ConneXium

TCSESM, TCSESM-E Managed Switch
Basic Configuration User Manual

31007122.08

www.schneider-electric.com

Schneider Electric

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein. This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Schneider Electric nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

You agree not to reproduce, other than for your own personal, noncommercial use, all or part of this document on any medium whatsoever without permission of Schneider Electric, given in writing. You also agree not to establish any hypertext links to this document or its content. Schneider Electric does not grant any right or license for the personal and noncommercial use of the document or its content, except for a non-exclusive license to consult it on an "as is" basis, at your own risk. All other rights are reserved.

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

When devices are used for applications with technical safety requirements, the relevant instructions must be followed.

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

Failure to observe this information can result in injury or equipment damage.

31007122 - 03/2018

Contents

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.

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	Reference Number
ConneXium TCSESM, TCSESM-E Managed Switch Redundancy Configuration User Manual	31007126
ConneXium TCSESM, TCSESM-E Managed Switch Basic Configuration User Manual	31007122
ConneXium TCSESM, TCSESM-E Managed Switch Command Line Interface Reference Manual	31007130
ConneXium TCSESM, TCSESM-E Managed Switch Web-based Interface Reference Manual	EIO0000000482
ConneXium TCSESM Managed Switch Installation Manual	31007118
ConneXium TCSESM-E Extended Managed Switch Installation Manual	EIO0000000529

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

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

The following thematic sequence has proven itself in practice:

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

- Function diagnosis
- Store the newly created configuration to nonvolatile memory

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

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

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

The “Command Line Interface” Reference Manual contains detailed information on using the Command Line Interface to operate the individual functions of the device.

Key

The designations used in this manual have the following meanings:

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

Execution in the Web-based Interface user interface

Execution in the Command Line Interface user interface

Symbols used:

	WLAN access point
	Router with firewall
	Switch with firewall
	Router
	Switch

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

Introduction

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

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

1 Access to the user interfaces

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

- System monitor via the V.24 interface (out-of-band)
- Command Line Interface (CLI) via the V.24 connection (out-of-band) 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: L2S-09.0.00 (2018-01-24 09:09))

   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)
- 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) 2004-2010 Schneider Electric

                             All rights reserved

                          TCSESM-E Release L2S-09.0.00

                          (Build date 2018-01-24 12:13)



                         System Name:  TCSESM063F2CU1
                         Mgmt-IP    :  10.0.1.105
                         Base-MAC   :  00:80:63:51:74:00
                         System Time:  2018-01-24 13:14:15


User:
```

Figure 3: Logging in to the Command Line Interface program

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

The start screen appears.

Note: For a TCSESM Switch, the preset 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 Java software 8 (“Java™ Runtime Environment Version 1.8.x”).

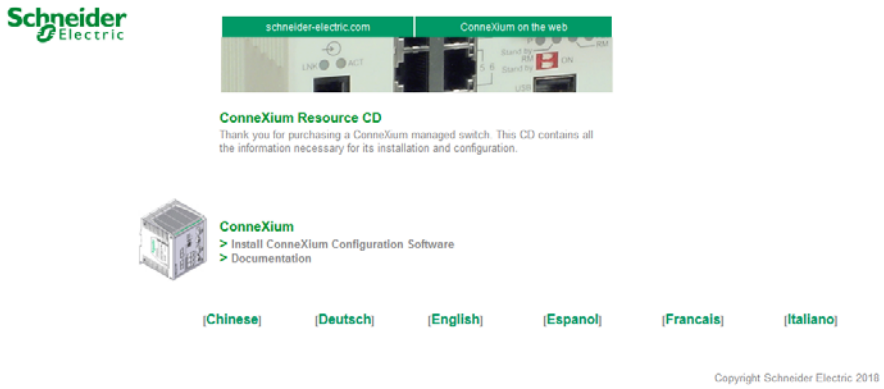


Figure 5: Installing Java

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

The login window appears on the screen.

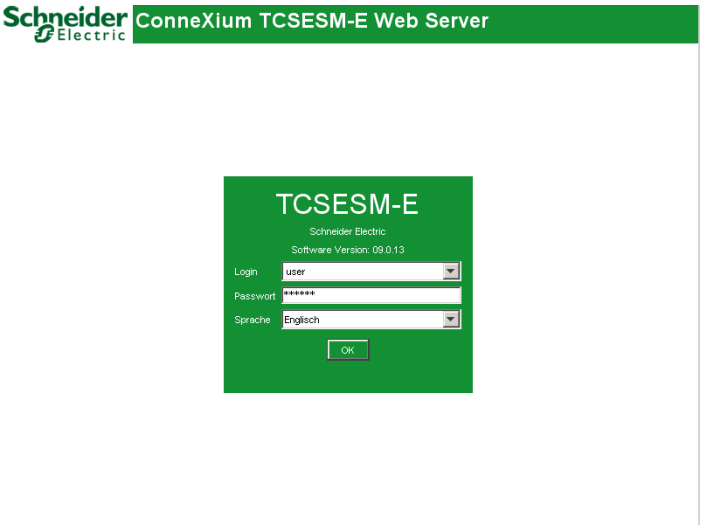


Figure 6: Login window

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

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

The website of the device appears on the screen.

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

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

2 Entering the IP Parameters

When you install the device for the first time enter the IP parameters.

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 on page 37 “Entering IP parameters via CLI”).
- Entry using the Ethernet Switch Configurator 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 on page 40 “Entering the IP Parameters via Ethernet Switch Configurator”).
- 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 on 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 on 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 on 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 on 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-Sahara Africa
- LACNIC (Regional Latin-American and Caribbean IP Address Registry) – Latin America and some Caribbean Islands
- RIPE NCC (Réseaux IP Européens) - Europe and Surrounding Regions

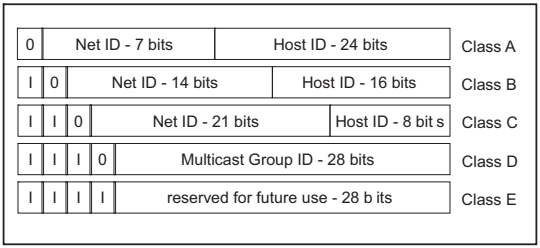


Figure 7: Bit representation of the IP address

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

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

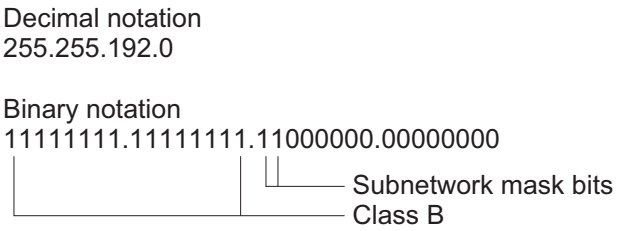
2.1.2 Netmask

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

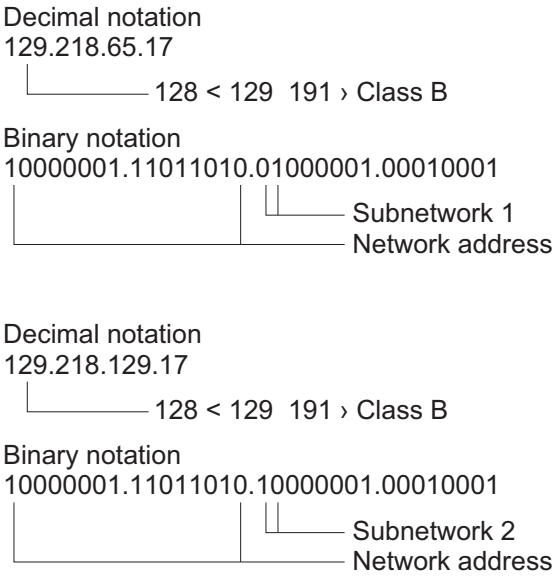
The division into subnetworks with the aid of the netmask is performed in much the same way as the division of the network addresses (net id) into classes A to C.

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

Example of a netmask:



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



Example of how the network mask is used

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

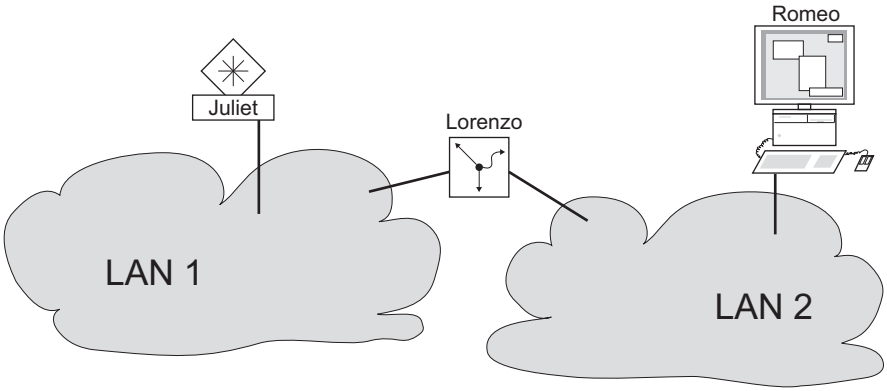


Figure 8: Management agent that is separated from its management station by a router

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

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

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

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

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

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

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

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

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

2.1.3 Classless Inter-Domain Routing

Class C with a maximum of 254 addresses was too small, and class B with a maximum of 65,534 addresses was too large for most users. 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. 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, binary
149.218.112.1	255.255.255.128	10010101 11011010 01110000 00000001
149.218.112.127		10010101 11011010 01110000 01111111

25 mask bits

CIDR notation: 149.218.112.0/25

Mask bits

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

2.2 Entering IP parameters via CLI

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

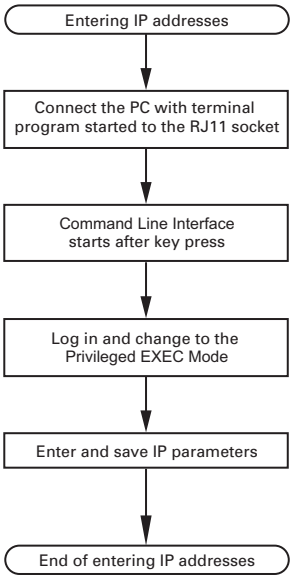


Figure 9: Flow chart for entering IP addresses

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.

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

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

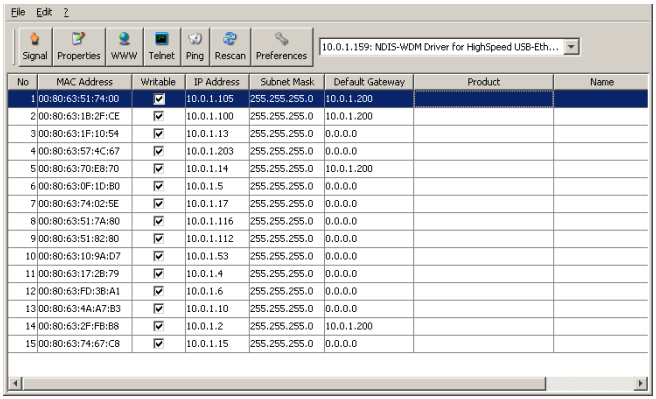
After entering the IP parameters, you can easily configure the device via the Web-based interface (see the “Web-based Interface” reference manual).

2.3 Entering the IP Parameters via Ethernet Switch Configurator

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

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

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



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

Figure 10: Ethernet Switch Configurator

When Ethernet Switch Configurator is started, it automatically searches the network for devices that support the Ethernet Switch Configurator protocol. Ethernet Switch Configurator uses the first network interface found on your PC. If your computer has more than 1 network interface, you may select a different network interface from the pull down list on Ethernet Switch Configurator‘s toolbar.

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

Ethernet Switch Configurator 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.

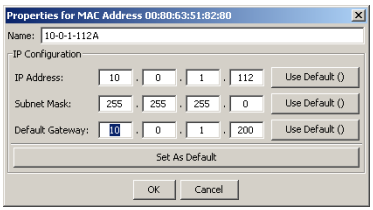


Figure 11: Ethernet Switch Configurator - assigning IP parameters

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 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.

Note: The following Memory Backup Adapter is used for the ConneXium Managed and Extended Managed switches : TCSEAM0100.

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

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

The password is valid if

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

To save the configuration data on the EAM (see on page “Saving locally (and on the EAM)”).

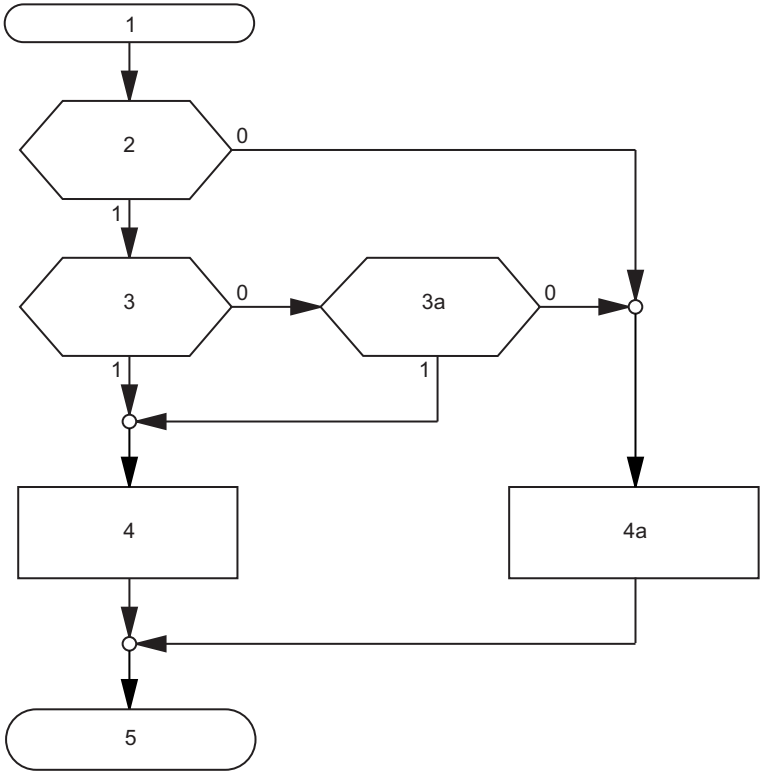


Figure 12: Flow chart of loading configuration data from the EAM
1 – Device start-up
2 – EAM plugged-in?
3 – Password in device and EAM identical?
3a – Default password in device?
4 – Load configuration from EAM,
EAM LEDs flashing synchronously
4a –Load configuration from local memory,
EAM LEDs flashing alternately
5 – Configuration data loaded

2.5 System configuration via BOOTP

When it is started up via BOOTP (bootstrap protocol), a device receives its configuration data in accordance with the “BOOTP process” flow chart (see figure 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 the CLI:

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

`enable`	Switch to the Privileged EXEC mode.
`network 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=10.1.112.83:tc=.global:
switch_02:ht=ethernet:ha=008063086502:ip=10.1.112.84:tc=.global:
.
.
```

