an EAM is connected to the device, the device always loads its configuration from the EAM.

The chapter [“Saving locally \(and on the EAM\)”](#) dialog on [page 65](#) 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 66 "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.

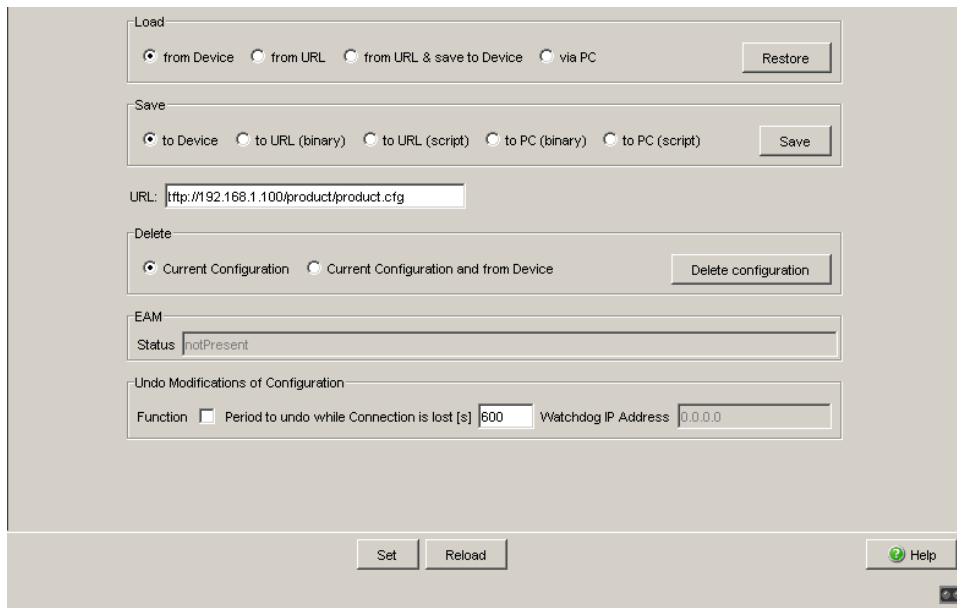


Figure 17: Load/Save dialog

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

3.1.4 Resetting the configuration to the state on delivery

The device enables you to

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

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

Setting in the system monitor:

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

3.2 Saving settings

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

- ▶ save the current configuration on the device
- ▶ save the current configuration in binary form in a file under the specified URL, or as an editable and readable script
- ▶ save the current configuration in binary form or as an editable and readable script 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 in the EAM.

- Select the `Basics: Load/Save` dialog.
- In the "Save" frame, click "to Device".
- Click "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 in the EAM.

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

3.2.3 Saving as a script on the PC

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

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

4 Loading software updates

■ Checking the software release installed

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

■ Loading the software


The device gives you two options for loading the software:

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

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

4.1 Loading the software from the tftp server

For a tftp update, you need a tftp server on which the software to be loaded is stored ([see on page 224 “TFTP Server for Software Updates”](#)).

 Select the `Basics:Software` dialog.

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

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

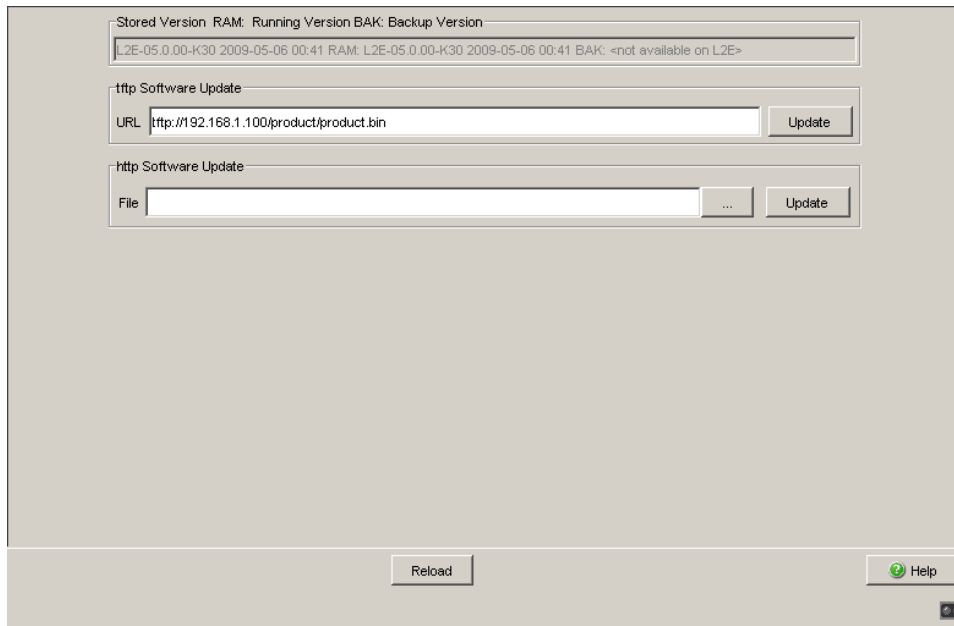


Figure 18: Software update dialog

- 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 update via a file selection window, the device software needs to be accessible from your PC.

- Select the `Basics:Software` dialog.
- In the file selection frame, click "...".
- In the file selection window, select the device software (`device.bin`) and click "Open".
- Click "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 misspelled or file does not exist).
 - ▶ Connection error (reason: incorrect file path).
- After successfully loading it, you activate the new software:
Select the `Basic Settings:Restart` dialog and perform a cold start.
In a cold start, the device reloads the software from the non-volatile memory, restarts, and performs a self-test.
 - In your browser, click "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 protect against unauthorized access.

- ▶ Password for SNMP access,
- ▶ Telnet/Web access may be enabled or disabled,
- ▶ Ethernet Switch Configurator Software function may be enabled or disabled,
- ▶ Port access control via IP or MAC address.

6.1 Password for SNMP access

6.1.1 Description of password for SNMP access

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

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

The device receives the SNMP packet and compares the IP address of the sending computer and the password with the entries in the device MIB. 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.

6.1.2 Entering the password for SNMP access

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

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

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

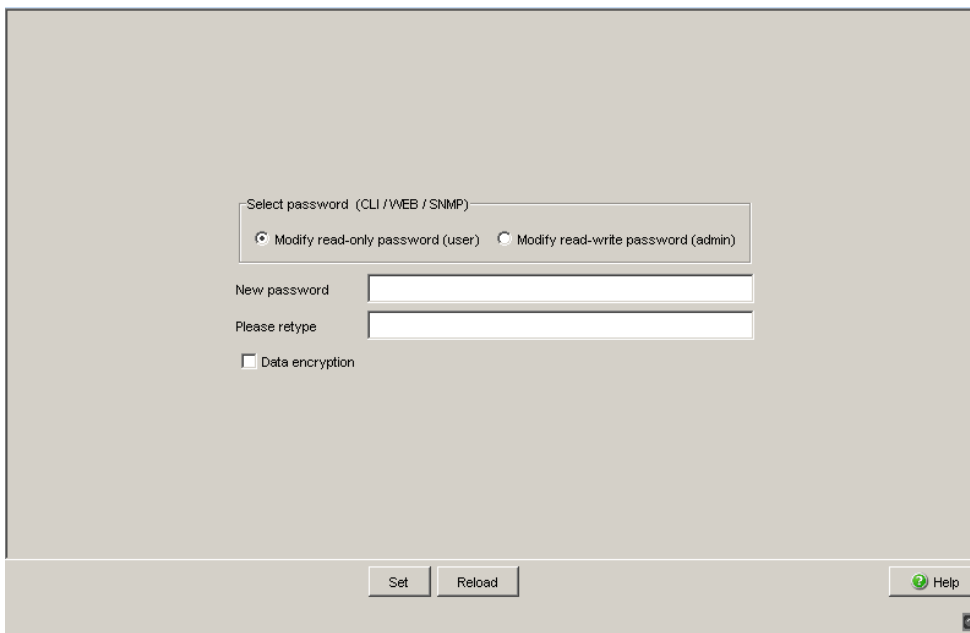


Figure 19: Password dialog

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

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

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

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

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

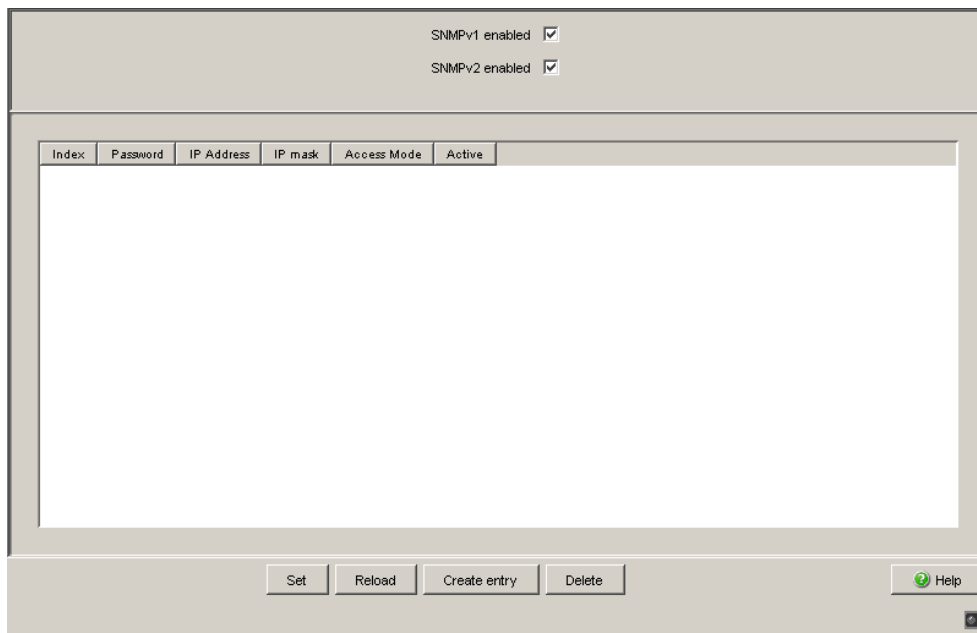


Figure 20: SNMPv1/v2 access dialog

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

6.2 Telnet/Web access

6.2.1 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.