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

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

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

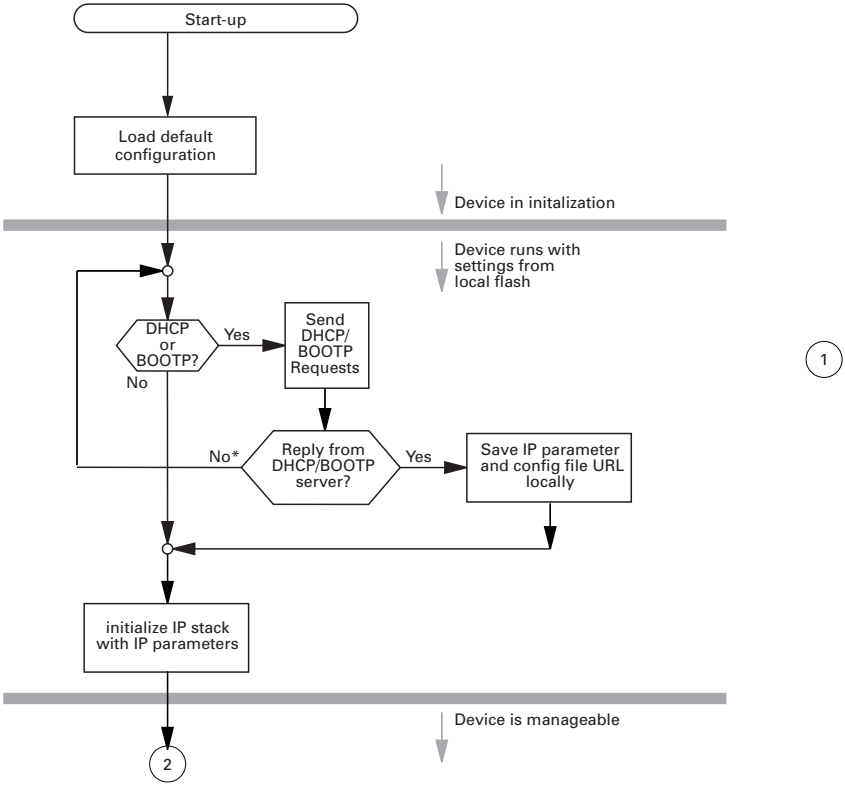


Figure 13: Flow chart for the BOOTP/DHCP process, part 1
** see figure 14*

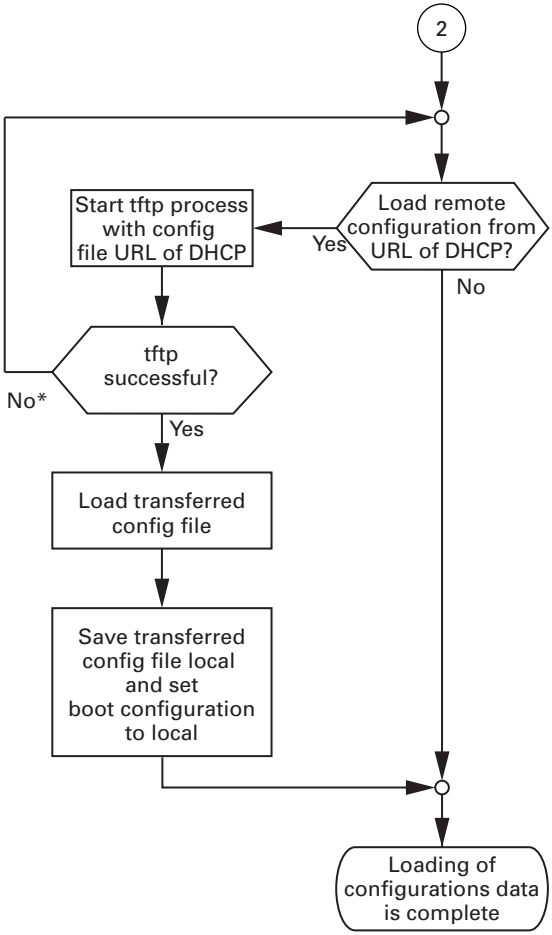


Figure 14: Flow chart for the BOOTP/DHCP process, part 2

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 a message regarding a detected error when saving a configuration, this could be due to an active loading process. DHCP/BOOTP only finishes a loading process when a valid configuration has been loaded. If DHCP/BOOTP does not find a valid configuration, then finish the loading process by loading the local configuration in the "Load" frame.

2.6 System Configuration via DHCP

The DHCP (Dynamic Host Configuration Protocol) is a further development of BOOTP, which it has replaced. The DHCP additionally allows the configuration of a DHCP client via a name instead of via the MAC address. For the DHCP, this name is known as the “client identifier” in accordance with RFC 2131.
The device uses the name entered under sysName in the system group of the MIB II as the client identifier. You can enter this system name directly via SNMP, the Web-based management (see system dialog), or the Command Line Interface.

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

The device sends its system name to the DHCP server. The DHCP server can then use the system name to allocate an IP address as an alternative to the MAC address.
In addition to the IP address, the DHCP server sends
– the netmask
– the default gateway (if available)
– the tftp URL of the configuration file (if available).

The device accepts this data as configuration parameters (see on page 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
17	Root Path
42	NTP server

Table 3: DHCP options which the device requests

Option	Meaning
61	Client Identifier
66	TFTP Server Name
67	Bootfile Name

Table 3: DHCP options which the device requests

To determine the path to the configuration file, the device evaluates the DHCP or BOOTP server‘s replies in the following way:

At first, the device evaluates the option 66 and the field “sname“.

- If the server includes the option 66, the device uses this value as the IP address for the configuration file‘s path.
  - If the server includes the field “sname“ instead of the option 66, the device uses the "sname“ value as the host name for the configuration file‘s path.
- If the server includes the option 66 as well as the field “sname“, the device only observes the option 66.
- If the server includes neither the option 66 nor the field “sname“, the device treats this as a nonexisting configuration file. Subsequently, the device does not evaluate the options 17 and 67.

If an option 66 of the field "sname“ is included in the server‘s response, the device subsequently evaluates the the options 17 and 67:

- If the server only includes the option 17, the device determines the configuration file‘s path as: <option 66> + <option 17> + “/“ + <Client Identifier> + “.prm“.
- If the server only includes the option 67, the device determines the configuration file‘s path as: <option 66> + <option 67>.
  - If the field "file“ is included in the reply, the device uses its value as a substitute for the option 67.
- If the server includes the option 17 as well as the option 67, the device only observes the option 17.
- If the server includes none of the options 17, 67 or the field “file“, the device determines the configuration file‘s path as: <option 66> + “/“ + <Client Identifier> + “.prm“.

The advantage of using DHCP instead of BOOTP is that the DHCP server can restrict the validity of the configuration parameters (“Lease”) to a specific time period (known as dynamic address allocation). Before this period (“Lease Duration”) elapses, the DHCP client can attempt to renew this lease. Alternatively, the client can negotiate a new lease. The DHCP server then allocates a random free address.
To help avoid this, DHCP servers provide the explicit configuration option of assigning a specific client the same IP address based on a unique hardware ID (known as static address allocation).

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

2.7 System Configuration via DHCP Option 82

On the device's front panel you will find the following hazard message.

⚠ 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 figure 13).

While the system configuration is based on the classic DHCP protocol on the device being configured (see on page 50 “System Configuration via DHCP”), Option 82 is based on the network topology. This procedure gives you the option of assigning the same IP address to any device which is connected to a particular location (port of a device) on the LAN.

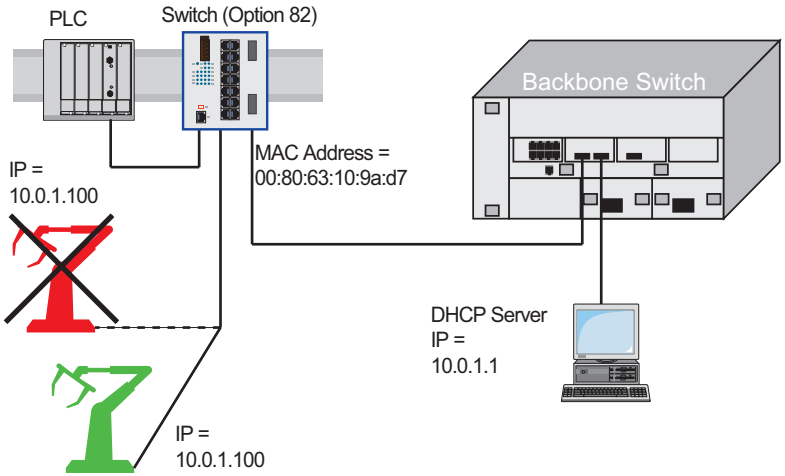


Figure 15: Application example of using Option 82

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.

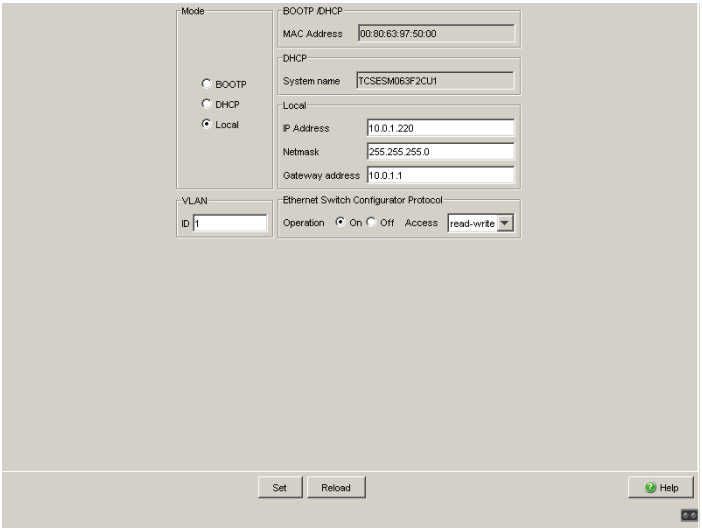


Figure 16: Network Parameters Dialog

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

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

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

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

2.9 Faulty Device Replacement

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

- Configuring the new device using an Memory Backup Adapter(see on page 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, check that the DIP switch settings to be sure that they are the same.

3 Loading/saving settings

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

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

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

3.1 Loading settings

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

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

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

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

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

3.1.1 Loading from the local non-volatile memory

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

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

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

3.1.2 Loading from the Memory Backup Adapter

If a EAM is connected to the device, the device automatically loads its configuration from the EAM during the boot procedure.
The chapter “Saving locally (and on the EAM)” on page 65 describes how to save a configuration file on an EAM.

Note: The device allows you to trigger the following events when the configuration stored on the EAM does not match what is in the device:
- an alarm (trap) is sent (see on page 175 “Configuring Traps”),
- the device status is updated (see on page 178 “Configuring the Device Status”),
- the status of the signal contacts is updated (see on page 180 “Controlling the Signal Contact”).

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 device" 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".

Note: When restoring a configuration by using one of the options in the frame “Load”, consider the following characteristics:

- The device can restore the configuration from a binary or a script file.
  - The option “from Device” restores the configuration only from the device’s internal binary file.
  - The 3 options “from URL”, “from URL & save to device” or "via PC" can restore the configuration from a binary file as well as from a script file. The device detects the file type automatically.
- When you restore the configuration from a script file, clear the device configuration first so that the default settings are overwritten properly. For more information (see on page 64 “Resetting the configuration to the state on delivery”).

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, 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 binary or script file on a URL”).

☐ In the "URL" line, enter the path of the tftp server, e.g. `tftp://10.1.112.214/switch/switch_01.cfg`.

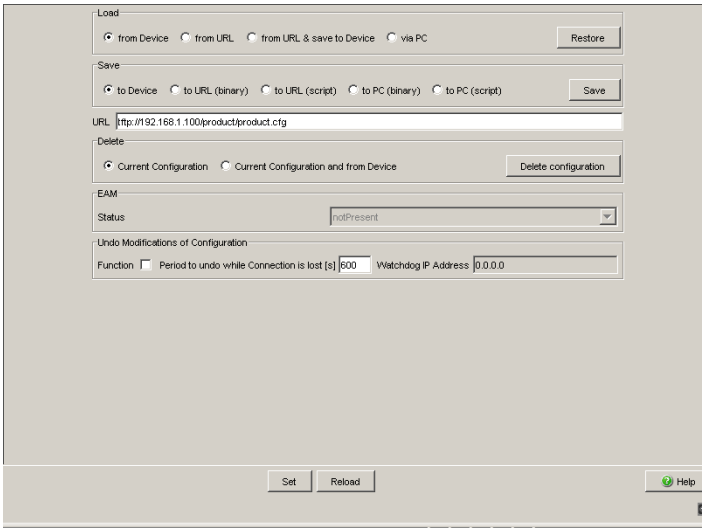


Figure 17: Load/Save dialog

```
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". The device will delete its configuration immediately.

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 the EAM.

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

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

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

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

Note: The device allows you to trigger the following events when the configuration stored on the EAM does not match what is in the device:
- an alarm (trap) is sent (see on page 175 “Configuring Traps”),
- the device status is updated (see on page 178 “Configuring the Device Status”),
- the status of the signal contacts is updated (see on page 180 “Controlling the Signal Contact”).

3.2.2 Saving to a binary or script file on a 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, select
“to URL (binary)” to generate a binary file, or
“to URL (script)” to generate an editable and readable script file.
☐ 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`	Switch to the Privileged EXEC mode.
`copy nvram:startup-config tftp://10.1.112.159/ switch/config.dat`	The device saves the configuration data in a binary file on a tftp server in the connected network
`copy nvram:script tftp://10.0.1.159/switch/ config.txt`	The device saves the configuration data in a script file on a tftp server in the connected network.

Note: When you save the configuration to a binary file, the device will save all its configuration settings to the binary file. In contrast, when you save the configuration to a script file, it will only save those configuration settings to the configuration script file that are different from the default configuration.

When loading script files, they are intended to overwrite the default configuration only.

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".

3.3 Configuration Signature

The device assigns a checksum or signature to identify a configuration so that changes to that configuration are visible. Every time you save a configuration, the device generates a random sequence of numbers and/or letters for the configuration signature. This signature changes every time you change the configuration. Each configuration has a unique identifier.

The device stores the random generated signature with the configuration to verify that the device maintained the configuration after a reboot.

The signature consists of a configuration file checksum and a random number. The device checks the signature to verify that it is different from previous generated numbers.

4 Loading Software Updates

Checking the installed software release

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

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

```
Last Alarm 1.......................... None
Alarm 2............................... None
System Description.................... TCSESM063F2CU1
System Name........................... TCSESM063F2CU1
System Location....................... Schneider TCSESM-E
System Contact..................... www.schneider-electric.com
System Up Time........................ 1 days 2 hrs 3 mins 4 secs
System Date and Time (local time zone). 2018-01-24 03:04:05
System IP Address..................... 10.0.1.220
Boot Software Release................. L2S-09.0.01
Boot Software Build Date.............. 2018-01-24 03:04
OS Software Release................... L2S-09.0.01
OS Software Build Date................ 2018-01-24 03:04
Hardware Revision..................... 1.32 / 11 / 0202
Hardware Description.................. TCSESM063F2CU1
Serial Number......................... 943953615061101003
Base MAC Address...................... 00:80:63:97:50:00
Number of MAC Addresses............... 26 (0x1a)
Configuration state..................... OK
Memory Backup Adapter, State.......... Not present
Memory Backup Adapter, Serial Number.... <None>
Power Supply P1, State................ Present
Power Supply P2, State................ Present
Media Module Information: TCSESM-E 6 Fast TX + 2 Fast FX
CPU Utilization....................... 12%
Average CPU Utilization............... 12%
Flashdisk (Kbytes free)............... 6413
```

Loading the software

The device gives you 2 options for loading the software:

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

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

4.1 Loading the Software manually from the EAM

You can connect the Memory Backup Adapter (EAM) to a USB port of your PC like a conventional USB stick and copy the device software into the main directory of the EAM.

☐ Copy the device software from your computer to the EAM.

☐ Now connect the EAM to the device‘s USB port.

☐ Open the system monitor (see on page 20 “Opening the system monitor”).

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

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

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

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

4.1.1 Select Boot Operating System Item 1

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

```
Select Operating System Image

(Available OS: Selected: 05.0.00 (2009-08-07 06:05), Backup: 04.2.00
(2009-07-06 06:05 (Locally selected: 05.0.00 (2009-08-07 06:05))

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

Figure 18: Update operating system screen display

- **Swap OS images**
  The memory of the device provides space for two images of the software. This gives you the ability to load a new version of the software without deleting the existing version.
  ☐ Select `1` to load the other software in the next booting process.

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

Test stored images in flash memory

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

Test stored images in USB memory

☐ Select 4 to check whether the images of the software stored in the EAM contain valid codes.

Apply and store selection

☐ Select 5 to confirm the software selection and to save it.

Cancel selection

☐ Select 6 to leave this dialog without making any changes.

4.1.2 Starting the software

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

4.1.3 Performing a cold start

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

4.2 Automatic software update by EAM

☐ For a software update via the EAM, first copy the new device software into the main directory of the Memory Backup Adapter. If the version of the software on the EAM is newer or older than the version on the device, the device performs a software update.

Note: Software versions with release 06.0.00 and higher in the non-volatile memory of the device support the software update via the EAM. If the device software is older, you have the option of loading the software manually from the EAM (see on page 73 “Loading the Software manually from the EAM”).

☐ Give the file the name that matches the device type and the software variant, e.g. tcsesm.bin for device type TCSESM.
If you have copied the software from a CD-ROM or from a Web server of the manufacturer, the software already has the correct file name.

☐ Also create an empty file with the name “autoupdate.txt” in the main directory of the EAM. Please note the case-sensitivity here.

☐ Connect the Memory Backup Adapter to the device and restart the device.

☐ The device automatically performs the following steps:
- During the booting process, it checks whether an EAM is connected.
- It checks whether the EAM has a file with the name “autoupdate.txt” in the main directory.
- It checks whether the EAM has a software file with a name that matches the device type in the main directory.
- If compares the software version stored on the EAM with the one stored on the device.
- If these conditions are fulfilled, the device loads the software from the EAM to its non-volatile memory as the main software.
- The device keeps a backup of the existing software in the non-volatile memory.
- The device then performs a cold start, during which it loads the new software from the non-volatile memory.

One of the following messages in the log file indicates the result of the update process:

- S_watson_AUTOMATIC_SWUPDATE_SUCCESSFUL: Update completed successfully.
- S_watson_AUTOMATIC_SWUPDATE_FAILED_WRONG_FILE: Update failed. Reason: incorrect file.
- S_watson_AUTOMATIC_SWUPDATE_FAILED_SAVING_FILE: Update failed. Reason: error when saving.

☐ In your browser, click on “Reload” so that you can use the Web-based interface to access the device again after it is booted.

4.3 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 266 “TFTP Server for Software Updates”).

☐ Select the `Basics:Software` dialog.

The URL identifies the path to the software stored on the tftp server. The URL is in the format
tftp://IP address of the tftp server/path name/file name
(e.g. `tftp://192.168.1.1/device/device.bin`).

☐ In the frame "tftp Software Update", click the option field "Firmware".

☐ Enter the path of the device software.