6.2.2 Enabling/disabling Telnet/Web access

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

```
enable
configure
lineconfig
transport input telnet
no transport input telnet
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.
Enable Telnet server.
Disable Telnet server.
Switch to the Configuration mode.
Enable Web server.
Disable Web server.

6.3 Ethernet Switch Configurator Software settings

6.3.1 Description of the Ethernet Switch Configurator Software protocol

The Ethernet Switch Configurator Software protocol allows you to assign the device an IP address based on its MAC address ([see on page 40 “Entering the IP Parameters via Ethernet Switch Configurator Software”](#)). 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.

6.3.2 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	Switch to the Privileged EXEC mode.
network protocol ethernet-switch-conf off	Disable the Ethernet Switch Configurator Software function.
network protocol ethernet-switch-conf read-only	Enable the Ethernet Switch Configurator Software function with "read-only" access
network protocol ethernet-switch-conf read-write	Enable the Ethernet Switch Configurator Software function with "read-write" access

6.4 Port access control

6.4.1 Description of the port access control

You can configure the device to help protect every port from unauthorized access. Depending on your selection, the device checks the MAC address or the IP address of the connected device.

The following functions are available for monitoring every individual port:

- ▶ Who has access to this port?
The device recognizes 2 classes of access control:
 - ▶ All:
 - no access restriction.
 - MAC address 00:00:00:00:00:00 or
 - IP address 0.0.0.0.
 - ▶ Devices with defined MAC or IP addresses:
 - exclusively devices with defined MAC or IP addresses have access.
 - you can define up to 10 IP or 10 MAC addresses or maskable MAC addresses.

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

6.4.2 Application example for port access control

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

The following is known:

Parameter	Value	Explanation
Allowed IP Addresses	10.0.1.228 10.0.1.229	The defined users are the device with the IP address 10.0.1.228 and the device with the IP address 10.0.1.229
Action	portDisable	Disable the port with the corresponding entry in the port configuration table (see on page 73 “Configuring the ports”) and send an alarm

Prerequisites for further configuration:

- ▶ The port for the LAN connection is enabled and configured correctly ([see on page 73 “Configuring the ports”](#))
- ▶ Prerequisites for the device to be able to send an alarm (trap) ([see on page 153 “Configuring traps”](#)):
 - You have entered at least one recipient
 - You have set the flag in the “Active” column for at least one recipient
 - In the “Selection” frame, you have selected “Port Security”

Configure the port security.

Select the `Security:Port Security` dialog.

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

In the table, click on the row of the port to be protected, in the “Allowed IP addresses” cell.

Enter in sequence:

- the IP subnetwork group: 10.0.1.228
- a space character as a separator
- the IP address: 10.0.1.229

Entry: 10.0.1.228 10.0.1.229

In the table, click on the row of the port to be protected, in the “Action” cell, and select `portDisable`.

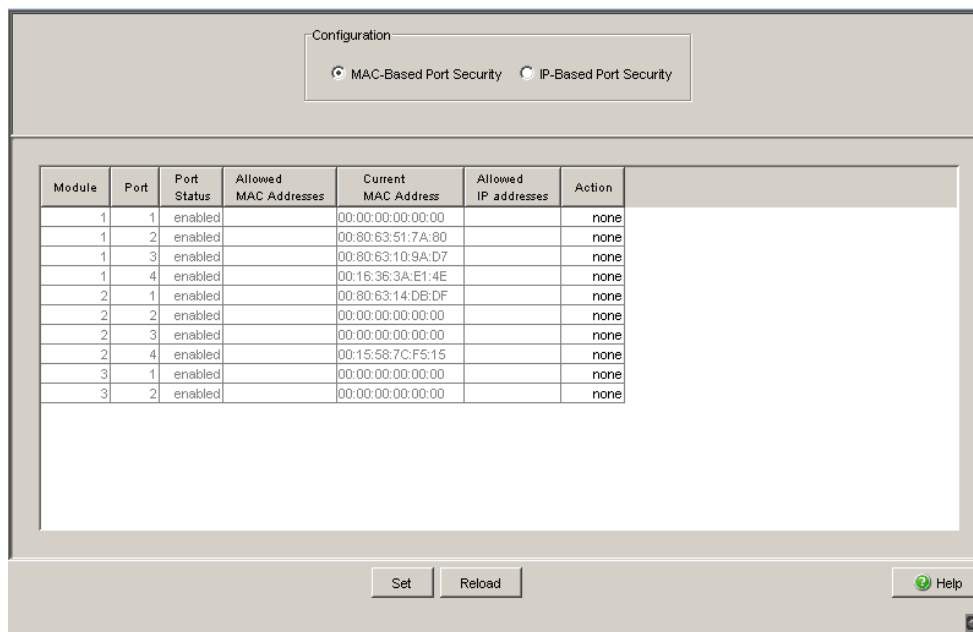


Figure 21: Port Security dialog

Save the settings in the non-volatile memory.

Select the dialog

Basic Settings:Load/Save.

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

7 Synchronizing the System Time in the Network

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

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

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

Examples of application areas include:

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

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

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

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 92 “Configuring SNTP”](#)).

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

- Select the `Time` dialog.

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

- ▶ The “IEEE 1588 time” displays the time determined using PTP. The “SNTP time” displays the time with reference to Universal Time Coordinated (UTC). The display is the same worldwide. Local time differences are not taken into account.
- ▶ The “System time” uses the “IEEE 1588 / SNTP time”, allowing for the local time difference from “IEEE 1588 / SNTP time”.
“System time” = “IEEE 1588 / SNTP time” + “Local offset”.
- ▶ “Time source” displays the source of the following time data. The device automatically selects the source with the greatest accuracy.
- With “Set time from PC”, the device takes the PC time as the system time and calculates the IEEE 1588 / SNTP time using the local time difference.
“IEEE 1588 / SNTP time” = “System time” - “Local offset”
- The “Local Offset” is for displaying/entering the time difference between the local time and the “IEEE 1588 / SNTP time”.

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

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

7.2 SNTP

7.2.1 Description of SNTP

The Simple Network Time Protocol (SNTP) enables you to synchronize the system time in your network.

The device supports the SNTP Server and SNTP Client functions.

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

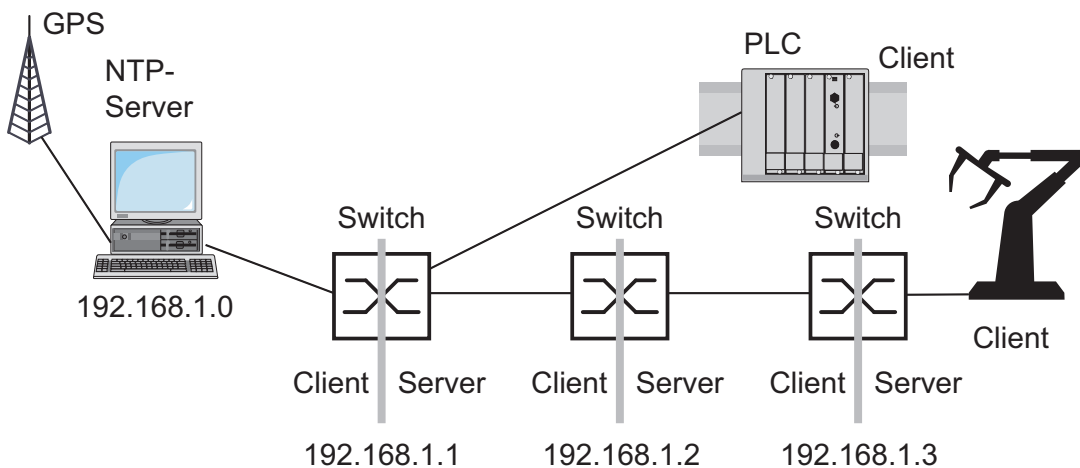


Figure 22: SNTP cascade

7.2.2 Preparing the SNTP coordination

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

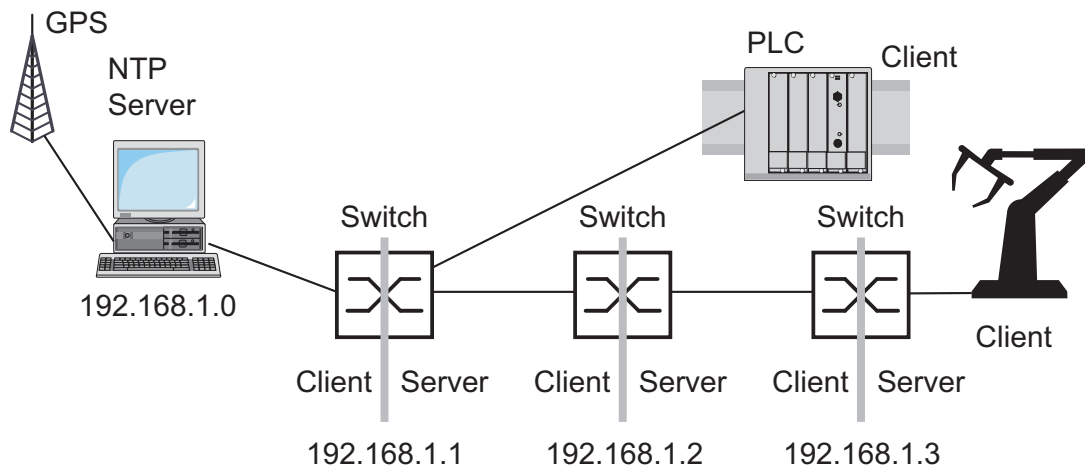


Figure 23: Example of SNTP cascade

- Enable the SNTP function on all devices whose time you want to set using SNTP.
The SNTP server of the device responds to Unicast requests as soon as it is enabled.
- If no reference clock is available, specify a device as the reference clock and set its system time as accurately as possible.

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

7.2.3 Configuring SNTP

- Select the `Time : SNTP` dialog.
- ▶ Configuration SNTP Client and Server
 - In this frame you switch the SNTP function on/off. When it is switched off, the SNTP server does not send any SNTP packets or respond to any SNTP requests. The SNTP client does not send any SNTP requests or evaluate any SNTP Broadcast/Multicast packets.
- ▶ SNTP Status
 - The “Status message” displays conditions such as “Server 1 is not responding”.
- ▶ Configuration SNTP Server
 - In “Anycast destination address” you enter the IP address to which the SNTP server on the device sends the SNTP packets.
 - In “VLAN ID” you specify the VLAN to which the device may periodically send SNTP packages.
 - In “Anycast send interval” you specify the interval at which the device sends SNTP packets (valid entries: 1 second to 3600 seconds, on delivery: 120 seconds).
 - With “Disable Server at local time source” the device disables the SNTP server function if the status of the time source is “local” (see Time dialog).

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

Table 4: Periodic sending of SNTP packets

► Configuration SNTP Client

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

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

- In “Server request interval” you specify the interval at which the device requests SNTP packets (valid entries: 1 second to 3,600 seconds, on delivery: 30 seconds).
- With “Accept SNTP Broadcasts” the device takes the system time from SNTP Broadcast/Multicast packets that it receives.

The screenshot shows the SNTP configuration dialog box with the following settings:

- Configuration SNTP Client And Server:** Operation is set to **On**.
- Configuration SNTP Server:**
 - Anycast destination address: 0.0.0.0
 - VLAN ID: 1
 - Anycast send interval [s]: 120
 - Disable Server at local time source:
- 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:

Buttons at the bottom: Set, Reload, Help.

Figure 24: SNTP dialog

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

Table 5: Settings for the example (see fig. 23)

7.3 Precision Time Protocol

7.3.1 Description of PTP functions

Precise time management is required for running time-critical applications via a LAN.

The IEEE 1588 standard with the Precision Time Protocol (PTP) describes a procedure that 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.

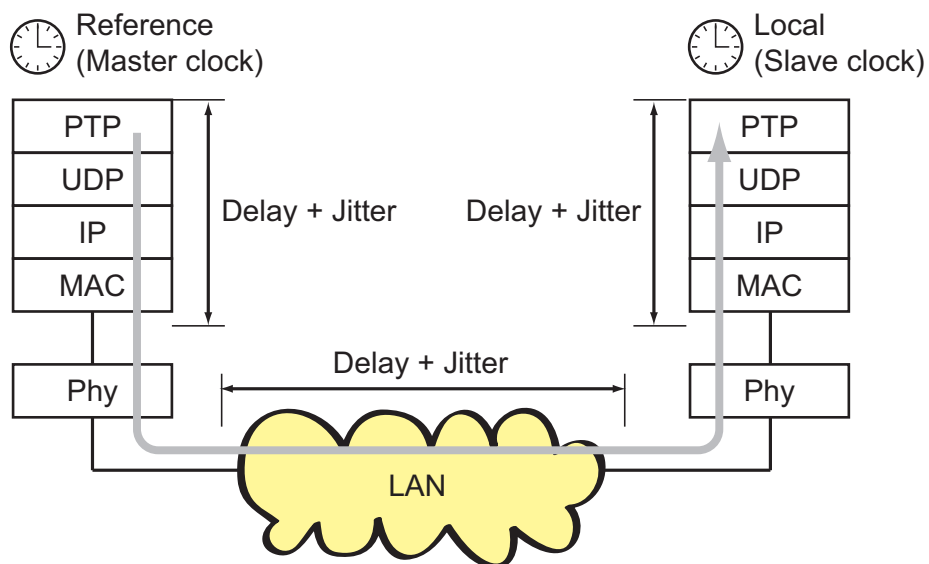
Factors influencing precision are:

- ▶ 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		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 25: 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
- ▶ Rate limiter
- ▶ Prioritization - QoS
- ▶ Flow control
- ▶ Virtual LANs (VLANs)

8.1 Direct packet distribution

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

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

8.1.1 Store-and-forward

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

8.1.2 Multi-address capability

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

- ▶ unknown 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 102 “Entering static address entries”](#)).

The device can learn up to 8.000 addresses. This is necessary if more than one terminal device is connected to one or more ports. It is thus possible to connect several independent subnetworks to the device.

8.1.3 Aging of learned addresses

The device monitors the age of the learned addresses. Address entries which exceed a certain age (30 seconds, aging time), are deleted by the device from its address table.

The device sends data packets with unknown destination addresses out all its ports.

The device directly distributes data packets with a known destination address.

Note: A reboot deletes the learned address entries.

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

8.1.4 Entering static address entries

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

The following are valid filter criteria:

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

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

- ▶ The management administrator describes the static part of the filter table (`dot1qStaticTable`).
- ▶ During operation, the device is capable of learning which of its ports receive data packets from which source address ([see on page 100 “Multi-address capability”](#)). This information is written to a dynamic part (`dot1qTpFdbTable`).
- ▶ Addresses learned dynamically from neighboring agents and those learned via GMRP are written to the other dynamic part.

Addresses already located in the static filter table are automatically transferred to the dynamic part by the device.

An address entered statically cannot be overwritten through learning.

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

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

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

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

- ▶ `learned`: the filter was created automatically by the device.
- ▶ `invalid`: with this status you delete a manually created filter.
- ▶ `permanent`: the filter is stored permanently in the device or on the URL (see on page 65 "Saving settings").
- ▶ `gmrp`: the filter was created by GMRP.
- ▶ `gmrp/permanent`: GMRP added further port markings to the filter after it was created by the administrator. The port markings added by the GMRP are deleted by a restart.
- ▶ `igmp`: the filter was created by IGMP.

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

8.1.5 Disabling the direct packet distribution

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

Select the `Switching:Global` dialog.

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 three distribution classes on the basis of the addressed recipients:

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

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

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

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

8.2.2 Example of a Multicast application

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

To prevent the video data from putting a load on the entire network, the device uses the GMRP to distribute the Multicast address information. As a result, the image data with a Multicast address is only distributed to those ports that are connected to the associated monitors for surveillance.

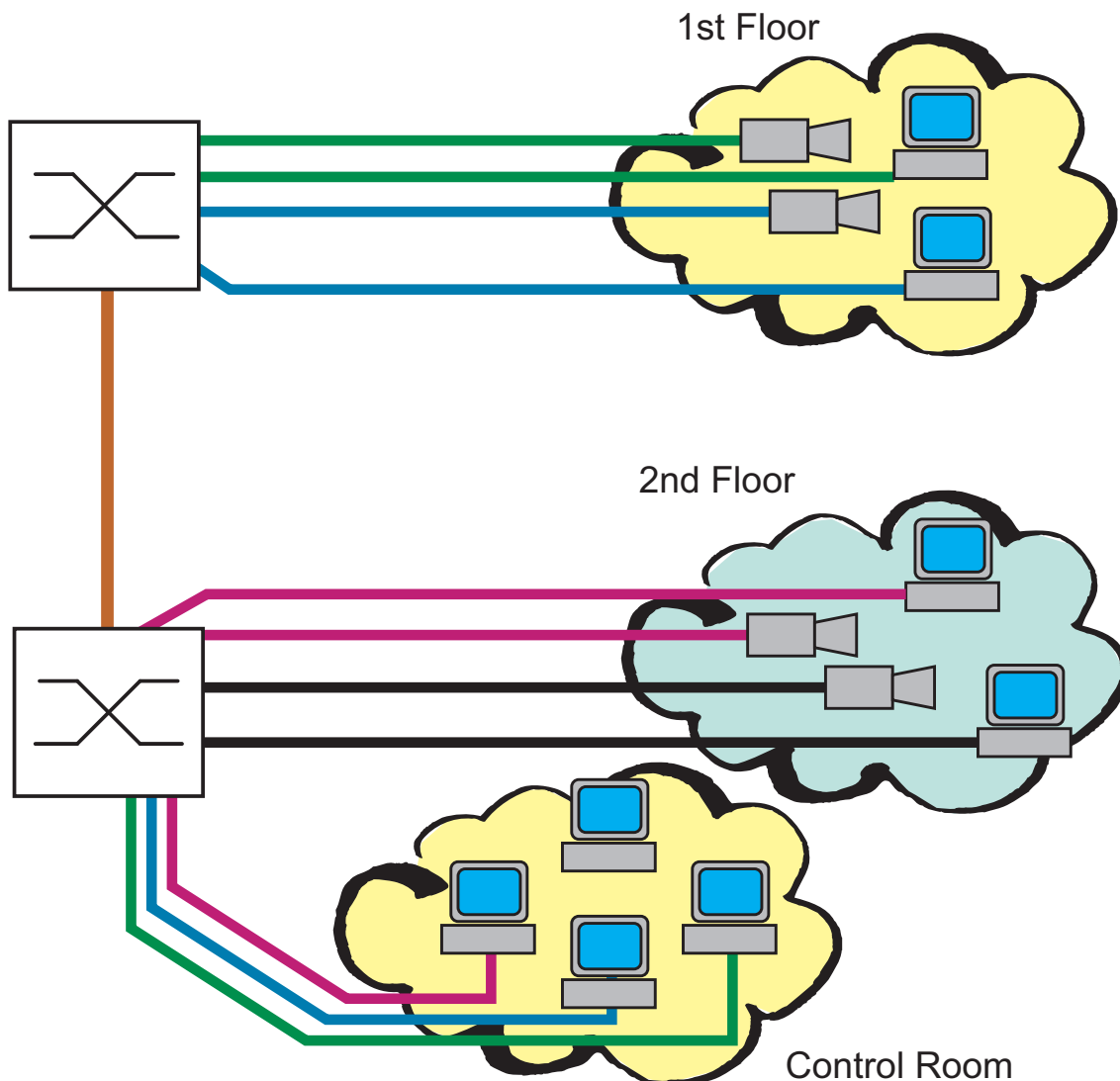


Figure 26: Example: Video surveillance in machine rooms

8.2.3 Description of IGMP Snooping

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

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

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

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

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

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

8.2.4 Description of GMRP

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

Devices that want to receive data packets with a Multicast address use GMRP to perform the registration of the Multicast address. For a Switch, registration involves entering the Multicast address in the filter table. When a Multicast address is entered in the filter table, the Switch sends this information in a GMRP packet to all the ports. Thus the connected Switches know that they have to forward this Multicast address to this Switch. The GMRP enables packets with a Multicast address in the destination address field to be sent to the ports entered. The other ports are not affected by these packets.

Data packets with unregistered Multicast addresses are sent to all ports by the Switch.

Default setting: "Global setting": disabled

8.2.5 Setting up the Multicast application

- Select the `Switching:Multicasts` dialog.

■ Global Configuration

"IGMP Snooping" allows you to enable IGMP Snooping globally for the entire device.

If IGMP Snooping is disabled, then

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

"GMRP" allows you to enable GMRP globally for the entire device.

If GMRP is disabled, then

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

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

"inactive" disables GMRP and IGMP Snooping.

■ IGMP Querier and IGMP settings

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

Prerequisite: In the `Switching:Multicasts:Global Configuration` dialog, the `IGMP Snooping mode` is selected.

IGMP Querier

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

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

In “Transmit Interval” you specify the interval at which the device sends query packets (valid entries: 2-3599 s, default setting: 125 s).

Note the connection between the parameters Max. Response Time, Send Interval and Group Membership Interval ([see on page 111 “Parameter values”](#)).

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

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

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

IGMP Settings

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

In “Max. Response Time” you specify the period within which the Multicast group members respond to a query (valid values: 1-3598 s, default setting: 10 s).

Note the connection between the parameters Max. Response Time, Send Interval and Group Membership Interval ([see on page 111 “Parameter values”](#)).

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

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

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

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 111 “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	1-25 seconds	10 seconds
	3	1-3.598 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

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

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

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

■ Known Multicasts

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

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

■ Settings per port (table)

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

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

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

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

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

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



- ▶ **GMRP per Port**

This table column enables you to enable/disable the GMRP for each port when the global GMRP is enabled. When you disable the GMRP at a port, no registrations can be made for this port, and GMRP packets cannot be sent out of this port.

- ▶ **GMRP Service Requirements**

Devices that do not support GMRP can be integrated into the Multicast addressing by means of

- ▶ a static filter address entry on the connecting port
- ▶ selecting "Forward all groups" in the table column "GMRP Service Requirement". The device enters ports with the selection "Forward all groups" in all Multicast filter entries learned via GMRP.

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

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

or

- ▶ enabling GMRP on the ring ports globally, and
- ▶ enabling "Forward all groups" on the ring ports.

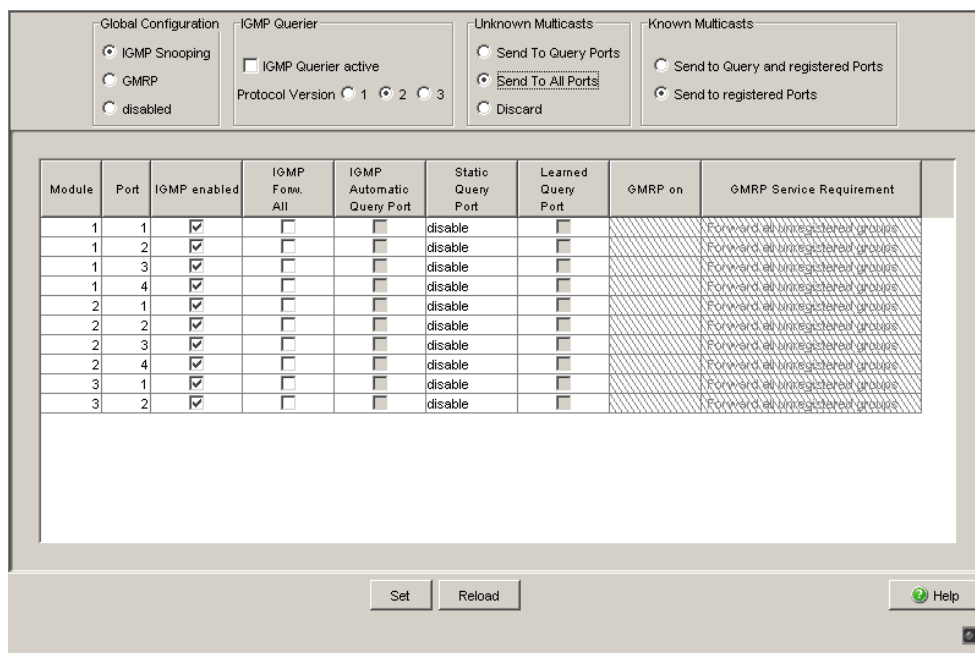


Figure 27: Multicasts dialog

8.3 Rate Limiter

8.3.1 Description of the Rate Limiter

The device can limit the rate of message traffic during periods of heavy traffic flow.

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

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

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

8.3.2 Rate Limiter settings

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

Setting options per port:

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

Module	Port	Ingress Packet Types	Ingress Limiter Rate (kbit/s)	Egress Limit (Pkt/s) Packet Type: BC	Egress Limit (kbit/s) Packet Type: all
1	1	BC	0	0	0
1	2	BC	0	0	0
1	3	BC	0	0	0
1	4	BC	0	0	0
1	5	BC	0	0	0
1	6	BC	0	0	0
1	7	BC	0	0	0
1	8	BC	0	0	0
1	9	BC	0	0	0
1	10	BC	0	0	0
1	11	BC	0	0	0
1	12	BC	0	0	0
1	13	BC	0	0	0
1	14	BC	0	0	0
1	15	BC	0	0	0

Figure 28: Rate Limiter

8.4 QoS/Priority

8.4.1 Description of Prioritization

This function prevents time-critical data traffic such as language/video or real-time data from being disrupted by less time-critical data traffic during periods of heavy traffic. By assigning high traffic classes for time-critical data and low traffic classes for less time-critical data, 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 73 "Configuring the ports"](#)) and when the port was configured to "trust dot1p".
Default setting: "trust dot1p".

Data packets can contain prioritizing/QoS information:

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

8.4.2 VLAN tagging

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

For data packets with a VLAN tag, the device evaluates

- ▶ the priority information, and
- ▶ the VLAN information if VLANs have been set up.

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

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

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

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

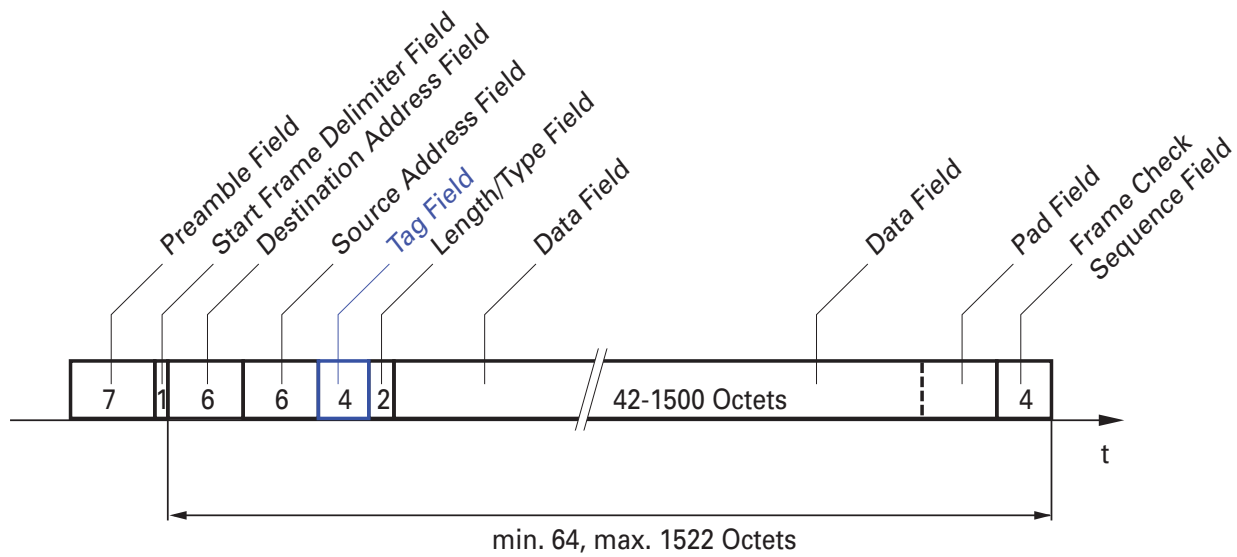


Figure 29: Ethernet data packet with tag

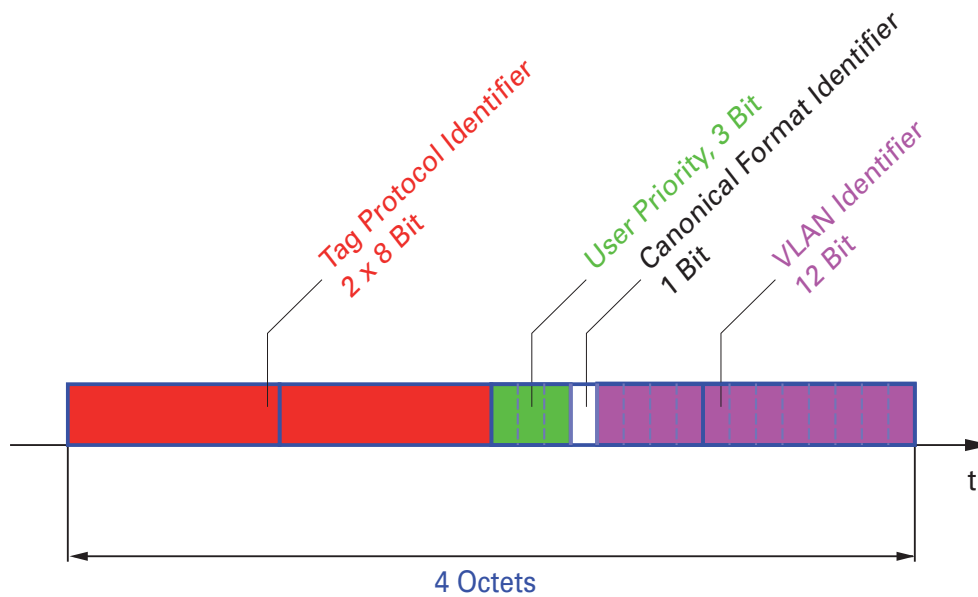


Figure 30: Tag format

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

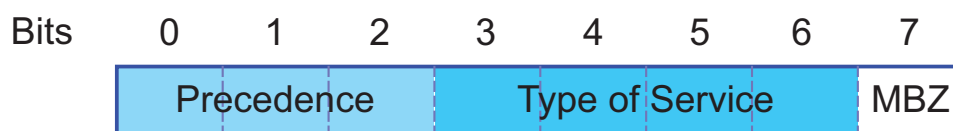
- The additional 4-byte VLAN tag enlarges the data packets. With small data packets, this leads to a larger bandwidth load.

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

8.4.3 IP ToS / DiffServ

■ TYPE of Service

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



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

Table 9: ToS field in the IP header

■ Differentiated Services

The newly defined Differentiated Services field in the IP header in RFC 2474 (see fig. 31) - often known as the DiffServ Code Point or DSCP, replaces the ToS field and is used to mark the individual packets with a DSCP. Here the packets are divided into different quality classes. The first three bits of the DSCP are used to divide the packets into classes. The next three bits are used to further divide the classes on the basis of different criteria. In contrast to the ToS byte, DiffServ uses six bits for the division into classes. This results in up to 64 different service classes.

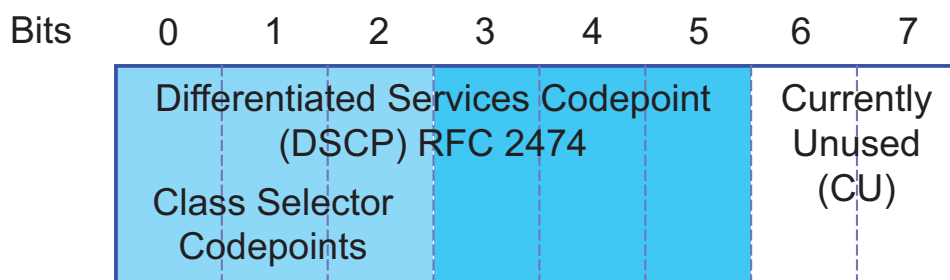


Figure 31: Differentiated Services field in the IP header

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

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

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

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

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

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

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

Table 11: Mapping the DSCP values onto the traffic classes

8.4.4 Management prioritization

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

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

8.4.5 Handling of received priority information

The device provides 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 119 “VLAN tagging”](#)). You can modify this assignment. The device assigns the port priority to packets that it receives without a tag.
- ▶ **untrusted**
The device ignores the priority information in the packet and always assigns the packets the port priority of the receiving port.
- ▶ **trust ip-dscp**
The device assigns the IP packets to the different traffic classes according to the DSCP value in the IP header, even if the packet was also VLAN-tagged. The assignment is based on the pre-defined values. You can modify this assignment.
The device prioritizes non-IP packets according to the port priority.

8.4.6 Handling of traffic classes

For the handling of traffic classes, the device provides:

- ▶ **Strict Priority**

■ Description of Strict Priority

With the Strict Priority setting, the device first transmits all data packets with a higher traffic class before transmitting any data packet with the next lower traffic class. The device transmits a data packet with the lowest traffic class only when no other data packets with a higher traffic class are in the queue. In some cases, a high amount of high class data traffic may result in so-called starvation (packets of lower traffic classes will not be sent).

In time- or latency-critical applications, such as VoIP or video, this method results in the immediate sending of high-priority data.

8.4.7 Setting prioritization

■ Assigning the port priority

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

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

```
enable
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-map-
ping 0 2
classofservice dot1p-map-
ping 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
configure
classofservice ip-dscp-map-
ping cs1 1
```

Switch to the Privileged EXEC mode.

Switch to the Configuration mode.

Assign traffic class 1 to DSCP CS1.

```
show classofservice ip-dscp-mapping
```

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

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

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

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

■ Configuring Layer 2 management priority

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

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

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


```

exit                               Switch to the privileged EXEC mode.
show network                       Displays the management VLAN priority.

```

```

System IP Address..... 10.0.1.116
Subnet Mask..... 255.255.255.0
Default Gateway..... 10.0.1.200
Burned In MAC Address..... 00:80:63:51:7A:80
Network Configuration Protocol (BootP/DHCP).... None
DHCP Client ID (same as SNMP System Name)..... "TCSESM-518280"
Ethernet Switch Configurator Protocol ..... Read-Write
Management VLAN ID..... 1
Management VLAN Priority..... 7
Management IP-DSCP Value..... 0 (be/cs0)
Web Mode..... Enable
JavaScript Mode..... Enable

```

■ Configuring Layer 3 management priority

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

```

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

exit                               Switch to the privileged EXEC mode.
show network                       Displays the management VLAN priority.

```

```

System IP Address..... 10.0.1.116
Subnet Mask..... 255.255.255.0
Default Gateway..... 10.0.1.200
Burned In MAC Address..... 00:80:63:51:7A:80
Network Configuration Protocol (BootP/DHCP).... None
DHCP Client ID (same as SNMP System Name)..... "TCSESM-518280"
Ethernet Switch Configurator Protocol ..... Read-Write
Management VLAN ID..... 1
Management VLAN Priority..... 7
Management IP-DSCP Value..... 56 (cs7)
Web Mode..... Enable
JavaScript Mode..... Enable

```

8.5 Flow control

8.5.1 Description of flow control

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

The example ([see fig. 32](#)) shows a graphic illustration of how the flow control works. Workstations 1, 2 and 3 want to simultaneously transmit a large amount of data to Workstation 4. The combined bandwidth of Workstations 1, 2 and 3 to the device is larger than the bandwidth of Workstation 4 to the device. This leads to an overflow of the send queue of port 4. The funnel on the left symbolizes this status.

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

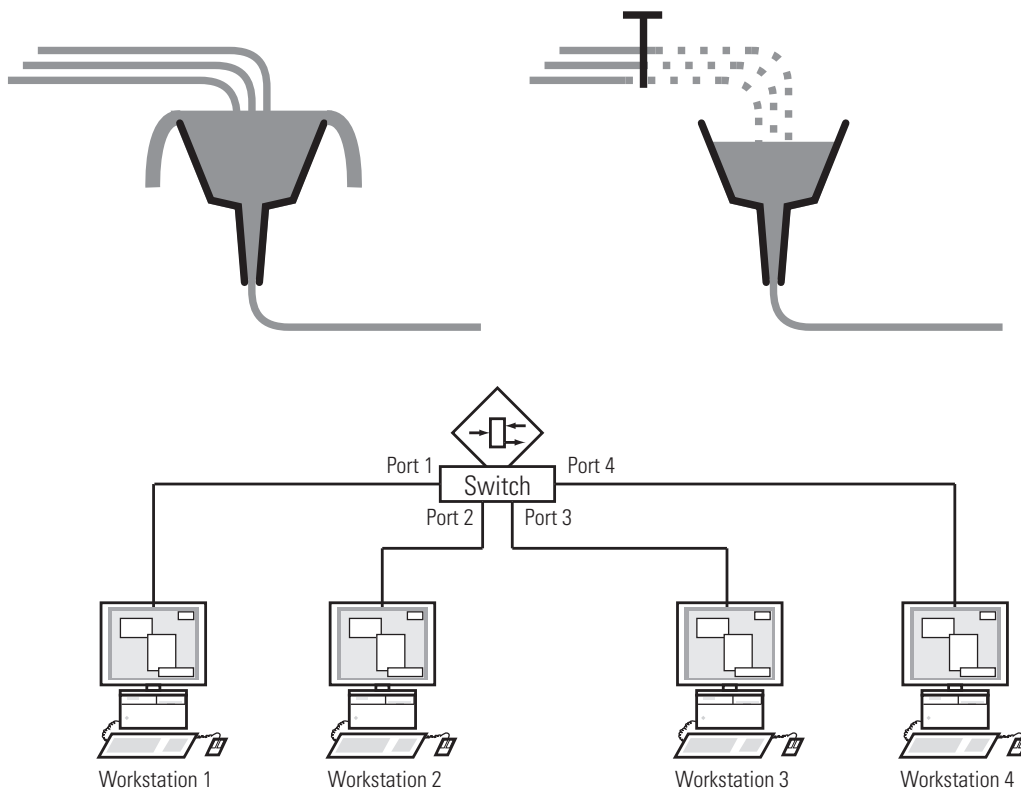


Figure 32: Example of flow control

■ Flow control with a full duplex link

In the example (see fig. 32) there is a full duplex link between Workstation 2 and the device.

Before the send queue of port 2 overflows, the device sends a request to Workstation 2 to include a small break in the sending transmission.

■ Flow control with a half duplex link

In the example (see fig. 32) there is a half duplex link between Workstation 2 and the device.

Before the send queue of port 2 overflows, the device sends data back so that Workstation 2 detects a collision and interrupts the sending process.

8.5.2 Setting the flow control

- Select the `Basics:Port Configuration` dialog.
In the "Flow Control on" column, you checkmark this port to specify that flow control is active here. You also activate the global "Flow Control" switch in the `Switching:Global` dialog.
- Select the `Switching:Global` dialog.
With this dialog you can
 - ▶ switch off the flow control at all ports or
 - ▶ switch on the flow control at those ports for which the flow control is selected in the port configuration table.

8.6 VLANs

8.6.1 VLAN description

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

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

The IEEE 802.1Q standard defines the VLAN function.

The most important benefits of VLANs are:

- ▶ **Network load limiting**
VLANs can reduce the network load considerably as a Switch only transmits Broadcast/Multicast data packets and Unicast packets with unknown (unlearned) destination addresses within the virtual LAN. The rest of the data network is unaffected by this.
- ▶ **Flexibility**
You have the option of forming user groups flexibly based on the function of the participants and not on their physical location or medium.
- ▶ **Clarity**
VLANs give networks a clear structure and make maintenance easier.

8.6.2 Examples of VLANs

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

■ Example 1

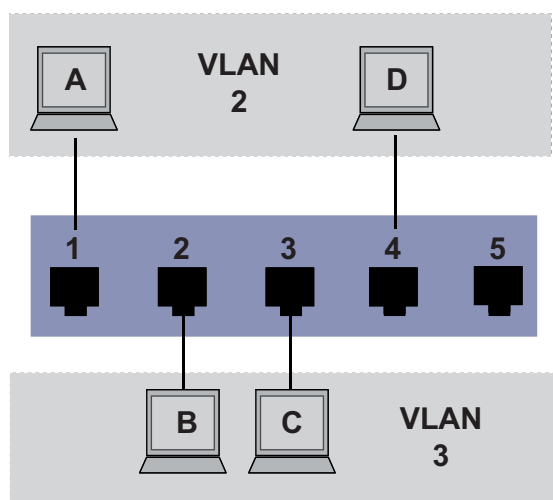


Figure 33: Example of a simple port-based VLAN

The example shows a minimal VLAN configuration (port-based VLAN). An administrator has connected multiple terminal devices to a transmission device and assigned them to 2 VLANs. This effectively prohibits any data transmission between the VLANs, whose members communicate only within their own VLANs.

When setting up the VLANs, you create communication rules for every port, which you enter in incoming (ingress) and outgoing (egress) tables. The ingress table specifies which VLAN ID a port assigns to the incoming data packets. Hereby, you use the port address of the terminal device to assign it to a VLAN.

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

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

For the above example, the status of the TAG field of the data packets is not relevant, so you can generally set it to „U“.

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

Table 12: Ingress table

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

Table 13: Egress table

Proceed as follows to perform the example configuration:

- Configure VLAN
- Select the Switching:VLAN:Static dialog.

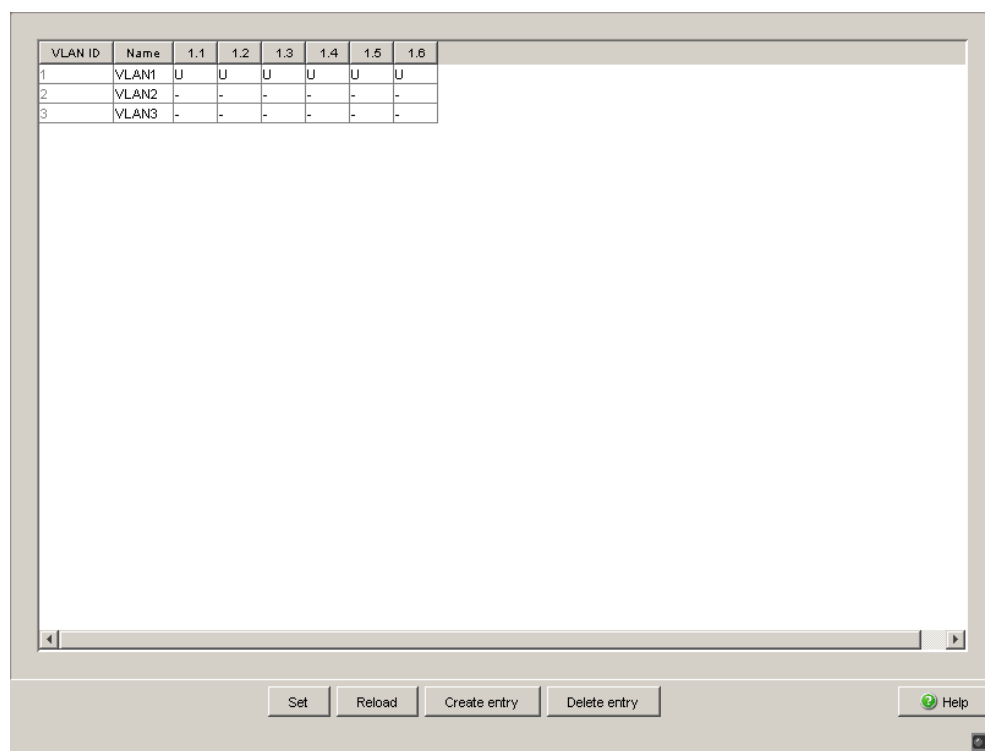


Figure 34: Creating and naming new VLANs

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


```

enable
vlan database
vlan 2
vlan name 2 VLAN2

vlan 3
vlan name 3 VLAN3

vlan name 1 VLAN1

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

```

Switch to the Privileged EXEC mode.

Switch to the VLAN configuration mode.

Create a new VLAN with the VLAN ID 2.

Give the VLAN with the VLAN ID 2 the name VLAN2.

Create a new VLAN with the VLAN ID 3.

Give the VLAN with the VLAN ID 3 the name VLAN3.

Give the VLAN with the VLAN ID 1 the name VLAN1.

Leave the VLAN configuration mode.

Display the current VLAN configuration.

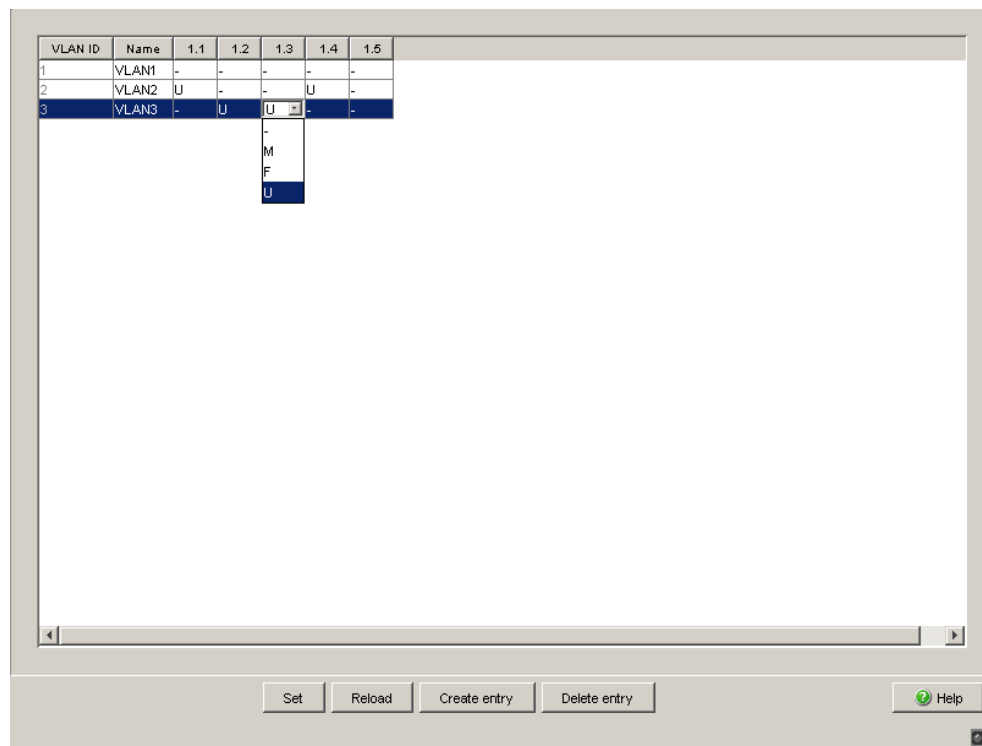
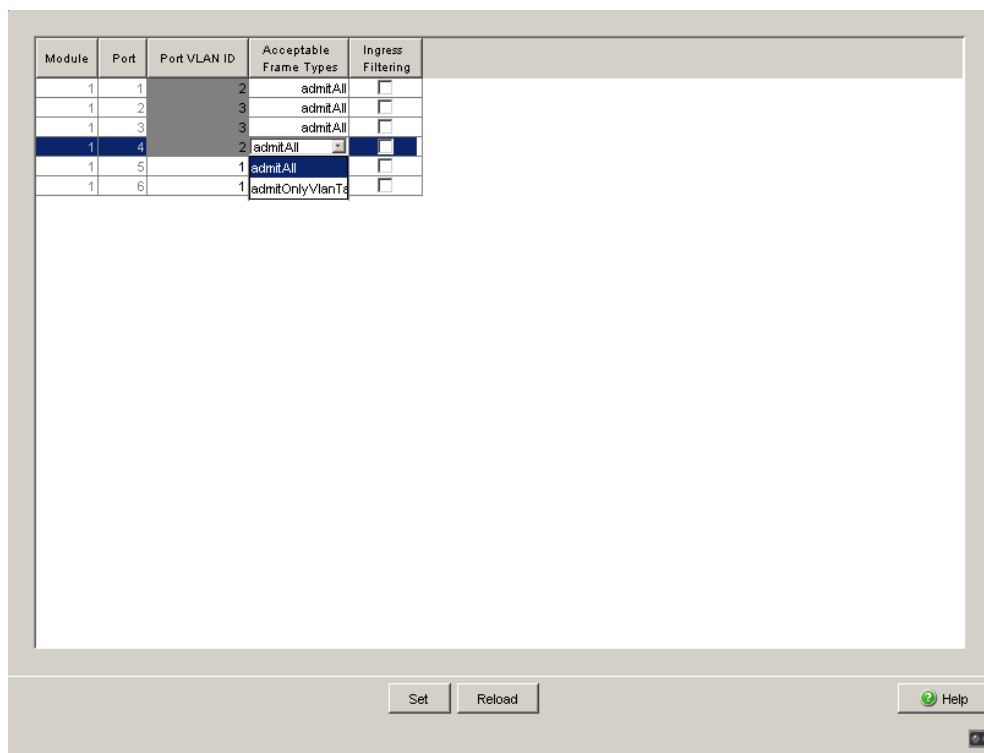
Configuring the ports


Figure 35: Defining the VLAN membership of the ports.

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



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

Buttons: Set, Reload, Help

Figure 36: Assign and save Port VLAN ID, Acceptable Frame Types and Ingress Filtering

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

```

enable
configure
interface 1/1

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

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

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

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

```

Switch to the Privileged EXEC mode.

Switch to the Configuration mode.

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

Port 1/1 becomes member untagged in VLAN 2.

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

Switch to the Configuration mode.

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

Port 1/2 becomes member untagged in VLAN 3.

Port 1/2 is assigned the port VLAN ID 3.

Switch to the Configuration mode.

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

Port 1/3 becomes member untagged in VLAN 3.

Port 1/3 is assigned the port VLAN ID 3.

Switch to the Configuration mode.

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

Port 1/4 becomes member untagged in VLAN 2.

Port 1/4 is assigned the port VLAN ID 2.

Switch to the Configuration mode.

Switch to the privileged EXEC mode.

Show details for VLAN 3.

■ Example 2

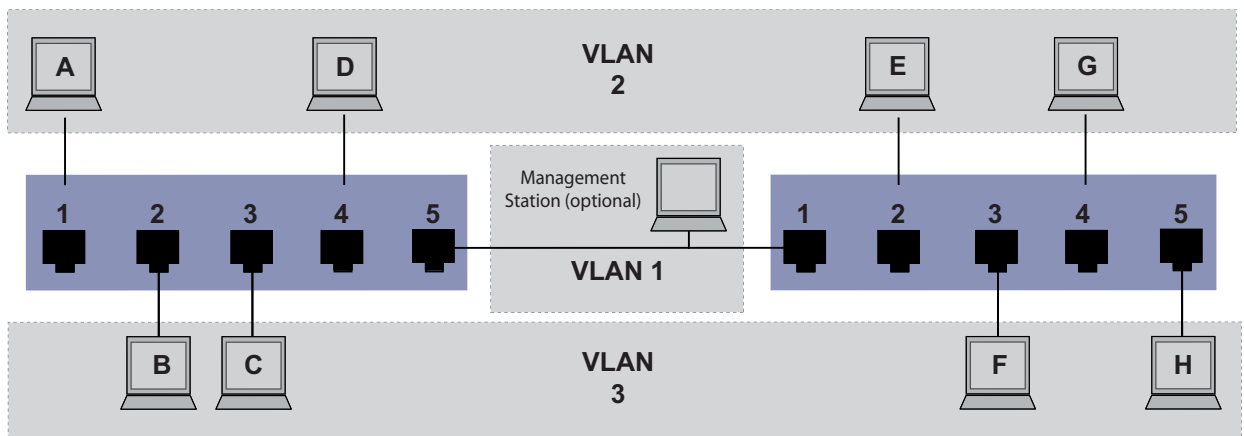


Figure 37: Example of a more complex VLAN constellation

The second example shows a more complex constellation with 3 VLANs (1 to 3). Along with the Switch from example 1, a second Switch (on the right in the example) is now used.

The terminal devices of the individual VLANs (A to H) are spread over two transmission devices (Switches). Such VLANs are therefore known as distributed VLANs. An optional Management Station is also shown, which enables access to all network components if it is configured correctly.

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

As in the previous example, uniquely assign the ports with their connected terminal devices to a VLAN. With the direct connection between the two transmission devices (uplink), the ports transport packets for both VLANs. To differentiate these, “VLAN tagging” is used, which prepares the packets accordingly ([see on page 119 “VLAN tagging”](#)). This maintains the respective VLAN assignments.

Proceed as follows to perform the example configuration:

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

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

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

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

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

Table 14: Ingress table for device on left

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

Table 15: Ingress table for device on right

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

Table 16: Egress table for device on left

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

Table 17: Egress table for device on right

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

The terminal devices “see” their respective part of the network and cannot reach any other participant outside their VLAN. Broadcast and Multicast data packets, and Unicast packets with unknown (unlearned) target addresses as also only sent within a VLAN.

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

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

Proceed as follows to perform the example configuration:

Configure VLAN

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

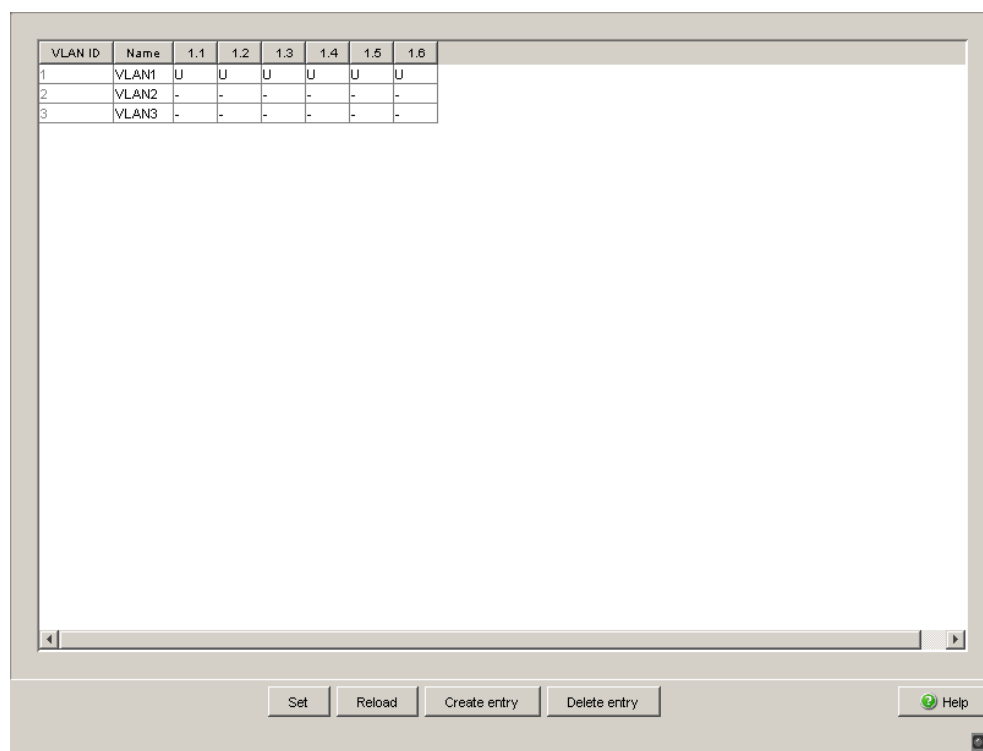


Figure 38: Creating and naming new VLANs

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