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

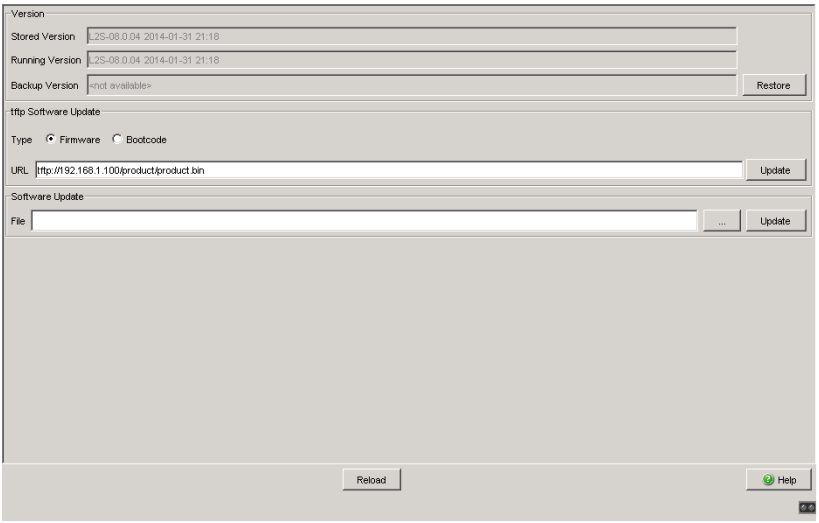


Figure 19: Software update dialog

☐ After successfully loading it, you activate the new software: Select the dialog `Basic Settings:Restart` and perform a cold start. 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`	Switch to the Privileged EXEC mode.
`copy tftp://10.0.1.159/ tcsesm.bin system:image`	Übertragen der Software-Datei "tcsesm.bin" vom tftp-Server mit der IP-Adresse 10.0.1.159 auf das Gerät.

4.4 Loading the Software via File Selection

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

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

The end of the update is indicated by one of the following messages:
- Update completed successfully.
- Update failed. Reason: incorrect file.
- Update failed. Reason: error when saving.
- File not found (reason: file name not found or does not exist).
- Connection error (reason: path without file name).

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

4.5 Bootcode Update via TFTP

In very rare cases, a bootcode with an expanded functionality is required to perform a software update. In such a case the service desk requests that you update the bootcode before performing the software update.

4.5.1 Updating the Bootcode file

For a tftp update, you need a tftp server to store the bootcode.
The URL identifies the path to the bootcode stored on the tftp server. The URL is in the format
tftp://IP address of the tftp server/path name/file name
(for example:).`tftp://192.168.1.1/device/device_bootrom.img`

- ☐ Open the "Basic Settings:Software" dialog.
- ☐ In the "tftp Software Update" frame, click the "Bootcode" radio button.
- ☐ Enter the path to the bootcode bin file in the "URL" text box.
- ☐ To start the update, click "Update".
- ☐ To start the new bootcode after loading, open the "Basic Settings:Restart" dialog and click "Cold start...".

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

`enable`	Switch to the privileged EXEC mode.

`configure`	Switch to the Configuration mode.
`copy <url> system:bootcode`	Copy the bootcode bin file from the tftp server to the device.

5 Configuring the Ports

The port configuration consists of:

- Switching the port on and off
- Selecting the operating mode
- Activating the display of detected loss of connection

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 detected loss of connection

In the default setting, the device displays a detected connection error 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 Assistance in the Protection from Unauthorized Access

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

- Password for SNMP access
- Telnet/Web access disabling
- Ethernet Switch Configurator function disabling
- Port access control via IP or MAC address
- Login Banner

6.1 Dealing with unauthorized access

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

☐ Deactivate SNMPv1 and SNMPv2 and select a password for SNMPv3 access other than the standard password (see on page 88 “Entering the password for SNMP access”).

☐ Deactivate Telnet access.
Deactivate web access after you have downloaded the applet for the web-based interface onto your management station. You can start the web-based interface as an independent program and thus have SNMP access to the device (see on page 93 “Enabling/disabling Telnet/Web/SSH access”).

☐ Deactivate Ethernet Switch Configurator access.

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

6.2 Password for SNMP access

6.2.1 Description of password for SNMP access

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

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

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

To help protect your device from unwanted access:

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

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

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

6.2.2 Entering the password for SNMP access

☐ Select the `Security:Password/SNMP Access` dialog.
This dialog gives you the option of changing the read and read/write passwords for access to the device via the Web-based interface, via the CLI, and via SNMPv3 (SNMP version 3).
Set different passwords for the read password and the read/write password so that a user that only has read access (user name “user”) does not know, or cannot guess, the password for read/write access (user name “admin”).
If you set identical passwords, when you attempt to write this data the device reports a general error.

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

Note: Passwords are case-sensitive.

☐ 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.
☐ The "Accept only encrypted requests" function encrypts the data of the Web-based management that is transferred between your PC and the device with SNMPv3. You can set the funtion differently for access with a read password and access with a read/write password.
☐ When you activate the "Synchronize password to v1/v2 community" function, when the password is changed the device synchronizes the corresponding community name.
  – When you change the password for the read/write access, the device updates the readWrite community for the SNMPv1/v2 access to the same value.
  – When you change the password for the read access, the device updates the readOnly community for the SNMPv1/v2 access to the same value.

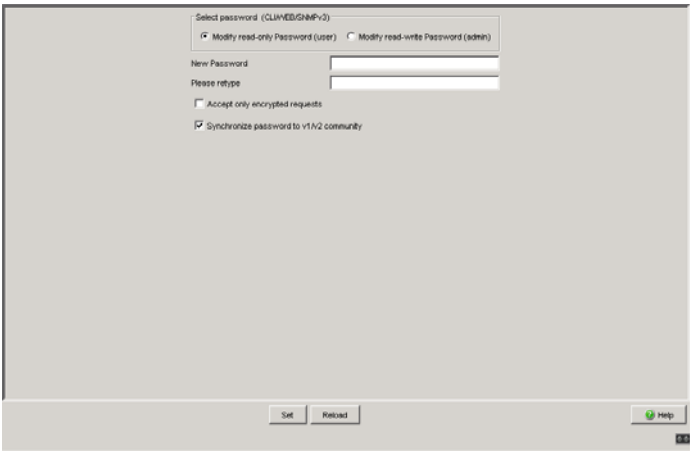


Figure 20: Password/SNMP Access dialog

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 device does not display the passwords. Make a note of every change. You cannot access the device without a valid password.

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

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

☐ Select the "Security:SNMPv1/v2 access" dialog.
With this dialog you can select the access via SNMPv1 or SNMPv2. In the state on delivery, both protocols are activated. You can thus use the device to 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, make the read password and the read/write password unique passwords; do not use identical passwords.
Please note that passwords are case-sensitive.

Index	Serial number for this table entry
Community Name	Password with which this computer can access the device. This password is independent of the SNMPv3 password. If you activate the "Synchronize community to v3 password" function in the "Configuration" frame, the device synchronizes the corresponding SNMPv3 password when you change the community name.
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.

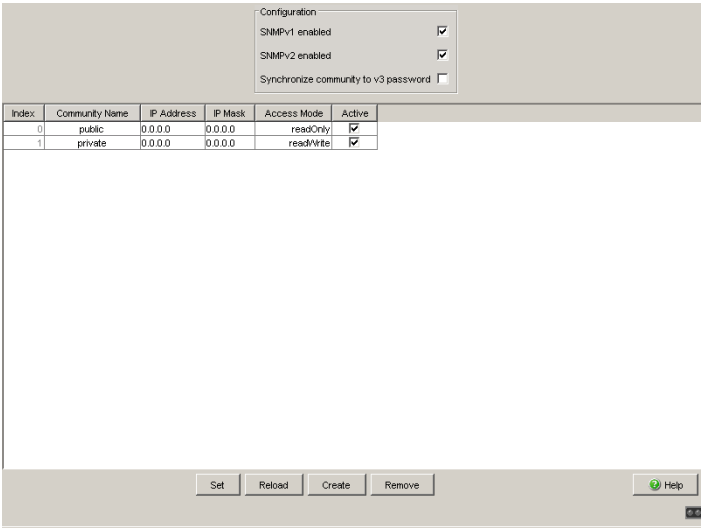


Figure 21: SNMPv1/v2 access dialog

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

6.3 Telnet/Web/SSH access

6.3.1 Description of Web Access (http)

The device's Web server allows you to configure the device by using the graphical user interface. You can deactivate the Web server to prevent Web access to the device.
The server is activated in its default setting.

After you switch the http Web server off, it is no longer possible to log in via a http Web browser. The http session in the open browser window remains active.

6.3.2 Description of SSH Access

The device's SSH server allows you to configure the device using the Command Line Interface (in-band). You can deactivate the SSH server to prevent SSH access to the device.
The server is deactivated in its default setting.
After the SSH server has been deactivated, you will no longer be able to access the device via a new SSH connection. If an SSH connection already exists, it is retained.

Note: The Command Line Interface (out-of-band) and the "Security:Telnet/Web/SSH Access" dialog in the graphical user interface allows you to reactivate the SSH server.

Note: To be able to access the device via SSH, you require a key that has to be installed on the device. See “Preparing access via SSH” on page 271.

The device supports SSH version 1 and version 2. You have the option to define the protocol to be used.

- ☐ Open the "Security:Telnet/Web/SHH Access" dialog.
- ☐ Select the protocol to be used in the "Configuration" frame, "SSH Version" field.

`enable`	Switch to the privileged EXEC mode.
`no ip ssh`	Deactivates the SSH server.
ip ssh protocol 2	The SSH server uses SSH version 2.
ip ssh protocol 1	The SSH server uses SSH version 1.
ip ssh protocol 1 2	The SSH server uses SSH versions 1 and 2.
`ip ssh`	Activates the SSH server.

6.3.3 Enabling/disabling Telnet/Web/SSH access

The Web server copies a Java applet for the graphical user interface onto your computer. The applet then communicates with the device by SNMPv3 (Simple Network Management Protocol). The Web server of the device allows you to configure the device using the graphical user interface. You can switch off the Web server in order to help prevent the applet from being copied.

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

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

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

6.3.4 Web access through HTTPS

The HTTPS communication protocol (HyperText Transfer Protocol Secure) helps protect data transfers from interception. The device uses the HTTPS protocol to encrypt and authenticate the communications between web server and browser.
The Web server uses HTTP to load a Java applet for the graphical user interface onto your computer. This applet then communicates with the device by SNMP (Simple Network Management Protocol). If you have enabled the "Web Server (HTTPS)" function, the Java applet starts setting up a connection to the device via HTTPS. The device creates an HTTPS tunnel through the SNMP. It uses DES encoding on 56 bits. You can upload HTTPS certificates to the device.

Certificate

An X.509/PEM Standard certificate (Public Key Infrastructure) is required for the encryption. In the as-delivered state, a self-generated certificate is already present on the device.

- ☐ You can create an X509/PEM certificate using the following CLI command: `# ip https certgen`
- ☐ You can upload a new certificate using the following CLI command:
  `copy tftp://<server_ip>/<path_to_pem> nvram:httpscert`
- ☐ You can switch the HTTPS server off and on again using the following CLI command sequence:
  ```
  # no ip https server
  # ip https server
  ```

Note: If you upload a new certificate, reboot the device or the HTTPS server in order to activate the certificate.

HTTPS connection

Note: The standard port for HTTPS connection is 443. If you change the number of the HTTPS port, reboot the device or the HTTPS server in order to make the change effective.

☐ You can change the HTTPS port number using the following CLI-command (where <port_no> is the number of the HTTPS port):

```
#ip https port <port_no>
```

Note: If you want to use HTTPS, switch on both HTTPS and HTTP. This is required in order to load the applet. In the as-delivered state, HTTPS is switched off.

☐ Open the "Security:Telnet/Web/SSH Access" dialog.

☐ Tick the boxes "Telnet Server active", "Web Server (http) active" and "Web Server (https) active". In the "HTTPS Port Number" box, enter the value `443`.

☐ To access the device by HTTPS, enter HTTPS instead of HTTP in your browser, followed by the IP address of the device.