```

enable                               Switch to the Privileged EXEC mode.
vlan database                         Switch to the VLAN configuration mode.
vlan 2                                Create a new VLAN with the VLAN ID 2.
vlan name 2 VLAN2                    Give the VLAN with the VLAN ID 2 the name
                                      VLAN2.
vlan 3                                Create a new VLAN with the VLAN ID 3.
vlan name 3 VLAN3                    Give the VLAN with the VLAN ID 3 the name
                                      VLAN3.
vlan name 1 VLAN1                    Give the VLAN with the VLAN ID 1 the name
                                      VLAN1.
exit                                  Switch to the privileged EXEC mode.
show vlan brief                       Display the current VLAN configuration.
Max. VLAN ID..... 4042
Max. supported VLANs..... 255
Number of currently configured VLANs..... 3
VLAN 0 Transparent Mode (Prio. Tagged Frames).. Disabled
VLAN ID VLAN Name                     VLAN Type VLAN Creation Time
-----
1      VLAN1                          Default   0 days, 00:00:05
2      VLAN2                          Static    0 days, 02:44:29
3      VLAN3                          Static    0 days, 02:52:26

```

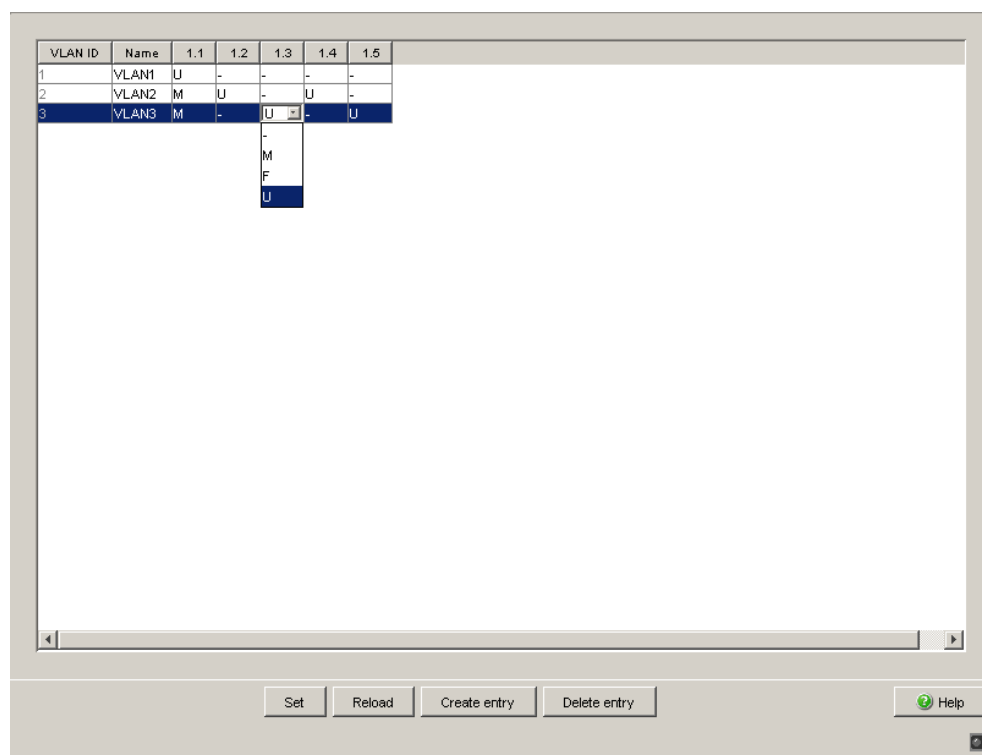
Configuring the ports


Figure 39: Defining the VLAN membership of the ports.

- Assign the ports of the device to the corresponding VLANs by clicking on the related table cell to open the selection menu and define the status. The selection options are:
 - ▶ - = currently not a member of this VLAN (GVRP allowed)
 - ▶ T = member of VLAN; send data packets with tag
 - ▶ U = Member of the VLAN; send data packets without tag
 - ▶ F = not a member of the VLAN (also disabled for GVRP)
 Because terminal devices usually do not interpret data packets with a tag, you select the U setting. You only select the T setting at the uplink port at which the VLANs communicate with each other.
- Click “Set” to temporarily save the entry in the configuration.
- Select the `Switching:VLAN:Port` dialog.

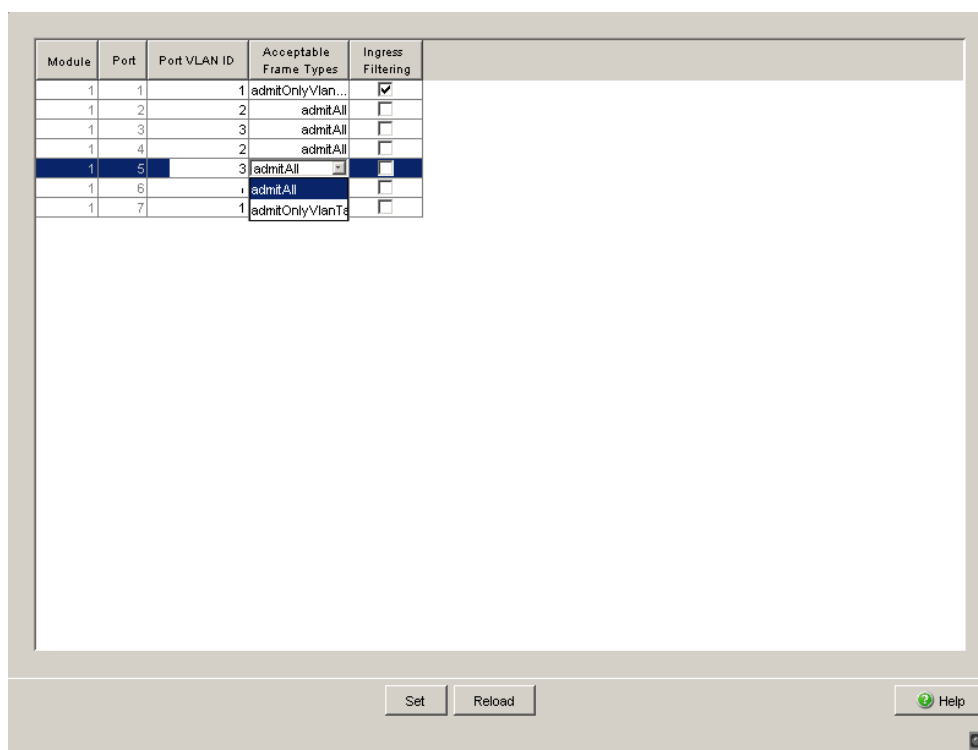


Figure 40: Assign and save Port VLAN ID, Acceptable Frame Types and Ingress Filtering

- Assign the ID of the related VLANs (1 to 3) to the individual ports.
- Because terminal devices usually do not send data packets with a tag, you select the `admitAll` setting for the terminal device ports. Configure the uplink port with `admit only VLAN tags`.
- Activate `Ingress Filtering` at the uplink port so that the VLAN tag is evaluated at this port.
- Click “Set” to temporarily save the entry in the configuration.
- Select the `Basics: Load/Save dialog`.
- In the “Save” frame, select “To Device” for the location and click “Save” to permanently save the configuration in the active configuration.

```

enable                               Switch to the Privileged EXEC mode.
configure                             Switch to the Configuration mode.
interface 1/1                         Switch to the Interface Configuration mode of
                                     interface 1/1.

vlan participation include 1          Port 1/1 becomes member untagged in VLAN 1.
vlan participation include 2          Port 1/1 becomes member untagged in VLAN 2.
vlan tagging 2                        Port 1/1 becomes member tagged in VLAN 2.
vlan participation include 3          Port 1/1 becomes member untagged in VLAN 3.
vlan tagging 3                        Port 1/1 becomes member tagged in VLAN 3.
vlan pvid 1                           Port 1/1 is assigned the port VLAN ID 1.
vlan ingressfilter                    Port 1/1 ingress filtering is activated.
vlan acceptframe vlanonly            Port 1/1 only forwards frames with a VLAN tag.
exit                                  Switch to the Configuration mode.
interface 1/2                         Switch to the interface configuration mode of in-
                                     terface 1/2.

vlan participation include 2          Port 1/2 becomes member untagged in VLAN 2.
vlan pvid 2                           Port 1/2 is assigned the port VLAN ID 2.
exit                                  Switch to the Configuration mode.
interface 1/3                         Switch to the Interface Configuration mode of
                                     Interface 1/3.

vlan participation include 3          Port 1/3 becomes member untagged in VLAN 3.
vlan pvid 3                           Port 1/3 is assigned the port VLAN ID 3.
exit                                  Switch to the Configuration mode.
interface 1/4                         Switch to the interface configuration mode of in-
                                     terface 1/4.

vlan participation include 2          Port 1/4 becomes member untagged in VLAN 2.
vlan pvid 2                           Port 1/4 is assigned the port VLAN ID 2.
exit                                  Switch to the Configuration mode.
interface 1/5                         Switch to the interface configuration mode of in-
                                     terface 1/5.

vlan participation include 3          Port 1/5 becomes member untagged in VLAN 3.
vlan pvid 3                           Port 1/5 is assigned the port VLAN ID 3.
exit                                  Switch to the Configuration mode.
exit                                  Switch to the privileged EXEC mode.
#show VLAN 3                          Show details for VLAN 3.
VLAN ID                               : 3
VLAN Name                             : VLAN3
VLAN Type                             : Static
VLAN Creation Time: 0 days, 00:07:47 (System Uptime)
Interface   Current   Configured   Tagging
-----
1/1         Include   Include     Tagged
1/2         Exclude  Autodetect  Untagged
1/3         Include   Include     Untagged
1/4         Exclude  Autodetect  Untagged
1/5         Include   Include     Untagged

```

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

9 Operation diagnosis

The device provides you with the following diagnostic tools:

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

9.1 Sending traps

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

Examples of such events are:

- ▶ a hardware reset
- ▶ changes to the configuration
- ▶ segmentation of a port
- ▶ ...

Traps can be sent to various hosts to increase the transmission reliability for the messages. A trap message consists of a packet that is not acknowledged.

The device sends traps to those hosts that are entered in the trap destination table. The trap destination table can be configured with the management station via SNMP.

9.1.1 SNMP traps during boot

The device sends the ColdStart trap every time it boots.

9.1.2 Configuring traps

- Select the `Diagnostics:Alarms (Traps)` dialog. This dialog allows you to determine which events trigger an alarm (trap) and where these alarms should be sent.
- Select "Create entry".
- In the "Address" column, enter the IP address of the management station to which the traps should be sent.
- In the "Enabled" column, you mark the entries which should be taken into account when traps are being sent.
- In the "Selection" frame, select the trap categories from which you want to send traps.

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

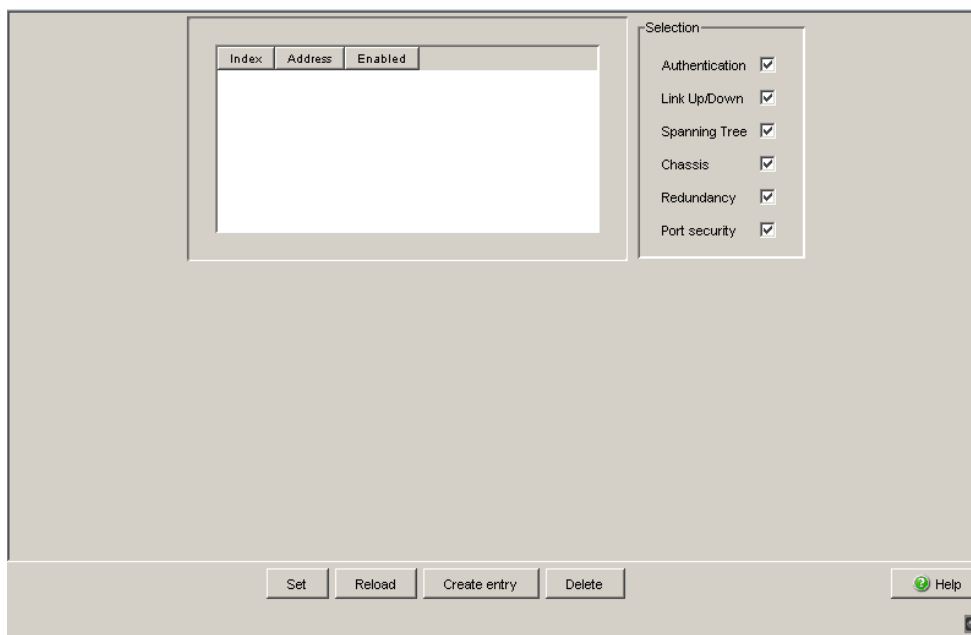


Figure 41: Alarms dialog

The events which can be selected are:

Name	Meaning
Authentication	The device has rejected an unauthorized access attempt (see the <code>Access for IP Addresses and Port Security</code> dialog).
Link Up/Down	At one port of the device, the link to a device connected there has been established/interrupted.
Spanning Tree	The topology of the Rapid Spanning Tree has changed.
Chassis	Summarizes the following events: <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"> – The Memory Backup Adapter has been added or removed. – One of the temperature thresholds has been exceeded.
Redundancy	The redundancy status of the ring redundancy (redundant line active/inactive) or the redundant Ring/Network coupling (redundancy exists) has changed.
Port security	On one port a data packet has been received from an unauthorized terminal device (see the <code>Port Security</code> dialog).

Table 18: 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 159 “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 temperature threshold has been exceeded or has not been reached.
- ▶ 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 74 “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 160 “Monitoring the device functions via the signal contact”](#)).

9.2.1 Configuring the device status

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

<code>enable</code>	Switch to the Privileged EXEC mode.
<code>configure</code>	Switch to the Configuration mode.
<code>device-status monitor all error</code>	Include all the possible events in the device status determination.
<code>device-status trap enable</code>	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.

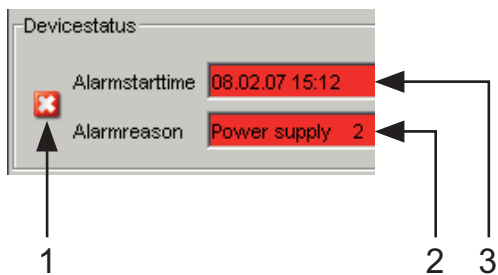


Figure 42: Device status and alarm display

- 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 temperature threshold has been exceeded or has not been reached.
- ▶ 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 74 “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 160 “Monitoring the device functions via the signal contact”](#)).

9.3.1 Controlling the signal contact

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

Application options:

- ▶ Simulation of an error during SPS error monitoring.

► Remote control of a device via SNMP, such as switching on a camera.

- Select the `Diagnostics:Signal Contact 1/2` dialog.
- In the "Mode Signal contact" frame, you select the "Manual setting" mode to switch the contact manually.
- Select "Opened" in the "Manual setting" frame to open the contact.
- Select "Closed" in the "Manual setting" frame to close the contact.

<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 155 "Monitoring the device status"](#)) via the signal contact.

9.3.3 Monitoring the device functions via the signal contact

■ Configuring the operation monitoring

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

<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

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

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

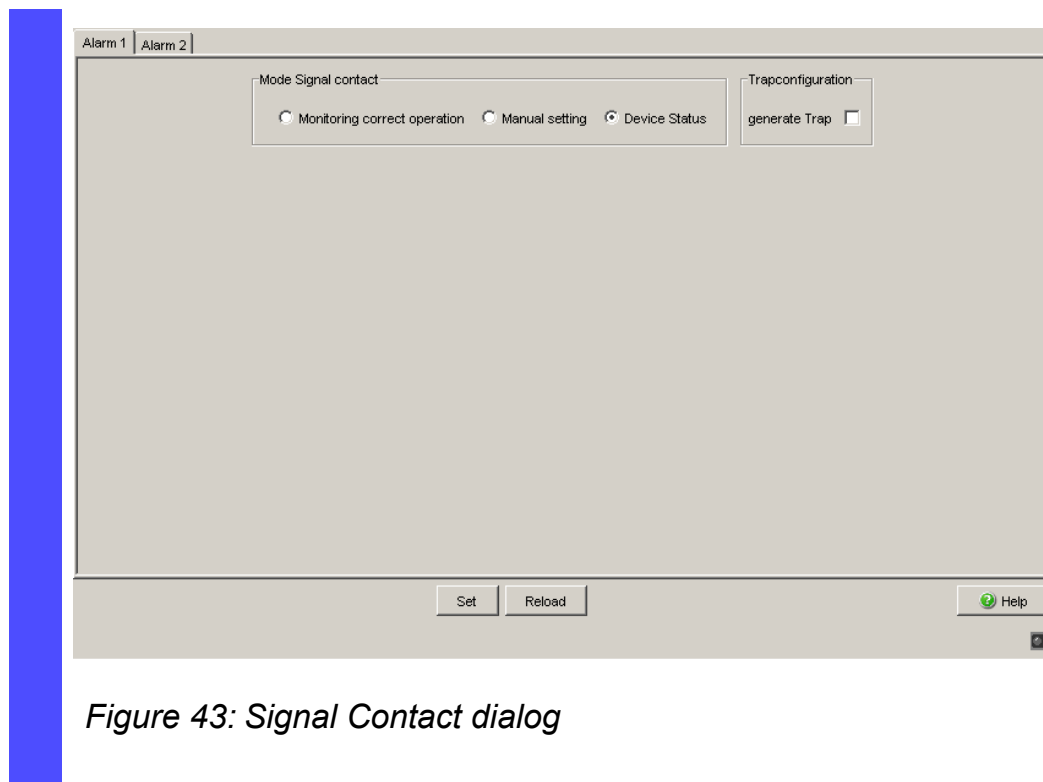


Figure 43: Signal Contact dialog

```
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.

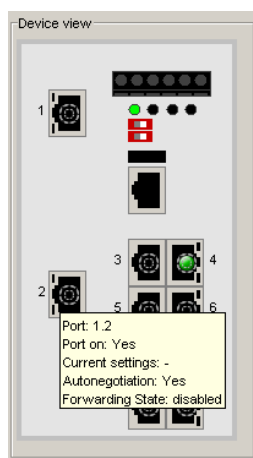









Figure 44: Device view

Meaning of the symbols:

-  The port (10, 100 Mbit/s, 1, 10 Gbit/s) is enabled and the connection is OK.
-  The port is disabled by the management and it has a connection.
-  The port is disabled by the management and it has no connection.
-  The port is in autonegotiation mode.
-  The port is in HDX mode.
-  The port is in RSTP discarding mode (100 Mbit/s).
-  The port is in routing mode (100 Mbit/s).

9.5 Event counter at port level

The port statistics table enables experienced network administrators to identify possible 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 19: Examples indicating possible detected problems

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

Module	Port	Transmitted Unicast Packets	Received Packets	Received Octets	Received Fragments	Detected CRC errors	Detected Collisions	Packets 64 bytes	Packets 65 to 127 bytes	Packets 128 to 255 bytes
1	1	0	0	0	0	0	0	0	0	0
1	2	331	872	759280	0	0	0	316	285	0
1	3	8033	8463	1705705	0	0	0	1603	813	1316
1	4	8667	9958	2490032	0	0	0	2644	899	1404
2	1	63	337	57276	0	0	0	2483	511	41
2	2	63	0	0	0	0	0	2486	519	0
2	3	0	0	0	0	0	0	0	0	0
2	4	2869	3708	1779532	0	0	0	4156	658	251
3	1	0	0	0	0	0	0	0	0	0
3	2	0	0	0	0	0	0	0	0	0

Figure 45: 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, once these devices have also activated LLDP.
- ▶ receives connection and management information from neighboring devices of the shared LAN, once these devices have also activated LLDP.
- ▶ sets up a management information schema and object definition for saving connection information of neighboring devices with active LLDP.

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

Content of the connection and management information:

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


- ▶ Information about the VLANs configured in the switch (VLAN ID and VLAN name).

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

To exchange information, LLDP uses an IEEE MAC address which devices do not usually send. For this reason, devices without LLDP support discard LLDP packets. Thus a non-LLDP-capable device between two LLDP-capable devices prevents LLDP information exchange between these two devices. To get around this, 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

-  Select the `Diagnostics:Topology Discovery` dialog.

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

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

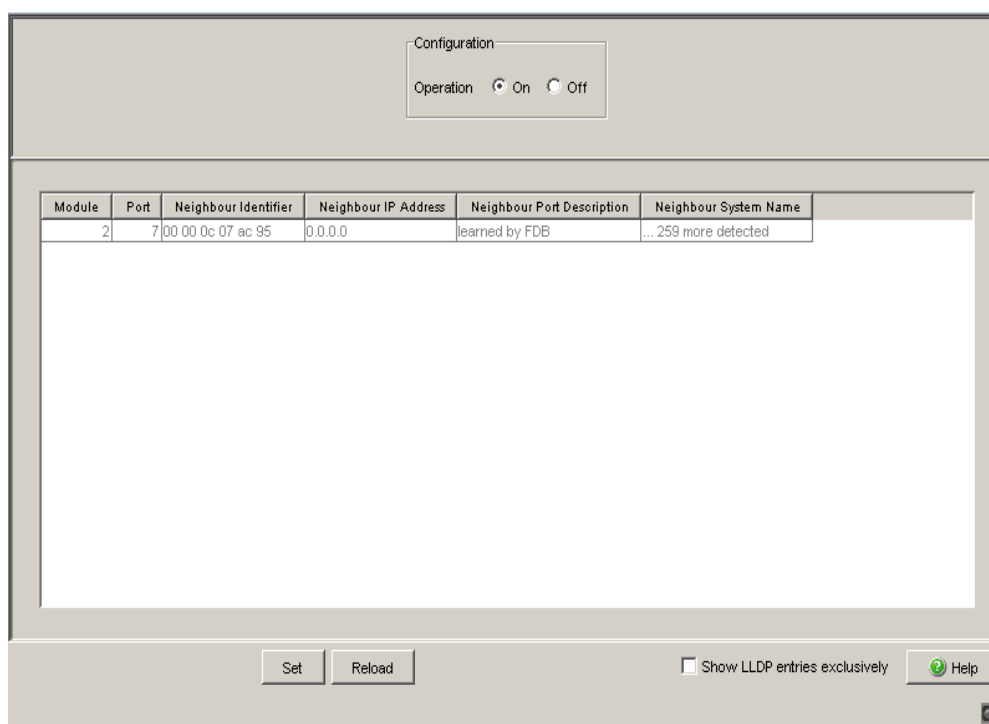


Figure 46: Topology discovery

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

If

- ▶ devices with active topology discovery function and
- ▶ devices without active topology discovery function are connected to a port, the topology table hides the devices without active topology discovery.

If

- ▶ only devices without active topology discovery are connected to a port, the table will contain one line for this port to represent all devices. This line contains the number of connected devices. MAC addresses of devices that the topology table hides for the sake of clarity, are located in the address table (FDB) ([see page 102 “Entering static address entries”](#)).

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. This prevents the device from connecting to the network with a duplicate IP address.
passiveOnly	Enables passive detection only. The device listens passively on the network to determine whether its IP address already exists. If it detects a duplicate IP address, it will initially defend its address by employing the ACD mechanism and sending out gratuitous ARPs. If the remote device does not disconnect from the network, the management interface of the local device will then disconnect from the network. Every 15 seconds, it will poll the network to determine if there is still an address conflict. If there isn't, it will connect back to the network.

Table 20: 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 20](#)).

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.

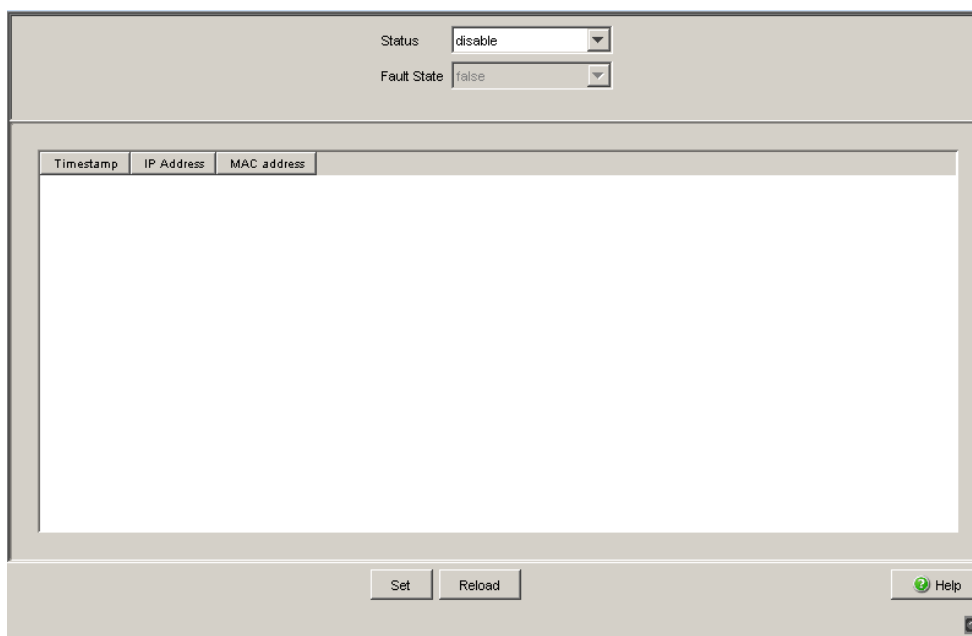


Figure 47: IP Address Conflict Detection dialog

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

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

- Select the `Diagnostics:Report` dialog.
- Click "Log File" to open the HTML file in a new browser window.
- Click "System Information" to open the HTML file in a new browser window.

9.9 Monitoring port traffic (port mirroring)

In port mirroring, the valid data packets of one port, the source port, are copied to another, the destination port. The data traffic at the source port is not influenced by port mirroring.

A management tool connected at the destination port, e.g. an RMON probe, can thus monitor the source port's data traffic in sending and receiving direction.

The destination port forwards the data to be sent and blocks data received.

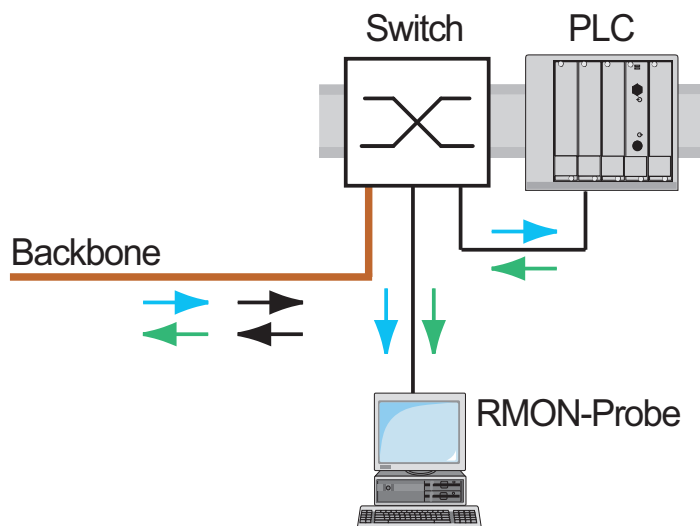


Figure 48: Port mirroring

- Select the `Diagnostics:Port Mirroring` dialog.

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

- Select the source port whose data traffic you want to observe.
- Select the destination port to which you have connected your management tool.
- Select "enabled" to switch on the function.

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

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

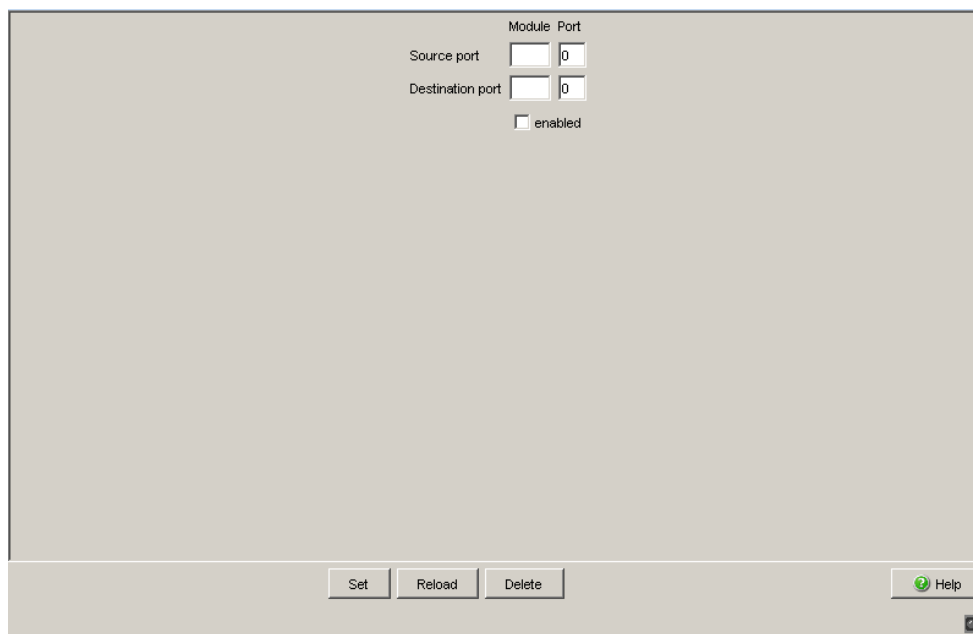


Figure 49: Port Mirroring dialog

10 EtherNet/IP

EtherNet/IP, that is accepted worldwide, is an industrial communication protocol standardized by the Open DeviceNet Vendor Association (ODVA) on the basis of Ethernet. It is build upon the widely used transport protocols TCP/IP and UDP/IP (standard). EtherNet/IP thus provides a broad basis, supported by leading manufacturers, for effective data communication in the industry sector.

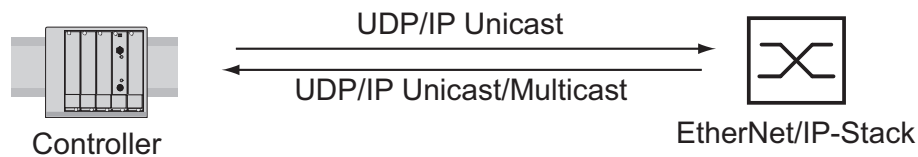


Figure 50: Communication between the Controller (PLC) and the Switch

EtherNet/IP extends Ethernet by the industry protocol CIP (Common Industrial Protocol), an application layer for automation applications. Ethernet is thus ideally suited to the industrial control technology sector.

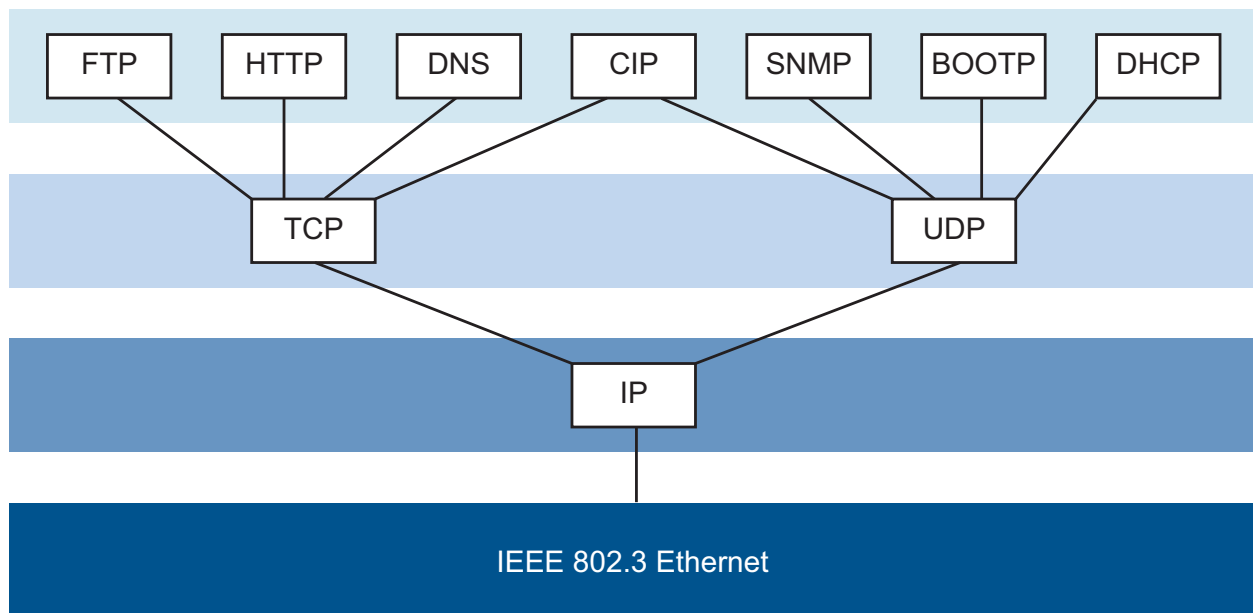


Figure 51: EtherNet/IP (CIP) in the ISO/OSI Reference Model

Note the following EtherNet/IP adapter details:

- The minimum Request Packet Interval (RPI) is 100 ms.
- The total number of CIP connections is 128. These connections are shared within the Class 1 / Class 3, and are listen-only connections. Example: If you have 128 Class 1 connections, no further connections are available for Class 3 or listen-only.

10.1 Integration into a Control System

After installing and connecting the Switch, you configure it according to the “Basic Configuration” user manual. Then:

- Use the Web-based interface in the `Switching:Multicasts` dialog to check whether the IGMP Snooping is activated.
- Use the Web-based interface in the `Advanced:EtherNet/IP` dialog to check whether EtherNet/IP is activated.
- Use the Web-based interface in the `Advanced:EtherNet/IP` dialog to load the EDS (= EtherNet/IP configuration file) and the Icon onto your local computer.

10.2 EtherNet/IP Parameters

10.2.1 Identity Object

The Switch supports the EtherNet/IP identity object (Class Code 01). The Schneider Electric manufacturer ID is 243. **Schneider Electric** uses the manufacturer-specific ID 149 (95_H) to designate the “Managed Ethernet Switch” product type.

Id	Attribute	Access Rule	Data type	Description
1	Vendor ID	Get	UINT	Schneider Electric 243
2	Device Type	Get	UINT	Vendor-specific definition 149 (95H) "Managed Ethernet Switch".
3	Product Code	Get	UINT	Product Code: mapping is defined for every device type, e.g. TCSESM10xxxxx is 5680.
4	Revision	Get	STRUCT USINT Major USINT Minor	Revision of the Ethernet/IP implementation, currently 1.1, Major Revision and Minor Revision
5	Status	Get	WORD	Not used
6	Serial Number	Get	UDINT	Serial number of the device (contains last 3 Bytes of MAC address).
7	Product Name	Get	Short String (max. 32 Byte)	Displayed as "Schneider Electric" + order code, e.g. Schneider Electric TCSESM10xxxxx.

Table 21: Identity Object

10.2.2 TCP/IP Interface Object

The Switch supports an instance (instance 1) of the TCP/IP Interface Object (Class Code F5_H, 245) of EtherNet/IP.

In the case of write access, the Switch stores the complete configuration in its flash memory. Saving can take 10 seconds. If the save process is interrupted, for example, by a power cut, the Switch may become inoperable.

Note: The Switch replies to the configuration change „Set Request” with a „Response” although saving of the configuration has not yet been completed.

Id	Attribute	Access rule	Data type	Description
1	Status	Get	DWORD	Interface Status (0: Interface not configured, 1: Interface contains valid config).
2	Interface Capability flags	Get	DWORD	Bit 0: BOOTP Client, Bit 1: DNS Client, Bit 2: DHCP Client, Bit 3: DHCP-DNS Update, Bit 4: Configuration settable (within CIP). Other bits reserved (0).
3	Config Control	Set/Get	DWORD	Bits 0 through 3: Value 0: using stored config, Value 1: using BOOTP, Value 2: using DHCP. Bit 4: 1 device uses DNS for name lookup (always 0 because not supported) Other bits reserved (0).
4	Physical Link Object	Get	Structure: UINT Path size EPATH Path	Path to the Physical Link Objekt, always {20H, F6H, 24H, 01H} describing instance 1 of the Ethernet Link Object.
5	Interface Configuration	Set/Get	Structure: UDINT IP address UDINT Net-mask UDINT Gateway address UDINT Name server 1 UDINT Name server 2 STRING Domain name	IP Stack Configuration (IP-Address, Netmask, Gateway, 2 Nameservers (DNS, not supported) and the domain name).
6	Host name	Set/Get	STRING	Host name (for DHCP DNS Update).

Table 22: TCP/IP Interface Object

10.2.3 Ethernet Link Object

The Switch supports at least one instance (instance 1 is the CPU Ethernet Interface's instance) of the Ethernet Link Object (Class Code F6_H, 246) of EtherNet/IP.

Id	Attribute	Access rule	Data type	Description
1	Interface Speed	Get	UDINT	Used interface speed in MBits/s (10, 100, 1000, ...). 0 is used when the speed has not been determined or is invalid because of detected problems.
2	Interface Flags	Get	DWORD	Interface Status Flags: Bit 0: Link State (1: Link up), Bit 1: 0: Half-Duplex, 1: FullDuplex1, Bits 2 through 4: Autoneg Status (0: Autoneg in Progress, 1: Autoneg failed, 2: failed but Speed detected, 3: Autoneg success, 4: No Autoneg), Bit 5: manual configuration requires reset (always 0 because not needed), Bit 6: detected hardware error.
3	Physical Address	Get	ARRAY of 6 USINTs	MAC address of physical interface.
4	Interface Counters	Get	Struct MIB II Counters Jewels UDINT	InOctets, InUcastPackets, InNUcastPackets, InDiscards, InErrors, InUnknownProtos, OutOctets, OutUcastPackets, OutNUcastPackets, OutDiscards, OutErrors.
5	Media Counters	Get	Struct Ethernet MIB Counters Jewels UDINT	Alignment Errors, FCS Errors, Single Collision, Multiple Collision, SQE Test Errors, Deferred Transmissions, Late Collisions, Excessive Collisions, MAC TX Errors, Carrier Sense Errors, Frame Too Long, MAC RX Errors.
6	Interface Control	Get/Set	Struct Control Bits WORD Forced Iface Speed UINT	Control Bits: Bit 0: Autoneg enable/disable (1: enable), Bit 1: Duplex mode (1: full duplex, if Autoneg is disabled). Interface speed in MBits/s: 10, 100,..., if Autoneg is disabled.

Table 23: Ethernet Link Object

The Switch supports additional manufacturer-specific attributes.

Id	Attribute	Access rule	Data type	Description
100 (64 H)	Ethernet Interface Index	Get	UDINT	Interface/Port Index (ifIndex from MIB II)
101 (65 H)	Port Control	Get/Set	DWORD	Bit 0 (RO): Link state (0: link down, 1: link up) Bit 1 (R/W): Link admin state (0: disabled, 1: enabled) Bit 8 (RO:) Access violation alarm Bit 9 (RO): Utilization alarm
102 (66 H)	Interface Utilization	Get	UDINT	The existing Counter from the private MIB hmlfaceUtilization is used. Utilization in percentage ^a . RX Interface Utilization.
103 (67 H)	Interface Utilization Alarm Upper Threshold	Get/Set	UDINT	Within this parameter the variable hmlfaceUtilizationAlarmUpperThreshold can be accessed. Utilization in percentage ^a . RX Interface Utilization Upper Limit.
104 (68 H)	Interface Utilization Alarm Lower Threshold	Get/Set	UDINT	Within this parameter the variable hmlfaceUtilizationAlarmLowerThreshold can be accessed. Utilization in percentage ^a . RX Interface Utilization Lower Limit.
105 (69 H)	Broadcast Limit	Get/Set	UDINT	Broadcast limiter Service (Egress BC-Frames limitation, 0: disabled), Frames/second
106 (6A H)	Ethernet Interface Description	Get	STRING [max. 64 Bytes] even number of Bytes	Interface/Port Description (from MIB II ifDescr), e.g. "Unit: 1 Slot: 2 Port: 1 - 10/100 Mbit TX", or "unavailable", max. 64 Bytes.

Table 24: Schneider Electric extensions for the Ethernet Link Object

a. Unit: 1 hundredth of 1%, i.e., 100 equals 1%

10.2.4 Ethernet Switch Agent Object

The Switch supports the Schneider Electric-specific Ethernet Switch Agent Object (Class Code F5_H, 149) for the Switch configuration and information parameters with one instance (instance 1).

You will find further information on these parameters and how to set them in the “Web-based Interface” reference manual.

Attribute	ID/Bit No.	Description
Switch Status	ID 01	DWORD (32 Bit) RO
	Bit 0	Overall state (0: ok, 1: inoperable) Like the signal contact.
	Bit 1	Power Supply 1 (0: ok, 1: inoperable or not existing)
	Bit 2	Power Supply 2 (0: ok, 1 : inoperable or not existing)
	Bit 3	Power Supply 3 (0: ok or not possible on this platform, 1: inoperable or not existing)
	Bit 4	Power Supply 4 (0: ok or not possible on this platform, 1: inoperable or not existing)
	Bit 5	Power Supply 5 (0: ok or not possible on this platform, 1: inoperable or not existing)
	Bit 6	Power Supply 6 (0: ok or not possible on this platform, 1: inoperable or not existing)
	Bit 7	Power Supply 7 (0: ok or not possible on this platform, 1: or not existing)
	Bit 8	Power Supply 8 (0: ok or not possible on this platform, 1: inoperable or not existing)
	Bit 9	DIP RM (on: 1, off: 0)
	Bit 10	DIP Standby (on: 1, off: 0)
	Bit 11	Signal Contact 1 (0: closed, 1: open)
	Bit 12	Signal Contact 2 (0: closed, 1: open)
	Bit 16	Temperature (0: ok, 1: threshold exceeded)
	Bit 17	Fan (0: ok or no fan, 1: inoperable)
	Bit 21	DIP Ring Ports, 0: Module 1 Port 1&2, 1: Module 2, Port 1 and 2
	Bit 22	DIP Configuration: 1: enabled, 0: disabled)
	Bit 23	DIP HIPER-Ring State: 1: on, 0: off)
	Bit 24	Module removed (1: removed)
	Bit 25	EAM removed (1: removed)
	Bit 28	HIPER-Ring (1: loss of redundancy reserve)
	Bit 29	Ring-/Netcoupling (1: loss of redundancy reserve)
	Bit 30	Connection Problem (1: link inoperable)

Table 25: Schneider Electric Ethernet Switch Agent Object

Attribute	ID/Bit No.	Description
Switch Temperature	ID 02	Struct{INT RO Temperature °F, INT RO Temperature °C}
Reserved	ID 03	Always 0, attribute is reserved for future use.
Switch Max Ports	ID 04	UINT (16 Bit) RO Maximum number of Ethernet Switch Ports
Multicast Settings (IGMP Snooping)	ID 05	WORD (16 Bit) RW
	Bit 0 RW	IGMP Snooping (1: enabled, 0: disabled)
	Bit 1 RW	IGMP Querier (1: enabled, 0: disabled)
	Bit 2 RO	IGMP Querier Mode (1: Querier, 0: Non-Querier)
	Bit 4-6 RW	IGMP Querier Packet Version 1: V1, 2: V2, 3: V3, 0: Off (IGMP Querier disabled)
Switch Existing Ports	ID 06	ARRAY OF DWORD RO Bitmask of existing Switch Ports (32 bit)
	Per Bit starting with Bit 0 (means Port 1)	1: Port existing, 0: Port not available. Array (bit mask) size is adjusted at the size of maximum number of Switch ports (e.g. a max. no of 28 ports means that 1 DWORD is used (32 bit)).
Switch Port Control	ID 07	ARRAY OF DWORD RW Bitmask Link Admin Status Switch Ports (32 bit)
	Per Bit starting with Bit 0 (means Port 1)	0: Port enabled, 1: Port disabled. Array (bit mask) size is adjusted at the size of maximum number of Switch ports (e.g. a max. no. of 28 ports means that 1 DWORD is used (32bit)).
Switch Ports Mapping	ID 08	ARRAY OF USINT (BYTE, 8 bit) RO Instance number of the Ethernet-Link-Object
	Starting with Index 0 (means Port 1)	All Ethernet Link Object Instances for the existing Ethernet Switch Ports (1..N (maximum number of ports)). When the entry is 0, the Ethernet Link Object for this port does not exist.
Switch Action Status	ID 09	DWORD (32 bit) RO
	Bit 0	Flash write in progress
	Bit 1	Unable to write to flash or write incomplete

Table 25: Schneider Electric Ethernet Switch Agent Object

The Schneider Electric-specific Ethernet Switch Agent Object provides you with the additional manufacturer-specific service with service code 35_H for saving the Switch configuration. The Switch responds to the request to save the configuration as soon as it has saved the configuration in the flash memory.

10.2.5 I/O Data

You will find the precise meaning of the individual bits of the device state in the I/O data in [“Ethernet Switch Agent Object” on page 185](#).

I/O Data	Value (data types and sizes to be defined)	Direction
Device Status	Bitmask (see Switch Agent Attribute 1)	Input, DWORD 32 Bit
Link Status	Bitmask, 1 Bit per port 0: No link, 1: Link up	Input, DWORD
Output Links Admin State applied	Bitmask (1 Bit per port) to acknowledge output. Link state change can be denied, e.g. for controller access port. 0: Port enabled, 1: Port disabled.	Input DWORD
Utilization Alarm	Bitmask, 1 Bit per port 0: No alarm, 1: Alarm on port	Input, DWORD
Access Violation Alarm	Bitmask, 1 Bit per port 0: No alarm, 1: Alarm on port	Input, DWORD
Multicast Connections	Integer, number of connections	Input, 1 DINT 32 Bit
TCP/IP Connections	Integer, number of connections	Input, 1 DINT 32 Bit
Link Admin State	Bitmask, one Bit per port 0: Port enabled, 1: Port disabled	Output, DWORD

Table 26: I/O Data

10.2.6 Mapping of the Ethernet Link Object Instances

The table displays the mapping of the Switch port number to the EthernetLink Object Instance.

Ethernet Link Object Instance	TCSESM, TCSESM-E
1	CPU
2	1
3	2
4	3
5	4
6	5
7	6
8	7
9	8
10	9
11	10
12	11
13	12
14	13
..	..

Table 27: Mapping Switch port numbers to Ethernet Link Object Instances

10.2.7 Supported Services

The following table gives an overview of the supported services by the Ethernet/IP implementation for the objects instance.

Service code	Identity Object	TCP/IP Inter- face Object	Ethernet Link Object	Switch Agent Object
Get Attribute All (01H)	All Attributes	All Attributes	All Attributes	All Attributes
Set Attribute All (02H)	-	Settable Attri- butes (3, 5, 6)	-	-
Get Attribute Single (0EH)	All Attributes	All Attributes	All Attributes	All Attributes
Set Attribute Single (10H)	-	Settable Attributes (3, 5, 6)	Settable Attributes (6, 65H, 67H, 68H, 69H)	Settable Attributes (7)
Reset (05H)	Parameter (0,1)	-	-	-
Save Configura- tion (35H) Vendor-specific	Parameter (0,1)	-	-	Save Switch Configuration

Table 28: Supported Services

10.3 TCSESM in a Premium System

The section describes the configuration of a TCSESM switch as an EtherNet/IP adapter in a Premium system using Unity Pro software.