`enable`	Switch to Privileged EXEC mode.
`# ip https server`	Switch on HTTPS-server.
`# ip https port <port_no>`	Set the HTTPS port number for a secure HTTP connection. - As-delivered state: 443. - Value range: 1-65535
`# no ip https server` `# ip https server`	If you change the HTTPS port number, switch the HTTPS server off and then on again in order to make the change effective.
`# show ip https`	Optional: Show the status of the HTTPS server and HTTPS port number.
`# ip https certgen`	Create X509/PEM certificates.

`# copy tftp://<server_ip>/ <path_to_pem> nvram:httpscert`	Upload an X509/PEM certificate for HTTPS using TFTP.
`# no ip https server` `# ip https server`	After uploading the HTTPS certificate, switch the HTTPS server off and then on again in order to activate the certificate.:

The device uses HTTPS protocol and establishes a new connection. When the session is ended and the user logs out, the device terminates the connection.

Note: The device allows you to open HTTPS- and HTTP connections at the same time. The maximum number of HTTP(S) connections that can be open at the same time is 16.

6.4 Ethernet Switch Configurator Access

6.4.1 Description of the Ethernet Switch Configurator Protocol

The Ethernet Switch Configurator protocol allows you to allocate an IP address to the device on the basis of its MAC address (see on page 40 “Entering the IP Parameters via Ethernet Switch Configurator”). Ethernet Switch Configurator is a Layer 2 protocol.

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

6.4.2 Enabling/disabling the Ethernet Switch Configurator function

- ☐ Select the "Basic settings:Network" dialog.
- ☐ Disable the "Ethernet Switch Configurator" function in the "Ethernet Switch Configurator Protocol v1/v2" 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" function.
`network protocol ethernet-switch-conf read-only`	Enable the "Ethernet Switch Configurator" function with `read-only` access.
`network protocol ethernet-switch-conf read-write`	Enable the "Ethernet Switch Configurator" function with `read-write` access.

6.5 Restricted Management Access

The device allows you to differentiate the management access to the device based on IP address ranges, and to differentiate these in turn based on management services (http, snmp, telnet, ssh). You thus have the option to set finely differentiated management access rights.

If you only want the device, which is located, for example, in a production plant, to be managed from the network of the IT department via the Web interface, but also want the administrator to be able to access it remotely via SSH, you can achieve this with the "Restricted management access" function.

You can configure this function using the graphical user interface or the CLI. The graphical user interface provides you with an easy configuration option. Confirm that you do not block your access to the device. The CLI access to the device via V.24 provided at all times is excluded from the function and cannot be restricted.

In the following example, the IT network has the address range 192.168.1.0/24 and the remote access is from a mobile phone network with the IP address range 109.237.176.0 - 109.237.176.255.

The device is already prepared for the SSH access (see on page 271 “Preparing access via SSH”) and the SSH client application already knows the fingerprint of the host key on the device.

Parameter	IT network	Mobile phone network
Network address	192.168.1.0	109.237.176.0
Netmask	255.255.255.0	255.255.255.0
Desired management access	http, snmp	ssh

Table 4: Example parameter for the restricted management access

☐ Select the "Security:Restricted Management Access" dialog.

- ☐ Leave the existing entry unchanged and use the "Create" button to create a new entry for the IT network.
- ☐ Enter the IP address 192.168.1.0.
- ☐ Enter the netmask 255.255.255.0.
- ☐ Leave the HTTP and SNMP management services activated and deactivate the Telnet and SSH services by removing the checkmarks from the respective boxes.
- ☐ Use the "Create" button to create a new entry for the mobile phone network.
- ☐ Enter the IP address 109.237.176.0.
- ☐ Enter the netmask 255.255.255.0.
- ☐ Deactivate the HTTP, SNMP and Telnet services and leave SSH activated.
- ☐ Confirm that you have CLI access to the device via V.24.
- ☐ Deactivate the preset entry, because this allows everything and would cause your subsequent entries to have no effect.
- ☐ Activate the function.
- ☐ Click on "Write" to temporarily save the data.
- ☐ If your current management station is also located in the IT network, you continue to have access to the graphical user interface. Otherwise the device ignores operations via the graphical user interface, and it also rejects a restart of the graphical user interface.
- ☐ Check whether you can access the device from the IT network via http and snmp: Open the graphical user interface of the device in a browser, login on the start screen, and check whether you can read data (as user `user`) or read and write data (as user `admin`).
  Check whether the device rejects connections via telnet and ssh.
- ☐ Check whether you can access the device from the mobile phone network via ssh: Open an SSH client, make a connection to the device, login, and check whether you can read data, or read and write data.
  Check whether the device rejects connections via http, snmp and telnet.
- ☐ When you have successfully completed both tests, save the settings in the non-volatile memory. Otherwise check your configuration. If the device rejects access with the graphical user interface, use the CLI of the device to initially deactivate the function via V.24.

`enable`	Switch to the privileged EXEC mode.
`show network mgmt-access`	Display the current configuration.
`network mgmt-access add`	Create an entry for the IT network. This is given the smallest free ID - in the example, 2.
`network mgmt-access modify 2 ip 192.168.1.0`	Set the IP address of the entry for the IT network.
`network mgmt-access modify 2 netmask 255.255.255.0`	Set the netmask of the entry for the IT network.
`network mgmt-access modify 2 telnet disable`	Deactivate telnet for the entry of the IT network.
`network mgmt-access modify 2 ssh disable`	Deactivate SSH for the entry of the IT network.
`network mgmt-access add`	Create an entry for the mobile phone network. In the example, this is given the ID 3.
`network mgmt-access modify 3 ip 109.237.176.0`	Set the IP address of the entry for the mobile phone network.
`network mgmt-access modify 3 netmask 255.255.255.0`	Set the netmask of the entry for the mobile phone network.
`network mgmt-access modify 3 http disable`	Deactivate http for the entry of the mobile phone network.
`network mgmt-access modify 3 snmp disable`	Deactivate snmp for the entry of the mobile phone network.
`network mgmt-access modify 3 telnet disable`	Deactivate telnet for the entry of the mobile phone network.
`network mgmt-access status 1 disable`	Deactivate the **preset** entry.
`network mgmt-access operation enable`	Activate the function **immediately**.
`show network mgmt-access`	Display the current configuration of the function.
`copy system:running-config nvram:startup-config`	Save the entire configuration in the non-volatile memory.

6.6 Port Access Control

6.6.1 Description of the Port Access Control

You can configure the device in such a way that it helps to 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:

- The device can distinguish between authorized and unauthorized access and supports two types of access control:
  - Access for all:
    – no access restriction.
    – MAC address 00:00:00:00:00:00 or
    – IP address 0.0.0.0.
  - Access exclusively for defined MAC and IP addresses:
    – only devices with defined MAC or IP addresses have access.
    – You can define up to 10 IP addresses, MAC addresses or maskable MAC addresses.
- The device can react to an unauthorized access attempt in 3 selectable ways:
  - none: no response
  - trapOnly: message by sending a trap
  - portDisable: message by sending a trap and disabling the port

6.6.2 Application Example for Port Access Control

You have a LAN connection in a room that is accessible to everyone. To set the device so that only defined users can use the LAN connection, activate the port access control on this port. An unauthorized access attempt will cause the device to shut down the port and alert 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 83 “Configuring the Ports”) and send an alarm

Prerequisities for further configuration:

- The port for the LAN connection is enabled and configured correctly (see on page 83 “Configuring the Ports”)
- Prerequisites for the device to be able to send an alarm (trap) (see on page 175 “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 you want 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 you want protected, in the "Action" cell, and select `portDisable`.

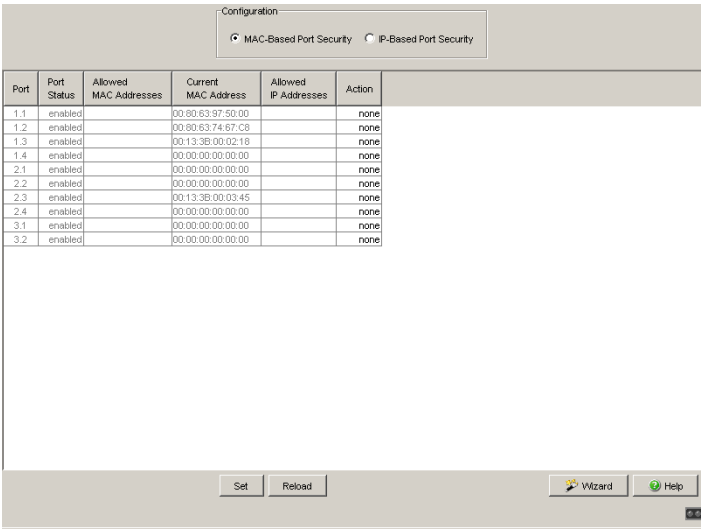


Figure 22: Port Security dialog

☐ 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.

6.7 Port Authentication IEEE 802.1X

6.7.1 Description of Port Authentication according to IEEE 802.1X

The port-based network access control is a method described in norm IEEE 802.1X to help protect IEEE 802 networks from unauthorized access. The protocol controls the access to this port by authenticating and authorizing a terminal device that is connected to one of the device's ports.
The authentication and authorization is carried out by the authenticator, in this case the device. The device authenticates the supplicant (the querying device, e.g. a PC, etc.), which means that it permits the access to the services it provides (e.g. access to the network to which the device is connected) or denies it. In the process, the device accesses an external authentication server (RADIUS server), which checks the authentication data of the supplicant. The device exchanges the authentication data with the supplicant via the Extensible Authentication Protocol over LANs (EAPOL), and with the RADIUS server via the RADIUS protocol.

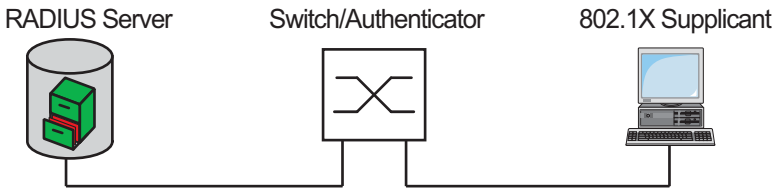


Figure 23: Radius server connection

6.7.2 Authentication Process according to IEEE 802.1X

A supplicant attempts to communicate via a device port.

- The device requests authentication from the supplicant. At this time, only EAPOL traffic is allowed between the supplicant and the device.
- The supplicant replies with its identification data.
- The device forwards the identification data to the authentication server.
- The authentication server responds to the request in accordance with the access rights.
- The device evaluates this response and provides the supplicant with access to this port (or leaves the port in the blocked state).

6.7.3 Preparing the Device for the IEEE 802.1X Port Authentication

- ☐ Configure your own IP parameters (for the device).
- ☐ Globally enable the 802.1X port authentication function.
- ☐ Set the 802.1X port control to "auto". The default setting is "force-authorized".
- ☐ Enter the "shared secret" between the authenticator and the Radius server. The shared secret is a text string specified by the RADIUS server administrator.
- ☐ Enter the IP address and the port of the RADIUS server. The default UDP port of the RADIUS server is port 1812.

6.7.4 IEEE 802.1X Settings

Configurating the RADIUS Server

☐ Select the "Security:RADIUS:RADIUS Server" dialog.

This dialog allows you to enter the data for 1, 2 or 3 RADIUS servers.

☐ Click "Create" to open the dialog window for entering the IP address of a RADIUS server.
☐ Confirm the IP address entered using "OK".
You thus create a new row in the table for this RADIUS server.
☐ In the "Shared secret" column you enter the character string which you get as a key from the administrator of your RADIUS server.
☐ With "Primary server" you name this server as the first server which the device should contact for port authentication queries. If this server is not available, the device contacts the next server in the table.
☐ "Selected server" shows which server the device actually sends its queries to.
☐ With "Delete entry" you delete the selected row in the table.