The addition of the EtherNet/IP function to Schneider’s Connexium Managed Switch product line allows the ESM to be configured as an EtherNet/IP adapter in a Premium system using a TSX ETC xxx Ethernet communication module. An example of such an arrangement is described below.

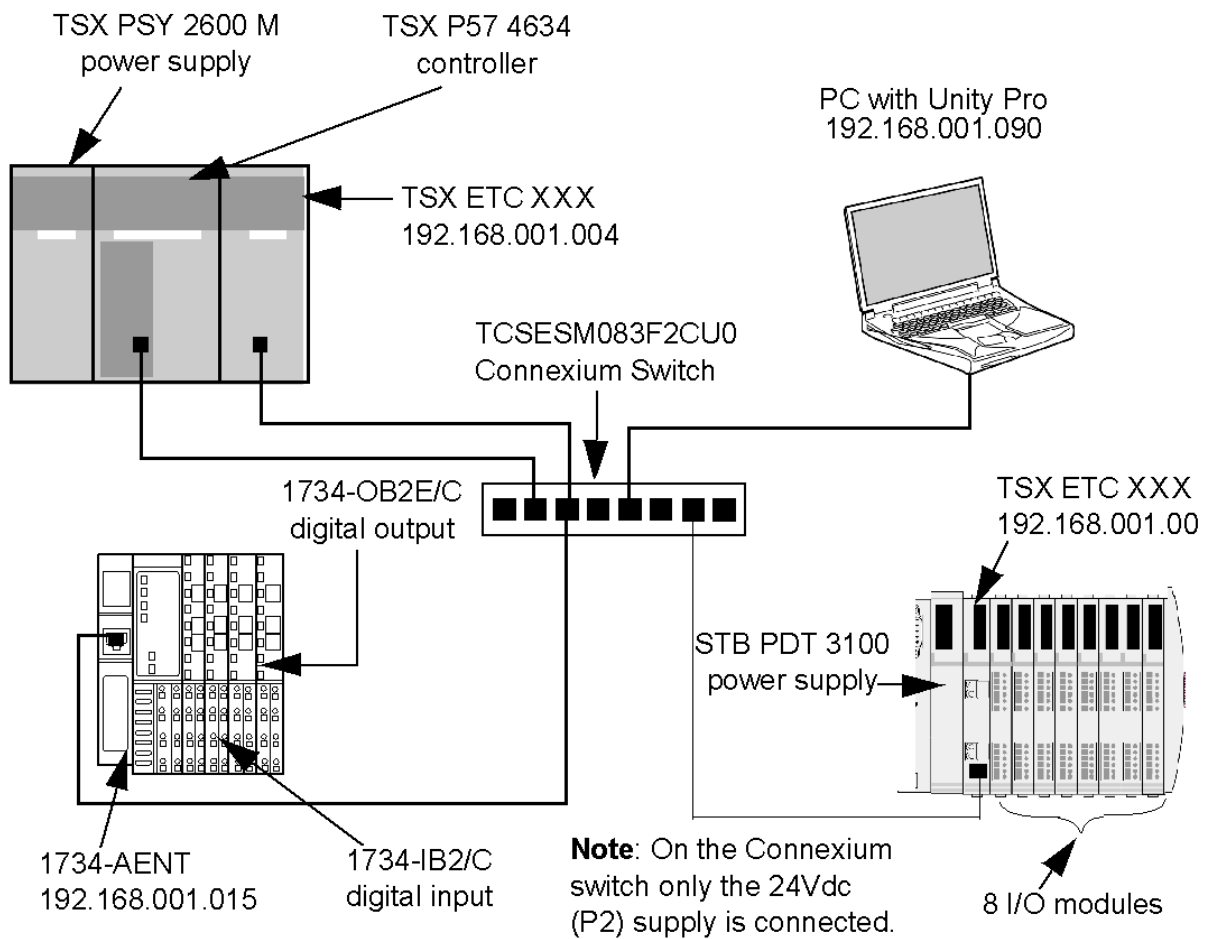


Figure 52: Required hardware and the connections involved to develop a network topology

To re-create this example, be sure to:

- ▶ use the IP addresses for your own configurations
 - PC
 - STB NIC 2212 EtherNet/IP network interface module
 - 1734-AENT PointIO adapter
 - TSX ETC xxx Ethernet communication module
- ▶ check all wiring

Note: Unity Pro software running in the PC is used to configure the Quantum controller. In this example, the PC is indirectly wired to the CPU's Ethernet port via the Ethernet switch. Alternatively, you could bypass the switch and directly wire the PC to another one of the CPU's ports.

10.3.1 Adding EDS Files

Before the TCSESM switch can be configured in a Premium system, the TCSESM EDS file has to be added to the Unity Pro EtherNet/IP Device Library. Unity Pro includes an EDS Management wizard that you can use to add one or more EDS files to the Device Library.

The wizard presents a series of instruction screens that:

- ▶ simplify the process of adding EDS files to the Device Library, and
- ▶ provide a redundancy check in case you attempt to add duplicate EDS files to the Device Library

Note: During the following procedure, you can select `Devices:Options...` to open the Display Options window, where you can enable/disable messages indicating the EDS file you are adding is a duplicate—or a different version—of an existing EDS file.

10.3.2 Adding one or more EDS files to the Device Library

- Open the Unity project with ETC configured.
- Open the ETC module configuration window.
- Add the switch's EDS file to the device library (for more information, refer to the ETC user manual).
 - Page 1 of the wizard opens.
- Click Next.
 - Page 2 of the wizard opens.

EDS Management

EtherNet/IP™

Select the Location of the EDS File(s):

Add File(s)

Add all the EDS from the Directory Look in Subfolders

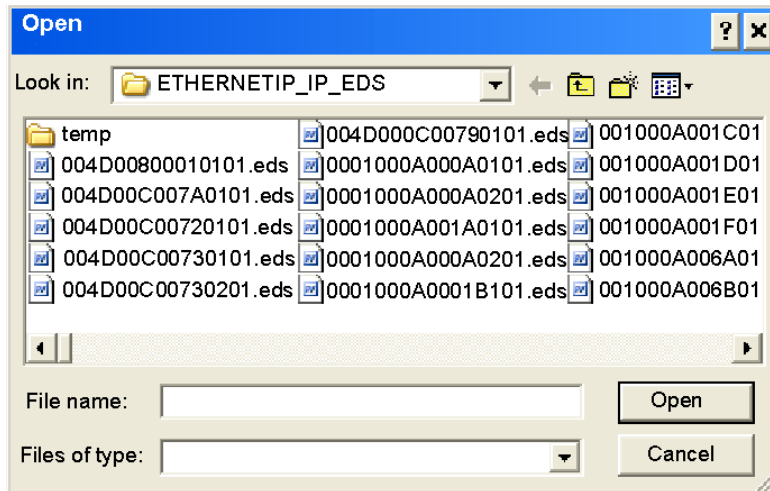
Directory or File Name:

The EDS Files usable in EIP-CT are registered in the EDS base. Select the location of the file(s) and click on the Next button to insert the EDS files in the base.

< Back Next > Cancel Help

- In the Select the Location of the EDS File(s) section, select either:
 - Add File(s), to add one or more EDS files you will individually select, or
 - Add all the EDS Files from the Directory, to add all files from a folder you will select.
 - Select Look in Subfolders to add EDS files in subfolders beneath the folder you select

- Click the Browse button.
The Open dialog opens.



- Use the Open dialog to navigate to and select:
 - one or more EDS files, or
 - a folder containing EDS files
- After you have made your selection(s), click Open.
The dialog closes and your selection appears in the Directory or File Name field.
- Click Next.
The wizard compares the selected EDS files against existing files in the Device Library.
- (Conditional) If one or more selected EDS files are duplicates and if notice of redundant files is enabled in the Display Options dialog, a File Already Exists message displays.
Close the message.
- Page 3 of the wizard opens indicating the Status of each device you attempted to add:
 - a green check mark indicates the EDS file can be added
 - a blue informational icon indicates a redundant file
 - a red check mark indicates an invalid EDS file
 (Optional) Select a file in the list, then click View Selected File to open it.
- Click Next to add the nonduplicate files.
Page 4 of the wizard opens, indicating the action is complete.
- Click Finish to close the wizard.
The device(s) you added can now be inserted into your EtherNet/IP configuration.

10.3.3 Automatically Detect and Add the TCSESM Switch

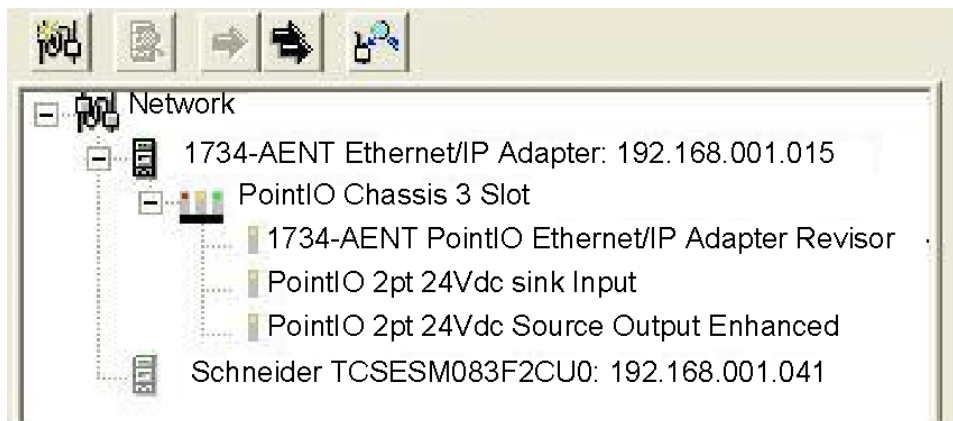
Use Unity Pro's network detection function to automatically detect the TCSESM switch. After it is detected, you can add it to your project.


Note: The TCSESM must be active online with a valid IP address before you can detect and add it to your project.

There are the 3 steps necessary to discover and add a device:

- Go on-line connecting your PC to the network.
- Initiate network detection.
- Select devices you would like to bring into your device from those displayed on your computer.

For more information, refer to the ETC user manual.



- Select the 1734-AENT PointIO Adapter in the Network Detection window.
- Click the Insert in Configuration button  to open the Properties window.

10.3.4 Configuring the TCSESM Switch Properties

The TCSESM switch properties window presents the following tabbed pages. Only some of these pages need to be edited for this example:

In this page...	Do the following...
General	- input device name- configure IP address- add the device to the project configuration
Connections	Accept the default settings.
Online Parameters	Accept the default settings, if any.
Module Information	(Read-only page—no configuration required)
Port Configuration	(Read-only page—no configuration required)
EDS file	(Read-only page—no configuration required)

The following settings were used in the sample configuration:

- Click on the General page:

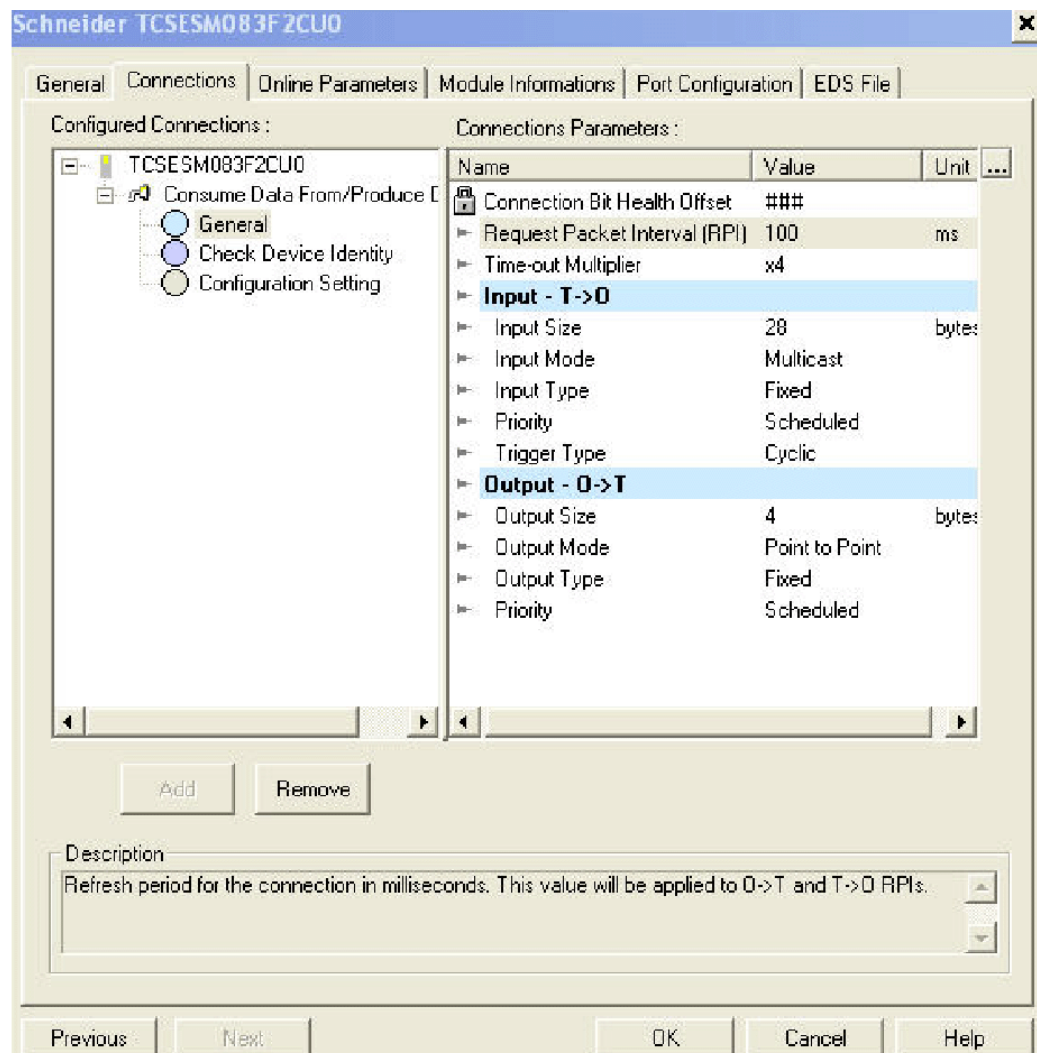
The screenshot shows the configuration window for a Schneider TCSESM083F2CU0 device. The 'General' tab is selected. The 'Device Designation' section contains the following fields: 'Device Name' is 'TCSESM', 'Number' is '041', 'Link Parameters' is unchecked, and 'Active Configuration' is checked. The 'Network Properties' section contains a table with the following data:

Name	Value	Unit
IP Address	192.168.001.041	
DHCP Relation		
Enable DHCP	FALSE	

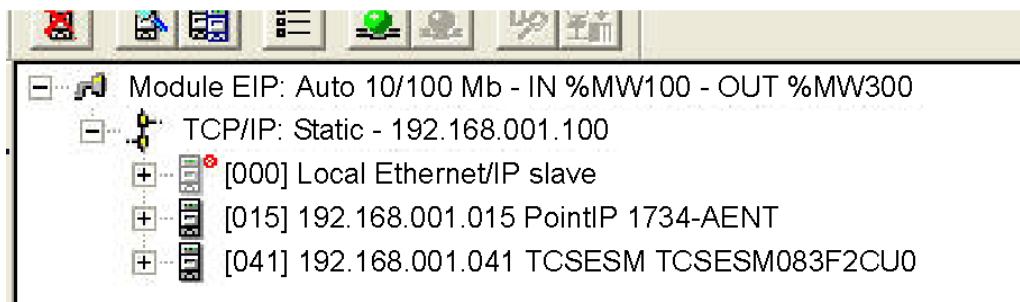
The 'Description' field contains 'IP address of the partner device.' The 'Ping' section has a 'Ping' button, 'Loop' and 'Stop on Error' checkboxes (both unchecked), and a 'Clear' button. The 'Ping Result' field is empty. The window has 'OK', 'Cancel', and 'Help' buttons at the bottom.

- In the General page, edit the following settings:
 - Device Name: TCSESM
 - Number: The sequence of the device in the Devices window. for this example, type in 041.
 - Active Configuration: Be sure this checkbox is selected.
 - IP Adress: 192.168.001.041

- Click on the Connection page:



- Under Configured Connections, select General.
 - Under Connection Parameters, select Request Packet Interval (RPI).
 - Select the value and change it to 100.
 - Click OK to save your settings and close the properties window.
- A node is added to the project configuration in the Devices window:



The next step is to view the remote device's inputs and outputs.

10.3.5 Viewing the TCSESM Switch Data

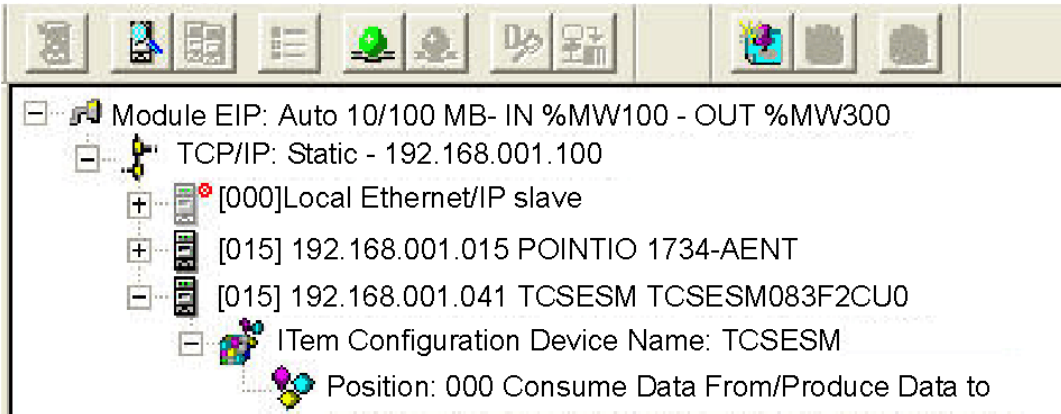
Because the Device Library includes EDS files for the TCSESM switch PointIO adapter and its discrete input and output modules, the Unity Pro EtherNet/IP configuration tool automatically:

- ▶ creates a single rack optimized CIP connection from the TCSESM's EtherNet/IP communication module to the 1734-AENT, and
- ▶ configures each input and output item by assigning:
 - an item name
 - an address location
 - a size allotment based on its data type

Note: In this example, the configuration tool created a single rack optimized connection, which is a more efficient use of CIP connections. A rack optimized connection can be used only with discrete (digital) I/O modules. For analog I/O modules, each analog module must be connected to the TCSESM using a separate connection.

To view the automatically created CIP connection and the I/O items in Unity Pro:

- In the Protocol window, navigate to and select Position: 000 Consume Data From/Produce Data to:



The automatically configured input and output items appear on the right side of the screen in the I/O area (shown below).

- If necessary, use the horizontal scroll bar to scroll to the far right of the input or output area and display the Address column, which identifies the location of the input or output in the TSX ETC xxx:

Input Item Name	Data Type	Offset/Device	Offset/Connection	Position in the Byte	Address
32 Switch_Status	Input dword	0	0		%MW114
32 Link_States	Input dword	4	4		%MW116
32 Link_Admin_Acknowledge	Input dword	8	8		%MW118
32 Utilization_Alarm	Input dword	12	12		%MW120
32 Access_Violation	Input dword	16	16		%MW122
32 Multicast_Connections	Input dword	20	20		%MW124
32 TCP_IP_Connection	Input dword	24	24		%MW126
Output Item Name	Data Type	Offset/Device	Offset/Connection	Position in the Byte	Address
32 Link_Admin_States	Output dword	0	0		%MW306



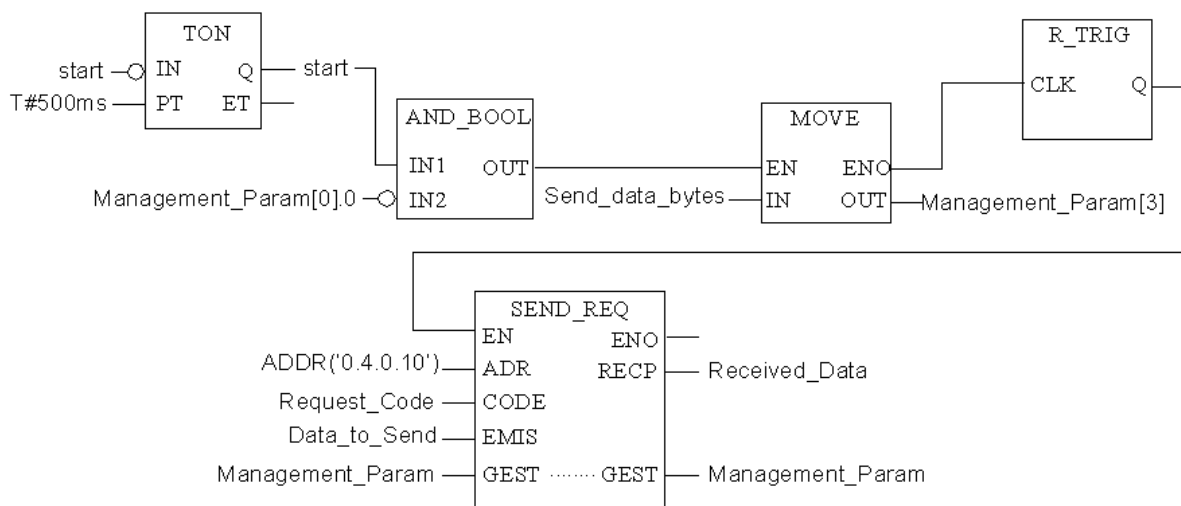
10.3.6 SEND_REQ Example-Get_Attributes_Single

Note: The following unconnected explicit messaging example shows you how to use the SEND_REQ function block to retrieve the switch status (Ethernet Switch Agent Object-Class 149 (hex 95), Instance 1, Attribute ID1)—using the Get_Attributes_Single service.

You can perform the same explicit messaging service using the Online Action window of the Unity Pro EtherNet/IP configuration tool.

■ Implementing the SEND_REQ Function

To implement the SEND_REQ function block, you need to create and assign variables for the following blocks, as follows:



■ Input Variables

Variables need to be created and assigned to input pins. For the purpose of this example, variables have been created—and named—as described below. (You can, of course, use different variable names in your explicit messaging configurations.)

Input pin	Variable	Data Type
IN	Start	BOOL
IN	Send_data_bytes	INT
CODE	Request_Code	INT
EMIS	Data_to_Send	Array [0...4] of 5 INT

Table 29: Input Variables

■ Input/Output Variables

A single variable needs to be created and assigned to the dual input/output GEST pins. For the purpose of this example, a variable has been created—and named—as described below. (You can, of course, use different variable names in your explicit messaging configurations.)