Selecting Ports

☐ Select the "Security:802.1x Port Authentication:Port Configuration" dialog.
☐ In the "Port control" column you select `auto` for the ports for which you want to activate the port-related network access control.

Activating Access Control

☐ Select the "Security:802.1x Port Authentication:Global" dialog.
☐ With "Operation" you enable the function.

6.8 Login Banner

The device gives you the option of displaying a greeting text to users before they login to the device. The users see this greeting text in the login dialog of the graphical user interface (GUI) and of the Command Line Interface (CLI).

Users logging in with SSH see the greeting text - depending on the client used - before or during the login.

Perform the following work steps:

- ☐ Open the "Security:Login Banner" dialog.
- ☐ Enter the greeting text in the "Banner Text" frame. Max. 255 characters allowed.
- ☐ Click "Set" to save the changes temporarily.

`enable`	Switch to the privileged EXEC mode.
`set pre-login-banner text "<string>"`	Assign the greeting text: – Put the text in quotation marks. – Max. 255 characters allowed. – Insert tab using string `\\t`. – Insert line break using string `\\n`.
`logout`	After you log out the greeting text is visible.

7 Synchronizing the System Time in the Network

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

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

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

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

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

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

7.1 Entering the Time

If no reference clock is available, you have the option of entering the system time in a device and then using it like a reference clock (see on page 116 “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.

☐ Open the "Time:Basic Settings" dialog.

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

- “System time (UTC)” displays the time determined using SNTP or PTP.
  The display is the same worldwide. Local time differences are not taken into account.

  Note: If the time source is PTP, consider that the PTP time uses the TAI time scale. TAI time is 34 s ahead of UTC time (as of 01.01.2011).
  If the UTC offset is configured correctly on the PTP reference clock, the device corrects this difference automatically when displaying “System time (UTC)”.
- The "System Time" uses "System Time (UTC)", allowing for the local time difference from "System Time (UTC)".
  "System Time" = "System Time (UTC)" + "Local Offset".

- ▶ Time Source displays the source of the following time data. The device automatically selects the source with the greatest accuracy. Possible sources are: `local`, `ptp` and `sntp`. The source is initially `local`.
  If PTP is activated and the device receives a valid PTP frame, it sets its time source to `ptp`. If SNTP is activated and if the device receives a valid SNTP packet, the device sets its time source to `sntp`. The device gives the PTP time source priority over SNTP.
- ☐ With "Set Time from PC", the device takes the PC time as the system time and calculates the "System Time (UTC)" using the local time difference.
  "System Time (UTC)" = "System Time" - "Local Offset"
- ☐ The "Local Offset" is for displaying/entering the time difference between the local time and the "System Time (UTC)".

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

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`sntp time <YYYY-MM-DD HH:MM:SS>`	Set the system time of the device.
`sntp client offset <-1000 to 1000>`	Enter the time difference between the local time and the "System Time (UTC)".

7.2 SNTP

7.2.1 Description of SNTP

The Simple Network Time Protocol (SNTP) enables you to synchronize the system time in your network.
The device supports the SNTP client and the SNTP server function.

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

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

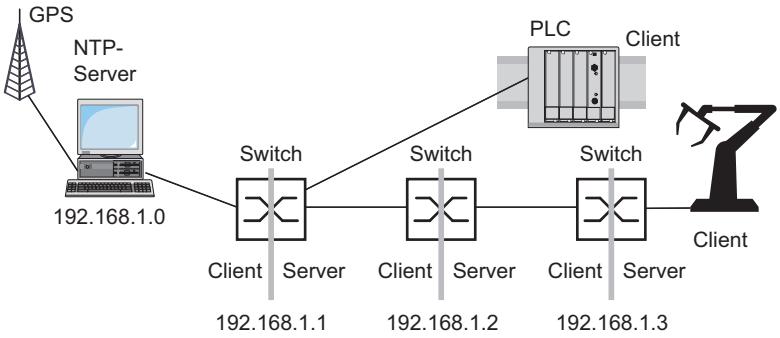


Figure 24: SNTP cascade

7.2.2 Preparing the SNTP Configuration

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

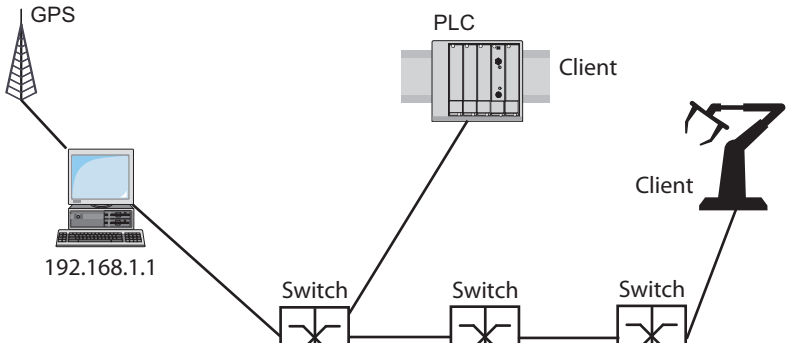


Figure 25: Example of SNTP cascade

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

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

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

7.2.3 Configuring SNTP

☐ Select the `Time:SNTP` dialog.

▶ Operation

☐ In this frame you switch the SNTP function on/off globally.

▶ SNTP Status

☐ The “Status message” displays statuses of the SNTP client as one or more test messages, `e.g. Server 2 not responding`.

▶ Configuration SNTP Client

☐ In "Client status" you switch the SNTP client of the device on/off.

☐ 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, enter the dedicated server adress(es) and disable the setting "Accept SNTP Broadcasts" (see below). You thus help ensure that the device uses the time of the servers entered and does not synchronize to broadcasts that might not be trustworthy.

☐ In "Server request interval" you specify the interval at which the device requests SNTP packets (valid entries: 1 s to 3600 s, on delivery: 30 s).

☐ With "Accept SNTP Broadcasts" the device takes the system time from SNTP Broadcast/Multicast packets that it receives.

☐ With "Deactivate client after synchronization", the device only synchronizes its system time with the SNTP server one time after the client status is activated, then it switches the client off.

Note: If you have enabled PTP at the same time, the SNTP client first collects 60 time stamps before it deactivates itself. The device thus determines the drift compensation for its PTP clock. With the preset server request interval, this takes about half an hour.

Configuration SNTP Server

- ☐ In “Server status” you switch the SNTP server of the device on/off.
- ☐ In “Anycast destination address” you enter the IP address to which the SNTP server of the device sends its SNTP packets (see table 5).
- ☐ In “VLAN ID” you specify the VLAN to which the device periodically sends its SNTP packets.
- ☐ In “Anycast send interval” you specify the interval at which the device sends SNTP packets (valid entries: 1 s to 3,600 s, on delivery: 120 s).
- ☐ With “Disable Server at local time source” the device disables the SNTP server function if the source of the time is `local` (see `Time` dialog).

IP destination address	Send SNTP packet to
0.0.0.0	Nobody
Unicast address (0.0.0.1 - 223.255.255.254)	Unicast address
Multicast address (224.0.0.0 - 239.255.255.254), especially 224.0.1.1 (NTP address)	Multicast address
255.255.255.255	Broadcast address

Table 5: Destination address classes for SNTP and NTP packets

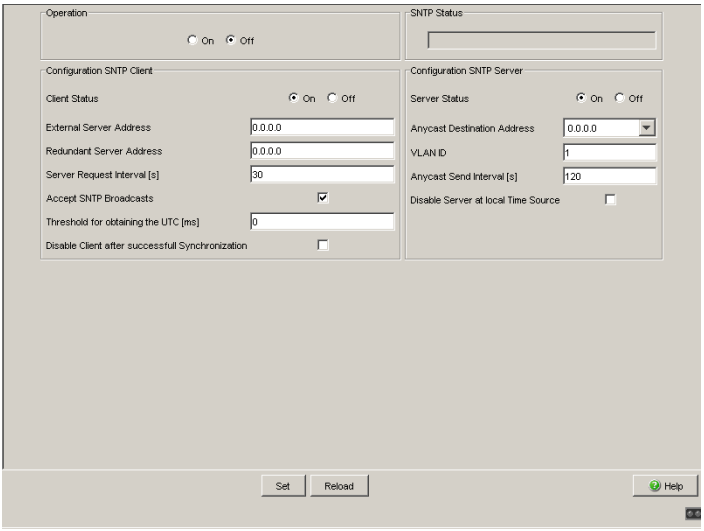


Figure 26: SNTP Dialog

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

Table 6: Settings for the example (see figure 25)

7.3 Precision Time Protocol

7.3.1 Description of PTP Functions

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

The IEEE 1588 standard with the Precision Time Protocol (PTP) describes a procedure that determines the best possible master clock in a LAN and thus enables precise synchronization of the clocks in this LAN.

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

Factors influencing precision are:

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

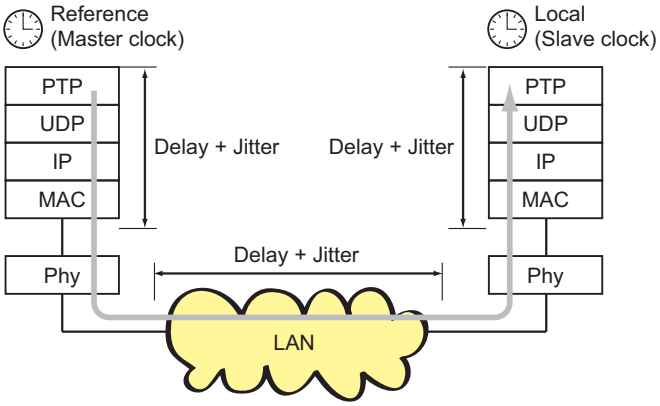
PTPv1 Stratum number	PTPv2 Clock class	Specification
0	– (priority 1 = 0)	For temporary, special purposes, in order to assign a higher accuracy to one clock than to all other clocks in the network.
1	6	Indicates the reference clock with the highest degree of accuracy. The clock can be both a boundary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

Table 7: Stratum – classifying the clocks

PTPv1 Stratum number	PTPv2 Clock class	Specification
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 not be used as the so-called best master clock.

Table 7: Stratum – classifying the clocks

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



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

Figure 27: Delay and jitter 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 (> 1502 bytes or CRC errors) as well as fragments (< 64 bytes) are rejected. Valid data packets are forwarded by the device.

8.1.2 Multi-Address Capability

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

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

in the destination address field are sent to this port. The device enters learned source addresses in its filter table (see on page 126 “Entering Static Addresses”).

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 particular age - the aging time - are deleted by the device from its address table.
Data packets with an unknown destination address are sent by the device to all ports.
Data packets with known destination addresses are selectively transmitted by the device.

Note: A reboot deletes the learned address entries.

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

8.1.4 Entering Static Addresses

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

The following are valid filter criteria:

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

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

- The management administrator describes the static part of the filter table (`dot1qStaticTable`).
- During operation, the device is capable of learning which of its ports receive data packets from which source address (see on page 124 “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 filter entries for Multicast addresses.

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

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

- `learned`: The filter was created automatically by the device.
- `permanent`: The filter is stored permanently in the device or on the URL (see on page 65 “Saving settings”).
- `invalid`: With this status you delete a manually created filter.
- `igmp`: The filter was created by IGMP Snooping.

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

8.1.5 Disabling the Direct Packet Distribution

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

☐ Select the `Switching:Switching Global` dialog.