Input pin	Variable	Data Type
GEST	Management_Param	Array [0...3] of 4 INT

Table 30: Input/Output Variables

■ Output Variables

A variable also needs to be created and assigned to the single RECP output pin. (The names assigned to the output variable apply only to this example, and can be changed in your explicit messaging configurations.)

Eingabekontakt	Variable	Datentyp
RECP	Received_Data	Array [0...3] of 4 INT

Table 31: Output Variables

■ **Configuring the Address Input Parameter**

To configure the Address parameter, use the ADDR function to convert a character string to an address, as follows:

▶ ADDR("{network.station} rack.module.channel.destination address")

Note: The parameters {network station} are required only when both the scanner and target devices are part of different networks, but the stations are connected via Fipway network.

The channel parameter value is always 0.

For this example, the Address Input Parameter is: ADDR{0.2.0.41}.

■ **Configuring the Request_Code Variable**

The Request_Code variable identifies the function type for the SEND_REQ function block—in this case, a CIP request:

Variable	Description	Value (hex)
Request_Code	Code identifies a CIP request	16#000E

Table 32: Configuring the Request_Code Variable

■ **Configuring the Data_to_Send Variable**

The Data_to_Send variable identifies the type of explicit message and the CIP request:

Variable	Description	Value (hex)
Data_to_Send[0]	Message type: - 0000 (unconnected), or - 0001 (connected) In this example, unconnected is selected.	16#0000
Data_to_Send[1]	High byte = Request path size (03) Low byte = Service: Get_Attribute_Single (0E)	16#030E
Data_to_Send[2]	High byte = Class (01) Low byte = Class Segment (20)	16#9520
Data_to_Send[3]	High byte = Instance (01) Low byte = Instance Segment (24)	16#0124
Data_to_Send[4]	High byte = Attribute (01) Low byte = Attribute Segment (30)	16#0130

Table 33: Configuring the Data_to_Send Variable

■ **Configuring the Management_Param Variable**

The Management_Param variable manages the explicit message:

Variable	Description	Value (hex)
Management_Param[0]	High byte = Exchange number (managed by system) Low byte = Activity bit (managed by system)	(read-only)
Management_Param[1]	High byte = Operation report Low byte = Communication report	(read-only)
Management_Param[2]	Timeout in ms—0 indicates infinite	16#0000
Management_Param[3]	At input = Length of Data_to_Send variable (in bytes) At output = Length of Received_Data variable (in bytes)	16#000A

Table 34: Configuring the Management_Param Variable

■ **Create and Configure the Send_data_bytes Variable**

The Send_data_bytes variable is used to specify the number of bytes in the explicit message to be sent to the end device. It is copied into the Management_Param(3) variable before the send_req is activated.

For this example the number of bytes is 10 decimal (A hex).

A single variable needs to be created to specify the length of data to send.

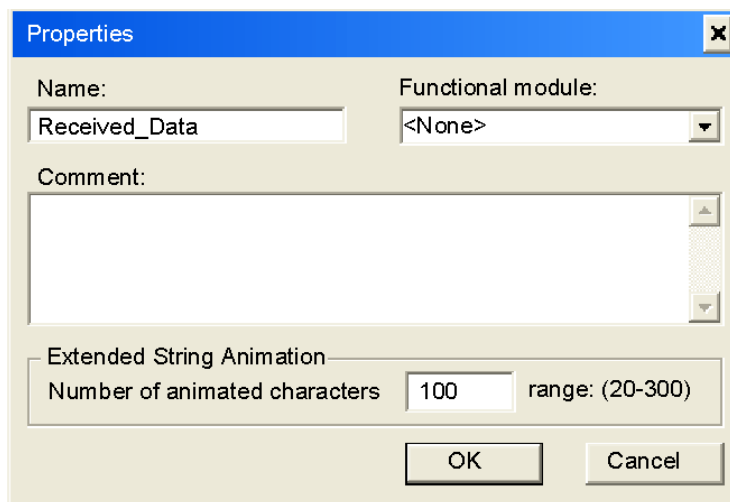
Variable	Description	Value (hex)
Data_to_Send[0]	Message type:- 0000 (unconnected), or- 0001 (connected)In this example, unconnected is selected.	16#0000
Data_to_Send[1]	High byte = Request path size (03) Low byte = Service: Get_Attribute_Single (0E)	16#030E
Data_to_Send[2]	High byte = Class (01) Low byte = Class Segment (20)	16#9520
Data_to_Send[3]	High byte = Instance (01) Low byte = Instance Segment (24)	16#0124
Data_to_Send[4]	High byte = Attribute (01) Low byte = Attribute Segment (30)	16#0130

Table 35: Create and Configure the Send_data_bytes Variable

■ Viewing the Response

Use a Unity Pro Animation table to display the Received_Data variable array. The Received_Data variable array consists of the entire data buffer. To display the CIP response, follow these steps:

- In Unity Pro, select `Tools:Project Browser` to open the Project Browser.
- In the Project Browser, select the Animation Tables folder, then click the right mouse button.
A pop-up menu appears.
- Select New Animation Table in the pop-up menu.
A new animation table and its Properties dialog both open.
- In the Properties dialog, edit the following values:
 - Type in a table name. For this example: Received_Data.
 - Functional module: Accept the default <None>.
 - Comment: (Optional) Type your comment here.
 - Number of animated characters: Type in 100, representing the size of the data buffer in words.
- The completed Properties dialog looks like this:



Click OK to close the dialog.

- In the animation table's Name column, type in the name of the variable assigned to the databuffer, Received_Data, and press Enter. The animation table displays the Received_Data variable.

- Expand the Received_Data variable to display its word array, where you can view the CIP response at Received_Data(0-4):

Name	Value	Type	Comment
Received_Data		ARRAY[0..10] OF INT	
Received_Data[0]	16#008E	INT	
Received_Data[1]	0	INT	
Received_Data[2]	2#0000_1000_0000_0011	INT	
Received_Data[3]	0	INT	
Received_Data[4]	0	INT	
Received_Data[5]	0	INT	
Received_Data[6]	0	INT	
Received_Data[7]	0	INT	
Received_Data[8]	0	INT	
Received_Data[9]	0	INT	
Received_Data[10]	0	INT	

Note: Each array entry presents 2 bytes of data in the byte order 'LSB first, followed by MSB', where the least significant byte (LSB) is stored in the smallest memory address. For example, '8E' in word[0] is the lower byte, and '00' is the upper byte.

In the above figure, the Received_Data(2) variable shows the Ethernet Switch Agent Object (class 149, instance 1, attribute 1) Switch Status.

For this example the hex value 0803 translates to the following:

- ▶ Bit 0 = 1 Overall State Inoperative
- ▶ Bit 1 = 1 Power Supply 1 Inoperative (as previously noted, only Power Supply 2 is connected)
- ▶ Bit 11 = 1 Signal Contact Open

10.4 TCSESM in a Quantum System

This section describes the configuration of a TCSESM switch as an EtherNet/IP adapter in a Quantum system using Unity Pro software. The addition of the EtherNet/IP function to Schneider's Connexium Managed Switch product line allows the ESM to be configured as an EtherNet/IP adapter in a Quantum system using a 140 NOC 771 xxx EtherNet/IP module. An example of such an arrangement is described below.

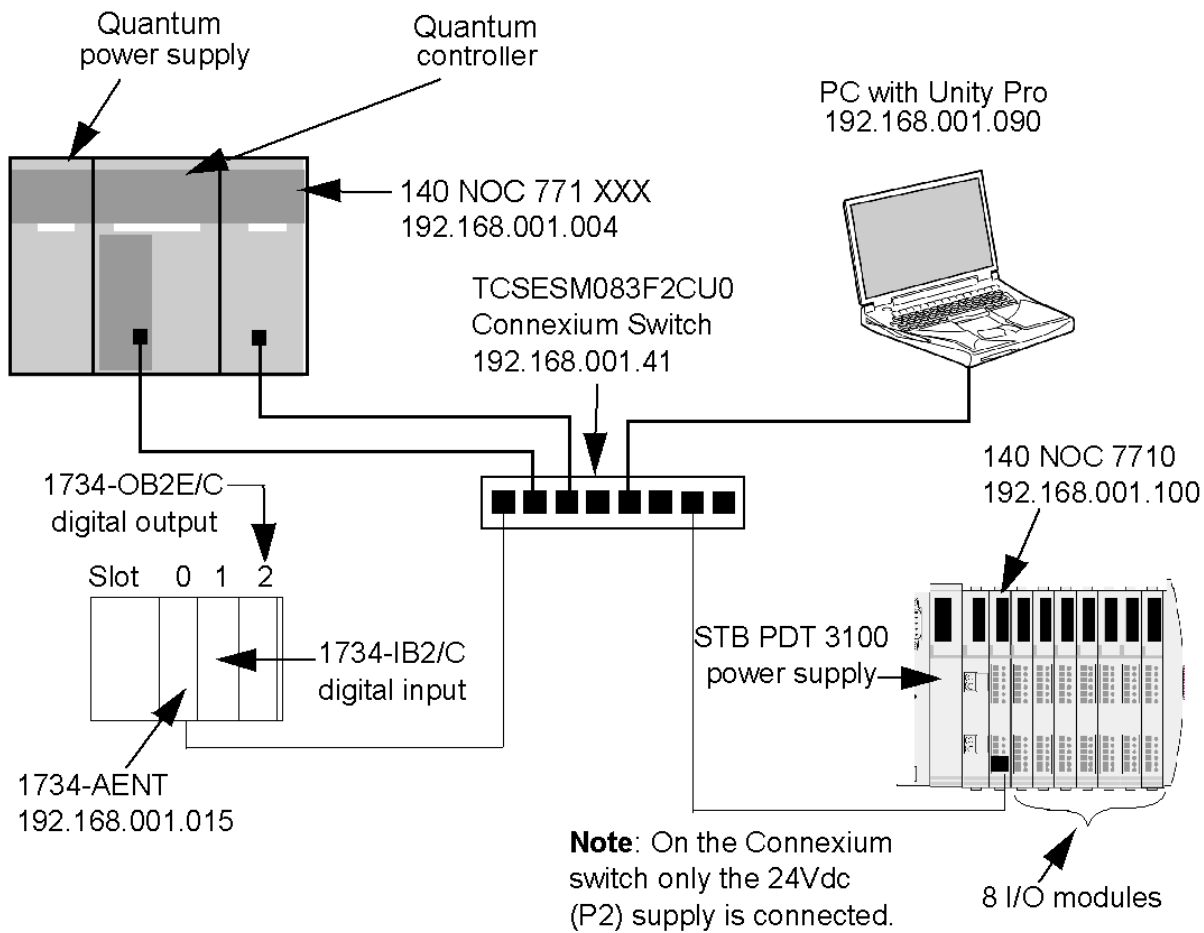


Figure 53: Required hardware and the connections involved to develop a network topology

To re-create this example, be sure to:

- ▶ use the IP addresses for your own configurations
 - PC
 - STB NIC 2212 EtherNet/IP network interface module
 - 1734-AENT PointIO adapter
 - 140 NOC 771 xxx Ethernet communication module
- ▶ check all wiring

Note: Unity Pro software running in the PC is used to configure the Quantum controller. In this example, the PC is indirectly connected to the controller CPU's Ethernet port via the Ethernet switch. Alternatively, you could bypass the switch and directly connect the PC to another one of the controller CPU's ports.

Refer to the Quantum 140 NOC 771 xxx Communication Module User Manual (31008209) for complete details on configuring a Quantum Ethernet system.

10.4.1 Adding EDS Files

Before the TCSESM switch can be configured in a Quantum system, the TCSESM EDS file has to be added to the Unity Pro EtherNet/IP Device Library. Unity Pro includes an EDS Management wizard that you can use to add one or more EDS files to the Device Library.

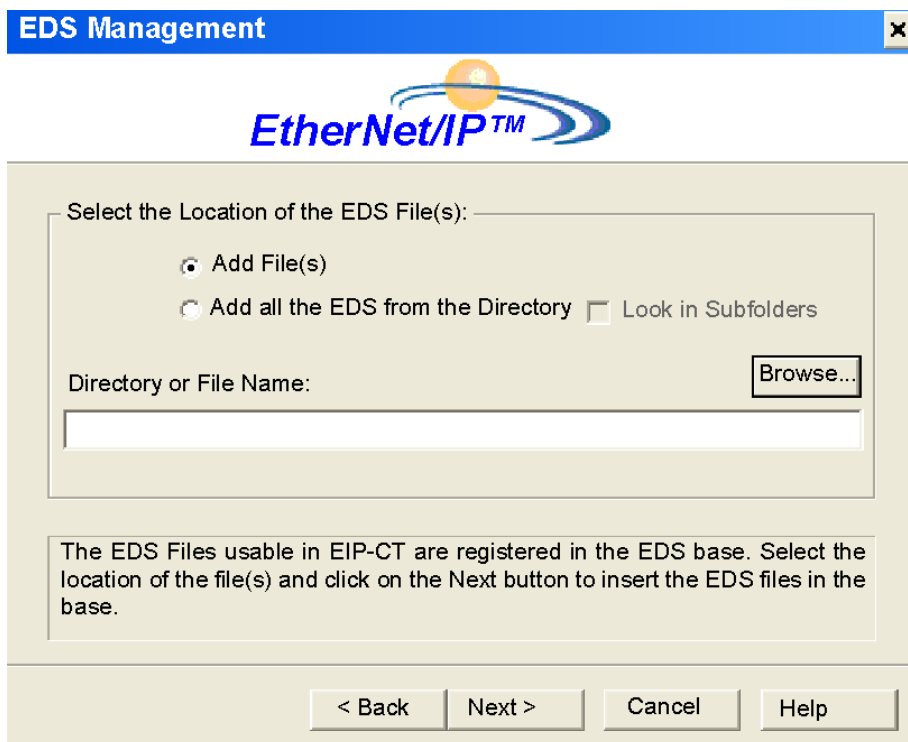
The wizard presents a series of instruction screens that:

- ▶ simplify the process of adding EDS files to the Device Library, and
- ▶ provide a redundancy check in case you attempt to add duplicate EDS files to the Device Library

Note: During the following procedure, you can select `Devices:Options...` to open the Display Options window, where you can enable/disable messages indicating the EDS file you are adding is a duplicate—or a different version—of an existing EDS file.

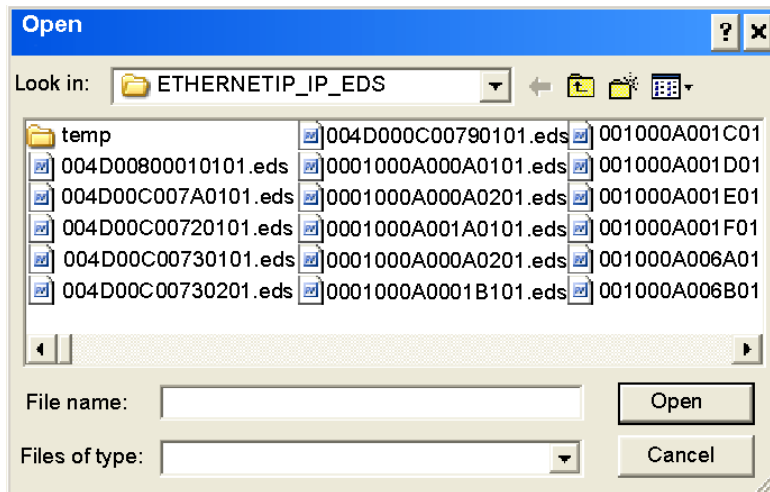
10.4.2 Adding one or more EDS files to the Device Library

- Open the Unity project with NOC configured.
- Open the NOC module configuration window.
- Add the switch's EDS file to the device library (for more information, refer to technical publications for PLC Ethernet module).
Page 1 of the wizard opens.
- Click Next.
Page 2 of the wizard opens.



- In the Select the Location of the EDS File(s) section, select either:

- Add File(s), to add one or more EDS files you will individually select, or
 - Add all the EDS Files from the Directory, to add all files from a folder you will select.
 - Select Look in Subfolders to add EDS files in subfolders beneath the folder you select
- Click the Browse button.
The Open dialog opens.



- Use the Open dialog to navigate to and select:
 - one or more EDS files, or
 - a folder containing EDS files
- After you have made your selection(s), click Open.
The dialog closes and your selection appears in the Directory or File Name field.
- Click Next.
The wizard compares the selected EDS files against existing files in the Device Library.
- (Conditional) If one or more selected EDS files are duplicates and if notice of redundant files is enabled in the Display Options dialog, a File Already Exists message displays.
Close the message.
- Page 3 of the wizard opens indicating the Status of each device you attempted to add:
 - a green check mark indicates the EDS file can be added
 - a blue informational icon indicates a redundant file
 - a red check mark indicates an invalid EDS file
 (Optional) Select a file in the list, then click View Selected File to open it.
- Click Next to add the nonduplicate files.
Page 4 of the wizard opens, indicating the action is complete.

- Click Finish to close the wizard.
The device(s) you added can now be inserted into your EtherNet/IP configuration.

10.4.3 Automatically Detect and Add the TCSESM Switch

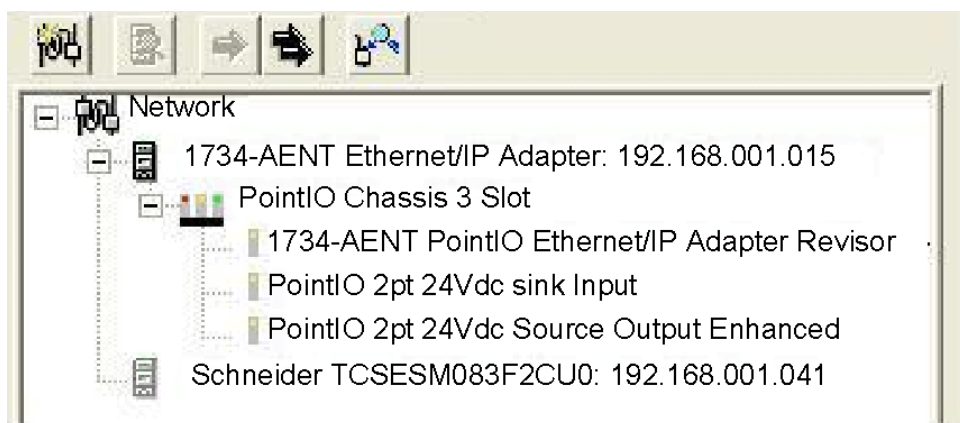
Use Unity Pro's network detection function to automatically detect the TCSESM switch. After it is detected, you can add it to your project.


Note: The TCSESM must be active online with a valid IP address before you can detect and add it to your project.

There are the 3 steps necessary to discover and add a device:

- Go on-line connecting your PC to the network.
- Initiate network detection.
- Select devices you would like to bring into your device from those displayed on your computer.

For more information, refer to the user manual for the PLC Ethernet Module.



- Select the 1734-AENT PointIO Adapter in the Network Detection window.
- Click the Insert in Configuration button  to open the Properties window.

10.4.4 Configuring the TCSESM Switch Properties

The TCSESM switch properties window presents the following tabbed pages. Only some of these pages need to be edited for this example:

In this page...	Do the following...
General	- input device name- configure IP address- add the device to the project configuration
Connections	Accept the default settings.
Online Parameters	Accept the default settings, if any.
Module Information	(Read-only page—no configuration required)
Port Configuration	(Read-only page—no configuration required)
EDS file	(Read-only page—no configuration required)

The following settings were used in the sample configuration:

- Click on the General page:

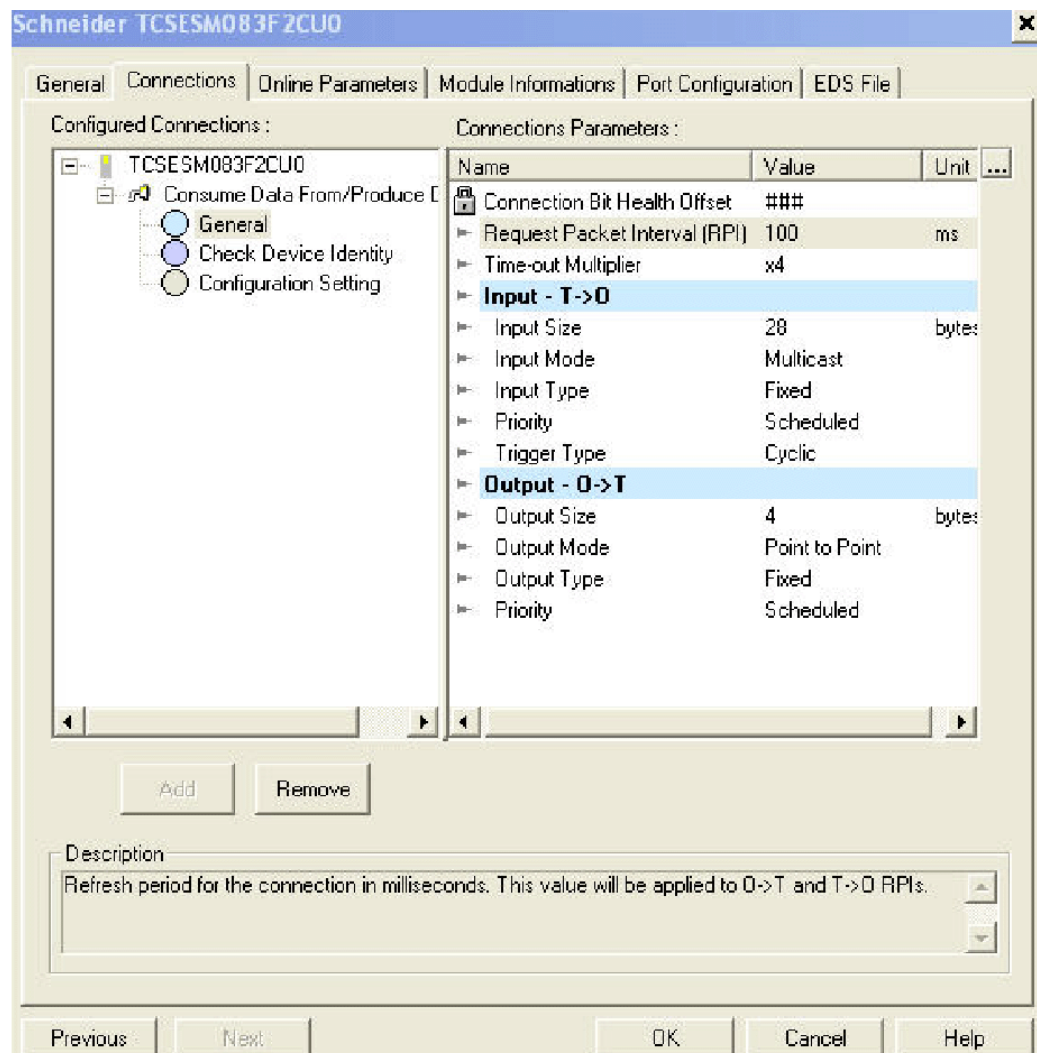
The screenshot shows the configuration window for a Schneider TCSESM083F2CU0 device. The 'General' tab is selected. The 'Device Designation' section includes a text field for 'Device Name' containing 'TCSESM', a dropdown for 'Number' set to '041', a checkbox for 'Link Parameters' which is unchecked, and a checked checkbox for 'Active Configuration'. A 'Comment' text area is empty. The 'Network Properties' section contains a table with the following data:

Name	Value	Unit
IP Address	192.168.001.041	
DHCP Relation		
Enable DHCP	FALSE	

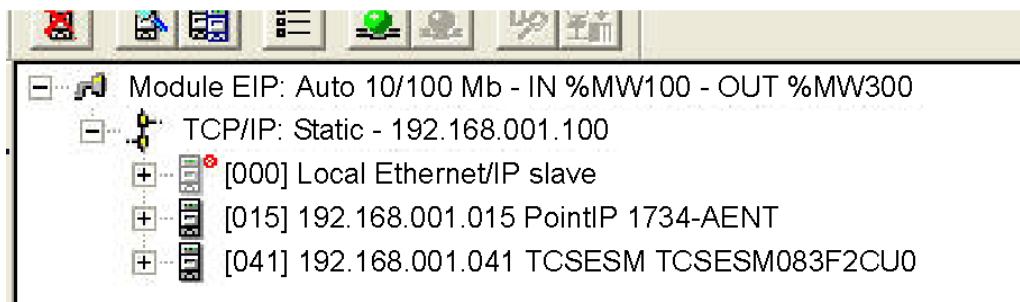
Below the table is a 'Description' text area containing 'IP address of the partner device.'. The 'Ping' section has a 'Ping' button, two unchecked checkboxes for 'Loop' and 'Stop on Error', and a 'Clear' button. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

- In the General page, edit the following settings:
 - Device Name: TCSESM
 - Number: The sequence of the device in the Devices window. for this example, type in 041.
 - Active Configuration: Be sure this checkbox is selected.
 - IP Adress: 192.168.001.041

- Click on the Connection page:



- Under Configured Connections, select General.
 - Under Connection Parameters, select Request Packet Interval (RPI).
 - Select the value and change it to 100.
 - Click OK to save your settings and close the properties window.
- A node is added to the project configuration in the Devices window:



The next step is to view the remote device's inputs and outputs.