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

8.2 Multicast Application

8.2.1 Description of the Multicast Application

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

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

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

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

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

8.2.2 Example of a Multicast Application

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

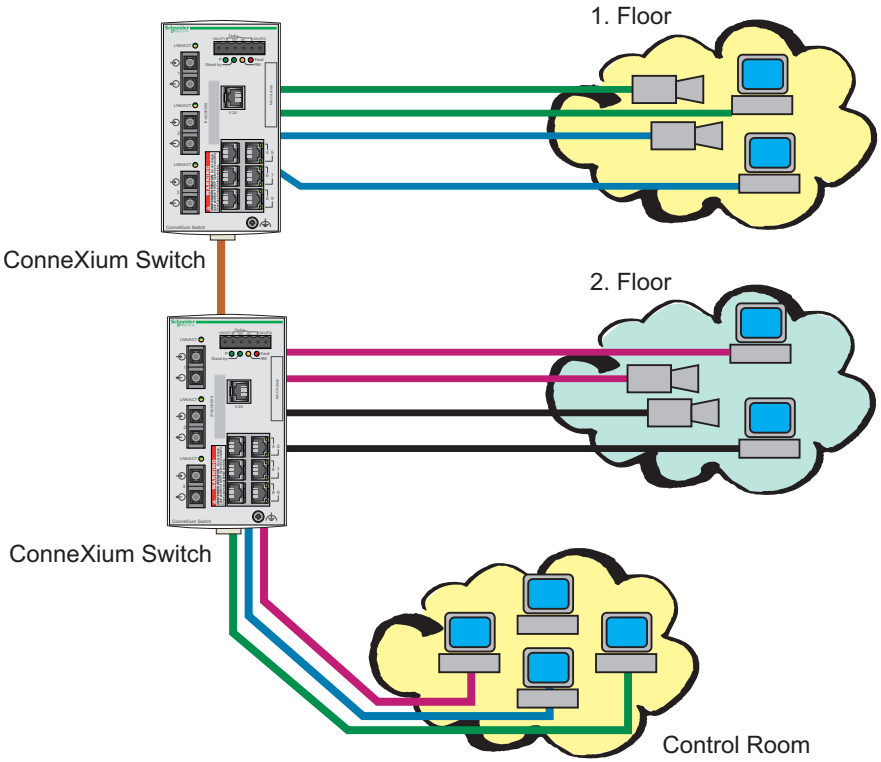


Figure 28: Example: Video surveillance in machine rooms

8.2.3 Description of IGMP Snooping

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

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

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

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

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

IGMP Snooping translates IP Multicast group addresses into MAC Multicast addresses, so that the IGMP functions can also be used by Layer 2 Switches. The Switch records the MAC addresses of the Multicast receivers, with are obtained via IGMP Snooping from the IP addresses, in the static address table. The Switch thus transmits these Multicast packets exclusively at the ports at which Multicast receivers are connected. The other ports are not affected by these packets.

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

Default setting: “Off”.

8.2.4 Setting IGMP Snooping

☐ Select the `Switching:Multicast:IGMP` dialog.

Operation

The “Operation” frame allows you to enable/disable IGMP Snooping globally for the entire device.
If IGMP Snooping is disabled, then

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

Settings for IGMP Querier and IGMP

With these frames you can enter global settings for the IGMP settings and the IGMP Querier function.
Prerequisite: The IGMP Snooping function is activated globally.

IGMP Querier

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

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

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

Note the connection between the parameters Max. Response Time, Send Interval and Group Membership Interval (see on page 132 “Parameter Values”).

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

IGMP Settings

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

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

Note the connection between the parameters Max. Response Time, Send Interval and Group Membership Interval (see on page 132 “Parameter Values”).

The Multicast group members select a random value within the maximum response time for their response, to prevent all the Multicast group members responding to the query at the same time.
Select a large value if you want to reduce the load on your network and can accept the resulting longer switching times.
Select a small value if you require short switching times and can accept the resulting network load.
In “Group Membership Interval” you specify the period for which a dynamic Multicast group remains entered in the device if it does not receive any report messages (valid values: 3-3,600 s, default setting: 260 s).

Note the connection between the parameters Max. Response Time, Send Interval and Group Membership Interval (see on page 132 “Parameter Values”).

Parameter Values

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

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

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

Parameter	Protocol Version	Value range	Default setting
Max. Response Time,	1, 2 3	1-25 seconds 1-3,598 seconds	10 seconds
Send Interval	1, 2, 3	2-3,599 seconds	125 seconds
Group Membership Interval	1, 2, 3	3-3,600 seconds	260 seconds

Table 8: Value range for
- Max. Response Time
- Send Interval
- Group Membership Interval

Multicasts

With these frames you can enter global settings for the Multicast functions.
Prerequisite: The IGMP Snooping function is activated globally.

Unknown Multicasts

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

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

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

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

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

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

Settings per Port (Table)

- “IGMP on”
  This table column enables you to enable/disable the IGMP for each port when the global IGMP Snooping is enabled. Port registration will not occur if IGMP is disabled.

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

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

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

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

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

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

Note: If the device is incorporated into a HIPER-Ring, you can use the following settings to quickly reconfigure the network for data packets with registered Multicast destination addresses after the ring is switched:

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

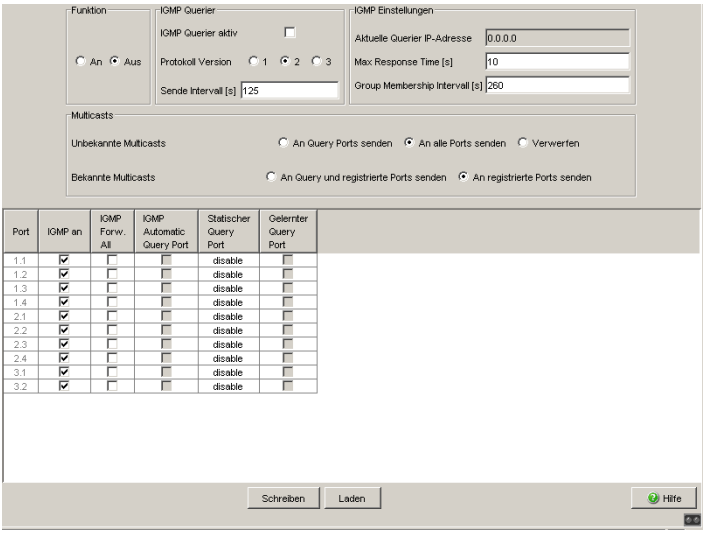


Figure 29: IGMP Snooping dialog

8.2.5 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 as the destination address use the 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: “On”.

8.2.6 Setting GMRP

☐ Select the `Switching:Multicasts:GMRP` dialog.

Operation

The “Operation” frame allows you to enable GMRP globally for the entire device.

It 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.

Multicasts

The "Multicasts" frame allows you to configure GMRP to discard multicasts addresses or send them to the ports.

Enable GMRP, then:

- when you select "Discard", the device deletes unknown multicasts
- when you select "Send To All Ports", the device evaluates the GMRP packets received, and sends (floods) received data packets to the ports.

Settings per Port (Table)

- "GMRP”
  This table column enables you to enable/disable the GMRP for each port when the GMRP is enabled globally. When you switch off the GMRP at a port, no registrations can be made for this port, and GMRP packets cannot be forwarded at this port.

- “GMRP Service Requirement”
  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 incorporated into a HIPER-Ring, you can use the following settings to quickly reconfigure the network for data packets with registered Multicast destination addresses after the ring is switched:
- Activate GMRP on the ring ports and globally, and
- activate “Forward all groups” on the ring ports.

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.

Note: The limiter functions work exclusively on layer 2 and serve the purpose of limiting the effects of storms of those frame types (typically broadcasts) that the Switch floods. The limiter function ignores any protocol information of higher layers like IP or TCP. This may affect e.g., TCP traffic.

You can minimize this effects by:

- applying the limiter function only to particular frame types (e.g., to broadcasts, multicasts and unicasts with an unlearned destination address) and excluding unicasts with a learned destination address from the limitation,
- using the egress limiter function instead of the ingress limiter function because the former cooperates slightly better with TCP‘s flow control (reason: frames buffered by the internal switching buffer),
- increasing the aging time for learned unicast destination addresses.

8.3.2 Rate Limiter settings

☐ Select the `Switching:Rate Limiter` dialog.

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

Setting options per port:

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

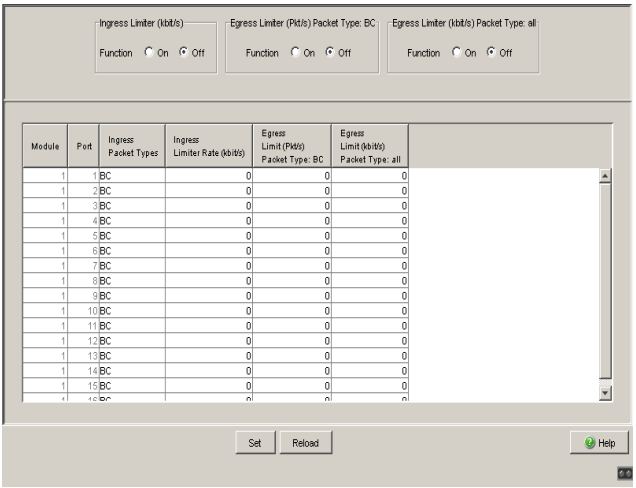


Figure 30: Rate Limiter

8.4 QoS/Priority

8.4.1 Description of Prioritization

This function helps prevent 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 “untrusted”.
- 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 83 “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 1Q standard. The VLAN tag consists of 4 bytes. It is inserted between the source address field and the type field.

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

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 9: Assignment of the priority entered in the tag to the traffic classes

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

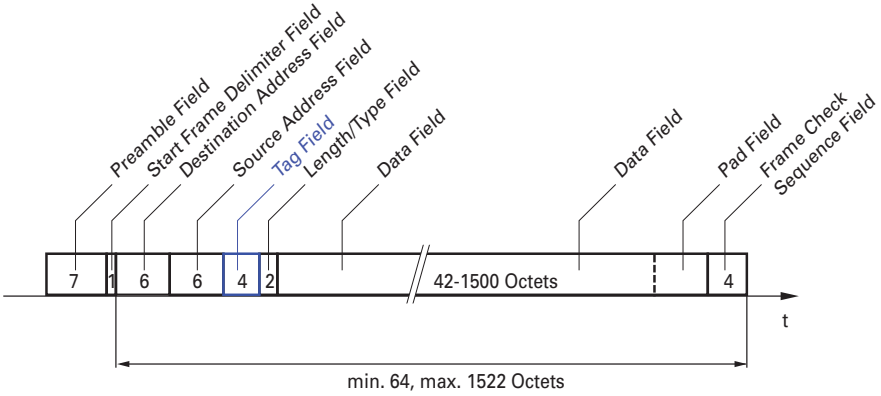


Figure 31: Ethernet data packet with tag

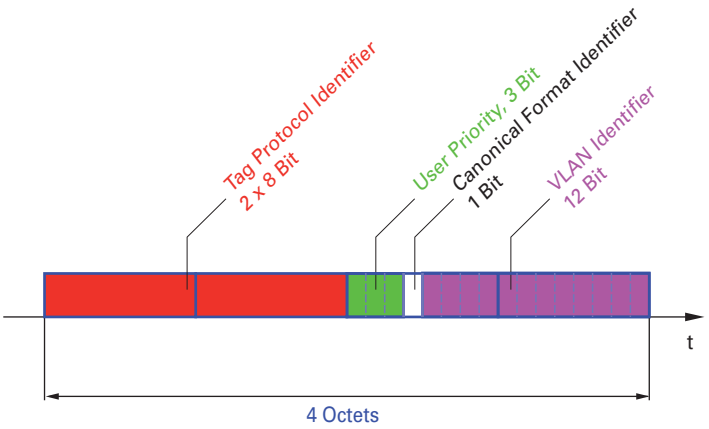


Figure 32: Tag format

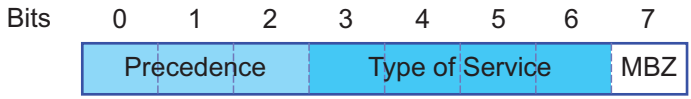
When using VLAN prioritizing, note the following special features:

- End-to-end prioritizing requires the VLAN tags to be transmitted to the entire network. Confirm that every network component is 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 10) 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		

Table 10: ToS field in the IP header

Bits (0-2): IP Precedence Defined	Bits (3-6): Type of Service Defined	Bit (7)
001 - Priority		
000 - Routine		

Table 10: ToS field in the IP header

Differentiated Services

The Differentiated Services field in the IP header (see figure 33) newly defined in RFC 2474 - often known as the DiffServ code point or DSCP - replaces the ToS field and is used to mark the individual packets with a DSCP. Here the packets are divided into different quality classes. The first 3 bits of the DSCP are used to divide the packets into classes. The next 3 bits are used to further divide the classes on the basis of different criteria. In contrast to the ToS byte, DiffServ uses 6 bits for the division into classes. This results in up to 64 different service classes.