10.4.5 Viewing the TCSESM Switch Data

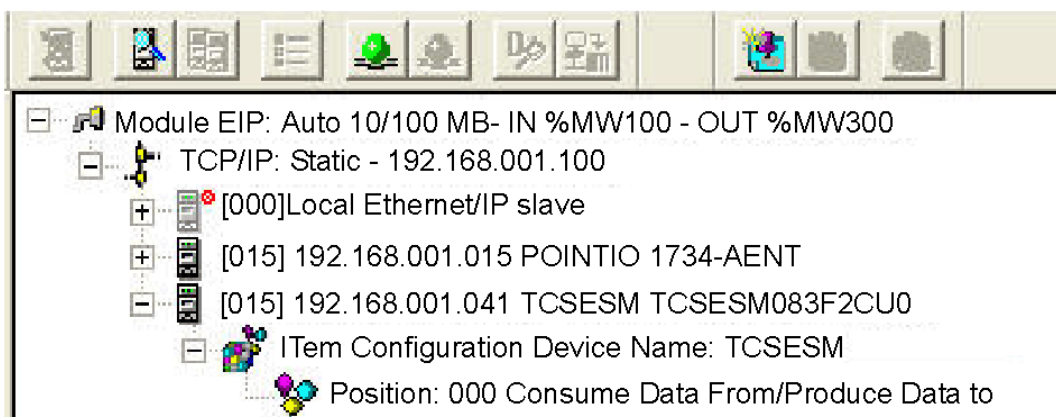
Because the Device Library includes EDS files for the TCSESM switch PointIO adapter and its discrete input and output modules, the Unity Pro EtherNet/IP configuration tool automatically:

- ▶ creates a single rack optimized CIP connection from the TCSESM's EtherNet/IP communication module to the 1734-AENT, and
- ▶ configures each input and output item by assigning:
 - an item name
 - an address location
 - a size allotment based on its data type

Note: In this example, the configuration tool created a single rack optimized connection, which is a more efficient use of CIP connections. A rack optimized connection can be used only with discrete (digital) I/O modules. For analog I/O modules, each analog module must be connected to the TCSESM using a separate connection.

To view the automatically created CIP connection and the I/O items in Unity Pro:

- In the Protocol window, navigate to and select Position: 000 Consume Data From/Produce Data to:



The automatically configured input and output items appear on the right side of the screen in the I/O area (shown below).

- If necessary, use the horizontal scroll bar to scroll to the far right of the input or output area and display the Address column, which identifies the location of the input or output in the NOC 771 xxx:

Input Item Name	Data Type	Offset/Device	Offset/Connection	Position in the Byte	Address
Switch_Status	Input dword	0	0		%MW114
Link_States	Input dword	4	4		%MW116
Link_Admin_Acknowledge	Input dword	8	8		%MW118
Utilization_Alarm	Input dword	12	12		%MW120
Access_Violation	Input dword	16	16		%MW122
Multicast_Connections	Input dword	20	20		%MW124
TCP_IP_Connection	Input dword	24	24		%MW126
Output Item Name	Data Type	Offset/Device	Offset/Connection	Position in the Byte	Address
Link_Admin_States	Output dword	0	0		%MW306

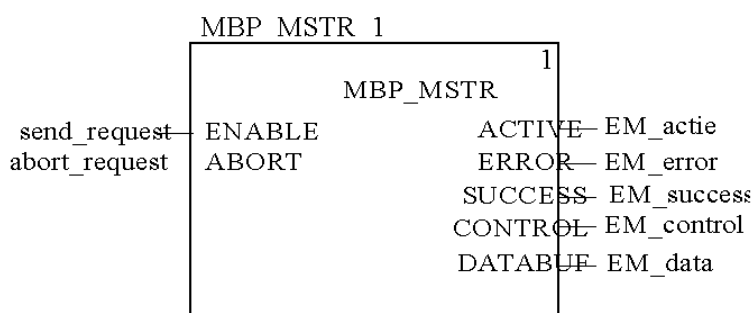
10.4.6 MPB_MSTR Example-Get_Attributes_Single

The following unconnected explicit messaging example shows you how to use the MBP_MSTR function block to retrieve the switch status [Ethernet Switch Agent Object-Class 149 (hex 95), Instance 1, Attribute ID1] module, using the Get_Attributes_Single service.

You can perform the same explicit messaging service using the Online Action window of the Unity Pro EtherNet/IP configuration tool.

■ Implementing the MBP_MSTR Function Block

To implement the MBP_MSTR function block, you need to create and assign variables for the following blocks, as follows:



■ Input Variables

Variables need to be created and assigned to input pins. For the purpose of this example, variables have been created—and named—as described below. (You can, of course, use different variable names in your explicit messaging configurations.)

Input Pin	Variable	Data Type
ENABLE	send_request	BOOL
ABORT	abort_request	IBOOL

Table 36: Input Variables

■ Output Variables

A variable also needs to be created and assigned to output pins. (The names assigned to the output variable apply only to this example, and can be changed in your explicit messaging configurations.)

Output Pin	Variable	Data Type	Address
ACTIVE	EM_active	BOOL	
ERROR	EM_Error	BOOL	
SUCCESS	EM_Success	BOOL	
COLTROL	EM_Control	Array of 9 words	% MW500
DATABUF	EM_Data	Array of 100 words	% MW600

Table 37: Output Variables

■ Control Array

The control array parameter (EM_control) consists of 9 contiguous words. You need to configure only some control words; other control words are read-only and are written to by the operation. In this example, the control array defines the operation as an unconnected explicit message, and identifies the target device.

Register	Description	Configure	Setting (hex)
CONTROL [0]	Operation: Low byte = OE (CIP explicit message) High byte = - 00 (unconnected), or - 01 (connected)	Yes	16#000E (unconnected)
CONTROL [1]	Status: read-only (written by operation).	No	—
CONTROL [2]	Data buffer length = 100 words	Yes	16#0004
CONTROL [3]	Response offset: offset—in words—for the beginning of the explicit message response in the databuffer	Yes	16#0004
CONTROL [4]	High byte = slot location	Yes	16#0004
CONTROL [5]	Device number: from the Devices window of the Unity Pro EtherNet/IP configuration tool	Yes	16#0029
CONTROL [6]	CIP request length (in bytes)	Yes	16#0008
CONTROL [7]	Length of received response (written by operation)	No	—
CONTROL [8]	(Reserved)	No	—

Table 38: Control Array

■ Configuring the Management_Param Variable

The Management_Param variable manages the explicit message:

Variable	Description	Value (hex)
Management_Param[0]	High byte = Exchange number (managed by system) Low byte = Activity bit (managed by system)	(read-only)
Management_Param[1]	High byte = Operation report Low byte = Communication report	(read-only)
Management_Param[2]	Timeout in ms—0 indicates infinite	16#0000
Management_Param[3]	At input = Length of Data_to_Send variable (in bytes) At output = Length of Received_Data variable (in bytes)	16#000A

Table 39: Configuring the Management_Param Variable

■ CIP Request

The CIP request is located at the beginning of the databuffer and is followed by the CIP response. In this example, the CIP request calls for the return of a single attribute value (switch state), and describes the request path through the target device's object structure leading to the target attribute:.

Request Word	High Byte		Low Byte	
	Description	Value (hex)	Description	Value (hex)
1	Request path size (in words)	16#03	EM Service: Get_Attributes_Single	16#0E
2	Request path: class assembly object	16#95	Request path: logical class segment	16#20
3	Request path: Instance	16#01	Request path: logical instance segment	16#24
4	Request path: attribute	16#01	Request path: logical attribute segment	16#30

Table 40: CIP Request

Combining the high and low bytes, above, the CIP request would look like this:

Request word	Value
1	16#030E
2	16#9520
3	16#0124
4	16#0130

Table 41: CIP Request: Combination of high and low bytes

■ Viewing the Response

Use a Unity Pro Animation table to display the Received_Data variable array. The Received_Data variable array consists of the entire data buffer, which includes:

- ▶ CIP request (4 words) located in EM_data(1-4)
- ▶ CIP service type (1 word) located in EM_data(5)
- ▶ CIP request status (1 word) located in EM_data(6)
- ▶ CIP response (in this case, 10 words) located in EM_data(7-16)

To display the CIP response, follow these steps:

- In Unity Pro, select `Tools:Project Browser` to open the Project Browser.
- In the Project Browser, select the Animation Tables folder, then click the right mouse button.
A pop-up menu appears.
- Select New Animation Table in the pop-up menu.
A new animation table and its Properties dialog both open.
- In the Properties dialog, edit the following values:
 - Type in a table name. For this example: Received_Data.
 - Functional module: Accept the default <None>.
 - Comment: (Optional) Type your comment here.
 - Number of animated characters: Type in 100, representing the size of the data buffer in words.

- The completed Properties dialog looks like this:

Properties

Name: Received_Data Functional module: <None>

Comment:

Extended String Animation
Number of animated characters: 100 range: (20-300)

OK Cancel

Click OK to close the dialog.

- In the animation table's Name column, type in the name of the variable assigned to the databuffer, Received_Data, and press Enter. The animation table displays the Received_Data variable.
- Expand the Received_Data variable to display its word array, where you can view the CIP response at Received_Data(0-4):

Name	Value	Type	Comment	Address
EM_data		ARRAY[0..99] OF WORD		%MW600
EM_data[0]	16#030E	WORD		%MW600
EM_data[1]	16#9520	WORD		%MW601
EM_data[2]	16#0124	WORD		%MW602
EM_data[3]	16#0130	WORD		%MW603
EM_data[4]	16#008E	WORD		%MW604
EM_data[5]	0	WORD		%MW605
EM_data[6]	16#0803	WORD		%MW606
EM_data[7]	0	WORD		%MW607
EM_data[8]	0	WORD		%MW608
EM_data[9]	0	WORD		%MW609
EM_data[10]	0	WORD		%MW610
EM_data[11]	0	WORD		%MW611
EM_data[12]	0	WORD		%MW612
EM_data[13]	0	WORD		%MW613
EM_data[14]	0	WORD		%MW614

Note: Each array entry presents 2 bytes of data in the byte order 'LSB first, followed by MSB', where the least significant byte (LSB) is stored in the smallest memory address. For example, '8E' in word[0] is the lower byte, and '00' is the upper byte.

In the above figure, the EM_data(6) variable shows the Ethernet Switch Agent Object (class 149), instance 1, attribute 1) Switch Status.

For this example the hex value 0803 translates to the following:

- ▶ Bit 0 = 1 Overall State Inoperative
- ▶ Bit 1 = 1 Power Supply 1 Inoperative (as previously noted, only Power Supply 2 is connected)
- ▶ Bit 11 - 1 Signal Contact Open

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. 54](#)) and whether the status of this process is "IW":

SunOS

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

HP

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

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

SunOS

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

HP

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

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

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

Special steps for HP workstations:

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

For example:

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

tftp user ID

* is in the password field

510 sample user ID

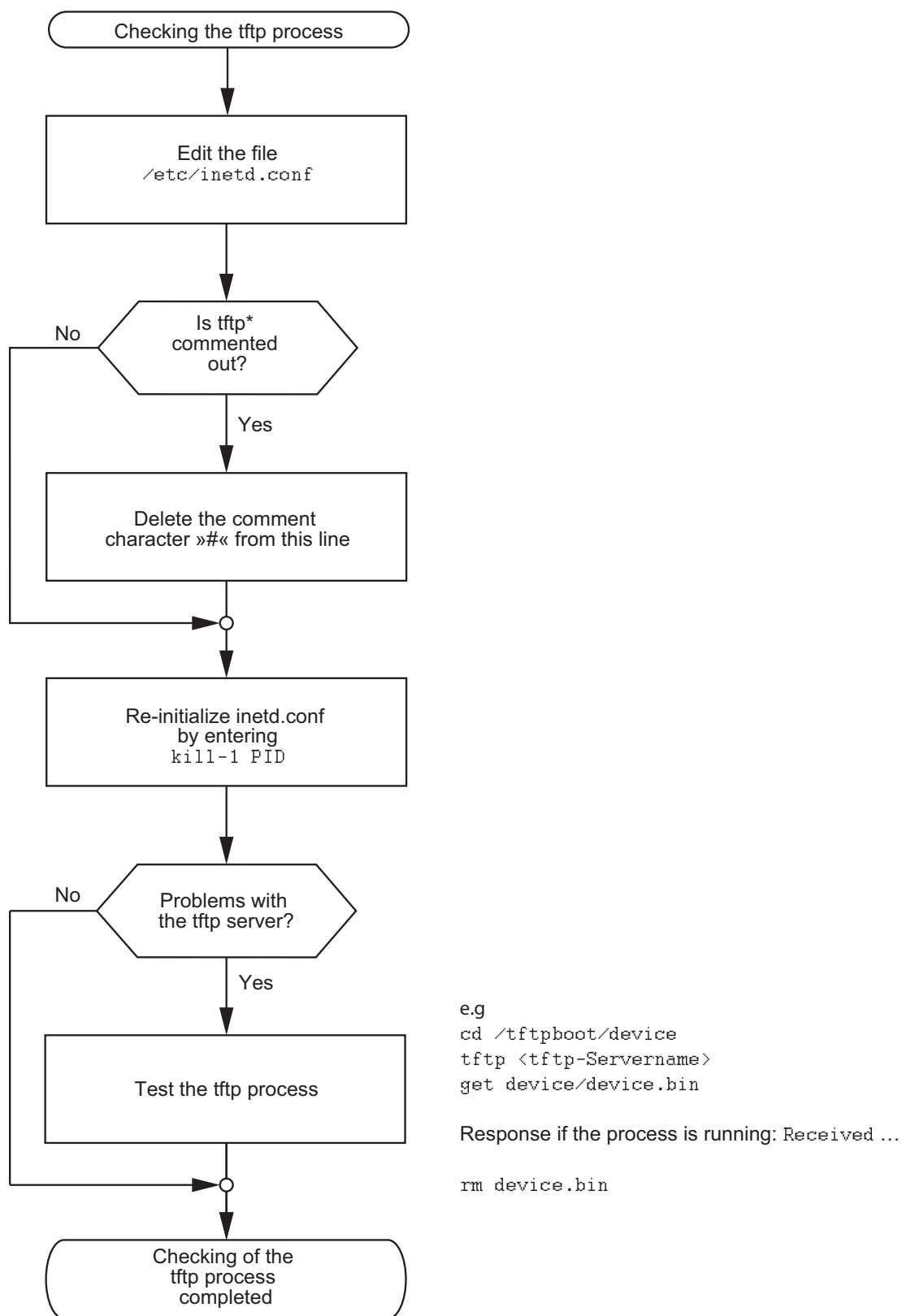
20 sample group number

tftp server any meaningful name

/bin/false mandatory entry (login shell)

- Test the tftp process with, for example:

```
cd /tftpboot/device
tftp <tftp server name> get device/device.bin
rm device.bin
```



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

Figure 54: Flow Chart for TFTP Server Setup with SunOS or 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 42: 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
BOOTP	Bootstrap Protocol
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
FDB	Forwarding Database
GARP	General Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocol
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocol
F/O	Optical Fiber
MAC	Media Access Control
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 „Reference Manual Web-based Interface“.

C Index

A			
Access	154	Device Status	155, 158
Access rights	76	Device status	155
Access security	73	DHCP	29, 50, 53, 60
ACD	171	DHCP Client	50
Address conflict	171	DHCP Option 82	53
Address Conflict Detection	171	DHCP server	88
Address table	101	Differentiated Services	122
AF	123	DiffServ	118
Aging time	101, 107	DiffServ Code Point	122
Alarm	153	DSCP	122, 125, 127, 128
Alarm messages	152	Dynamic	102
APNIC	31	E	
ARIN	31	EAM	43, 60
ARP	35	EDS	179
Assured Forwarding	123	EF	122
Authentication	154	Ethernet Switch Configurator Software	40, 81
Automatic configuration	73	Expedited Forwarding	122
B		F	
Bandwidth	105, 130	Faulty device replacement	57
Booting	20	FDB	102
BOOTP	29, 51, 60	Filter	102
Broadcast	93, 100, 102, 105	Filter table	102, 108
Browser	25	First installation	29
C		Flash memory	64
CIDR	36	Flow control	130
CIP	177	Forwarding database	102
Class Selector	122	G	
Classless Inter Domain Routing	36	GARP	108
Classless Inter-Domain Routing	35	Gateway	32, 38
CLI	77	GMRP	105, 108
Clock	95	GMRP per Port	114
Clock synchronization	97	Grandmaster	95
Closed circuit	158	H	
Command Line Interface	22	Hardware address	46
Common Industrial Protocol	177	Hardware reset	152
Configuration	64	HIPER-Ring	154
Configuration changes	152	Host address	32
Configuration data	45, 53, 62, 65	I	
Configuration file	50, 61	IANA	31
Connection error	74	Icon	179
D		IEEE 1588 time	88
Data transfer parameter	20	IEEE 802.1 Q	119
Destination address	102, 103, 108	IEEE MAC address	167
Destination address field	100	IGMP	107
Destination port	175	IGMP Querier	110
Destination table	152		

IGMP Snooping	105, 107, 179	Priority	119, 125
in-band	22	Priority queues	118
Internet Assigned Numbers Authority	31	Priority tagged frames	119
Internet service provider	31	PTP	87, 88, 95
IP Address	50	Q	
IP address	31, 38, 46, 171	QoS	118
IP header	118, 121, 122	Query	107
IP Parameter	29	Query function	110
IP Parameters (device network settings)	55	Queue	126
ISO/OSI layer model	35		
J		R	
Java	26	Rate Limiter settings	116
Java Runtime Environment	25	Read access	27
JavaScript	26	Real time	87, 118
L		Receiving port	103
LACNIC	31	Redundancy	13
Leave	107	Reference clock	88, 91, 95
Link monitoring	155, 158	Relay contact	158
LLDP	169	Remote diagnostics	158
Local clock	96	Report	107, 174
Login	26	Request interval (SNTP)	93
M		Ring manager	102
MAC destination address	35	Ring/Network Coupling	154
Memory Backup Adapter	43	RIPE NCC	31
Message	152	RMON probe	175
Multicast	93, 102, 105, 107	Router	32
Multicast address	108	S	
N		Segmentation	152
Netmask	32, 38	Service	174
Network address	31	Service provider	31
Network topology	53	Signal contact	74, 154, 158
NTP	90	Signal runtime	91
O		Simple Network Time Protocol	87
ODVA	177	SNMP	25, 76, 77, 152
Operating mode	73	SNTP	87
Operation monitoring	158	SNTP client	90, 92
Option 82	30, 53	SNTP request	92
out-of-band	22	SNTP server	90, 92
Overload protection	130	Software	228
P		Software release	69
Password	23, 27, 66, 77, 78	Source address	100
PHB	122	Source port	175
Polling	152	State on deliver	64
Port configuration	73	State on delivery	64, 76
Port mirroring	175	Static	102
Port priority	125	Strict Priority	125, 126
Precedence	122	Subnetwork	38, 101
Precision Time Protocol	87, 95	Summer time	88
		Supply voltage	154
		Symbol	15
		System Monitor	20
		System Name	50

Index

System name 50
System time 91, 93

T

TCP/IP 177
TCP/IP stack 225
Telnet 22
tftp 224
tftp update 71
Time difference 88
Time management 95
Time zone 88
Topology 53, 169
ToS 118, 121, 122
Traffic class 125, 127
Traffic classes 118
Transmission reliability 152
Trap 152, 153
Trap Destination Table 152
Trivial File Transfer Protocol 224
trust dot1p 125
trust ip-dscp 125
Type field 119
Type of Service 121

U

UDP/IP 177
Unicast 105
Universal Time Coordinated 90
untrusted 125
Update 20
User name 23
UTC 88, 90

V

V.24 22
Video 126
VLAN 119, 125, 133
VLAN ID (device network settings) 55
VLAN priority 127
VLAN tag 119, 133
VoIP 126

W

Web-based Interface 25
Web-based interface 25
Web-based management 26
Website 27
Winter time 88
Write access 27