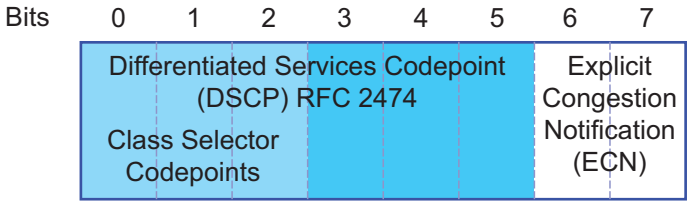


Figure 33: Differentiated Services field in the IP header

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

- Class Selector (CS0-CS7): For reasons of compatibility to TOS/IP Precedence
- Expedited Forwarding (EF): Premium service.
  Reduced delay, jitter + packet loss (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 helping ensure 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)
Immidiate	010	CS2 (010000)
Priority	001	CS1 (001000)
Routine	000	CS0 (000000)

Table 11: 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 12: 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, confirm that the configuration of the corresponding ports permits 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 144 “VLAN tagging”). You can modify this assignment. The device assigns the port priority to packets that it receives without a tag.
- untrusted
  The device ignores the priority information in the packet and always assigns the packets the port priority of the receiving port.
- trust ip-dscp
  The device assigns the IP packets to the different traffic classes according to the DSCP value in the IP header, even if the packet was also VLAN-tagged. The assignment is based on the pre-defined values (see table 12). 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 data packets that have a higher traffic class (higher priority) before transmitting a data packet with the next highest traffic class. The device transmits a data packet with the lowest traffic class (lowest priority) when there are no other data packets remaining in the queue. In unfortunate cases, the device not sends packets with a low priority if there is a high volume of high-priority traffic waiting to be sent on this port.
In applications that are time- or latency-critical, such as VoIP or video, Strict Priority enables high-priority data to be sent immediately..

8.4.7 Setting prioritization

Assigning the Port Priority

- ☐ Select the `QoS/Priority:Port Configuration` dialog.
- ☐ In the “Port Priority” column, you can specify the priority (0-7) with which the device sends data packets which it receives without a VLAN tag at this port.
- ☐ In the column "Trust Mode“, you have the option to control which criterion the the device uses to assign a traffic class to received data packets (see on page 143 “Description of Prioritization”).

Note: If you have set up VLANs, pay attention to the “VLAN 0 Transparent mode” (see `Switching:VLAN:Global`)

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

Assigning the VLAN Priority to the Traffic Classes

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

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

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

Assigning the traffic class to a DSCP

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

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

```
show classofservice ip-dscp-mapping

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

Always assign the DSCP priority to received IP data packets globally

☐ 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 159 “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-517A80"
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 cs7`	Assign the value cs7 to the management priority so that management packets with the highest priority are handled.
`exit`	Switch to the privileged EXEC mode.
`show network`	Displays the management VLAN priority.

```
System IP Address.............................. 10.0.1.116
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-517A80"
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 figure 34) 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.

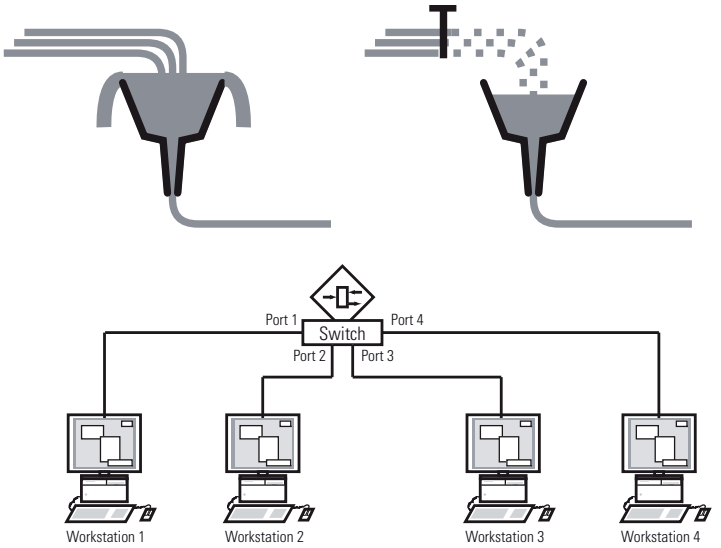


Figure 34: Example of flow control

- **Flow Control with a full duplex link**
  In the example (see figure 34) 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 figure 34) 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
`Basic Settings:Port Configuration` dialog.
In the “Activate Flow Control” column, you checkmark this port to specify that flow control is active here. You also activate the global “Flow Control” switch in the
`Switching:Switching Global` dialog.

☐ Select the `Switching:Switching Global` dialog.
With this dialog you can:

- switch off the flow control on all ports or
- switch on the flow control on those ports for which the flow control is selected in the port configuration table.

Note: When you are using a redundancy function, you deactivate the flow control on the participating ports. Default setting: flow control deactivated globally and activated on all ports.
If the flow control and the redundancy function are active at the same time, the redundancy may not work as intended.

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

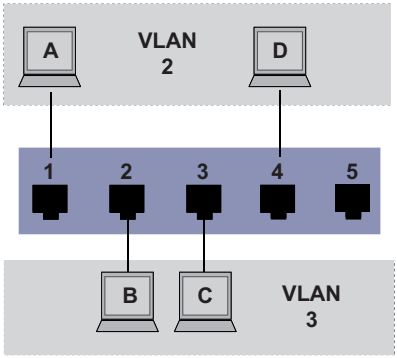


Figure 35: Example of a simple port-based VLAN

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 13: Ingress table

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

Table 14: Egress table

Proceed as follows to perform the example configuration:

☐ Configure VLAN

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

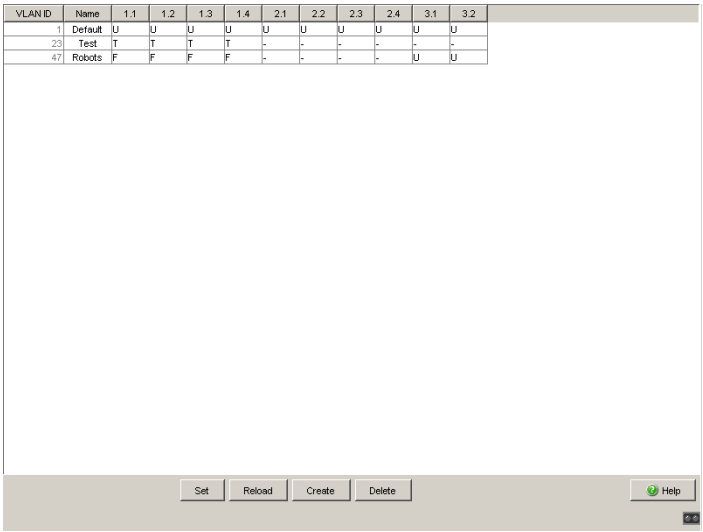


Figure 36: Creating and naming new VLANs

- ☐ 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`	Switch to the Privileged EXEC mode.
`vlan database`	Switch to the VLAN configuration mode.
`vlan 2`	Create a new VLAN with the VLAN ID 2.
`vlan name 2 VLAN2`	Give the VLAN with the VLAN ID 2 the name VLAN2.
`vlan 3`	Create a new VLAN with the VLAN ID 3.
`vlan name 3 VLAN3`	Give the VLAN with the VLAN ID 3 the name VLAN3.
`vlan name 1 VLAN1`	Give the VLAN with the VLAN ID 1 the name VLAN1.
`exit`	Leave the VLAN configuration mode.

`show vlan brief` Display the current VLAN configuration.

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

☐ Configuring the ports

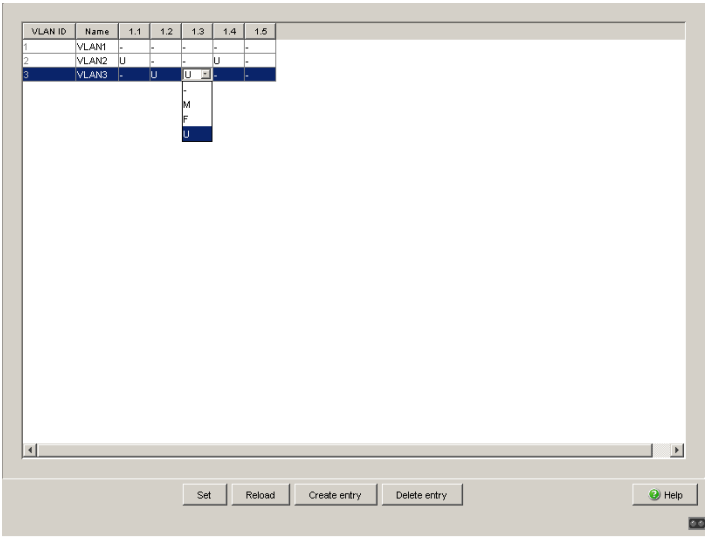


Figure 37: Defining the VLAN membership of the ports.

☐ 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.

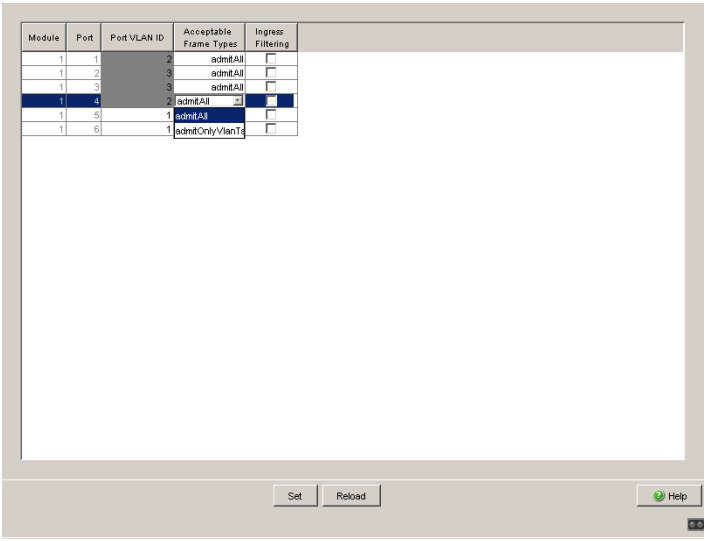


Figure 38: Assign and save Port VLAN ID, Acceptable Frame Types and Ingress Filtering

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

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

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

Example 2

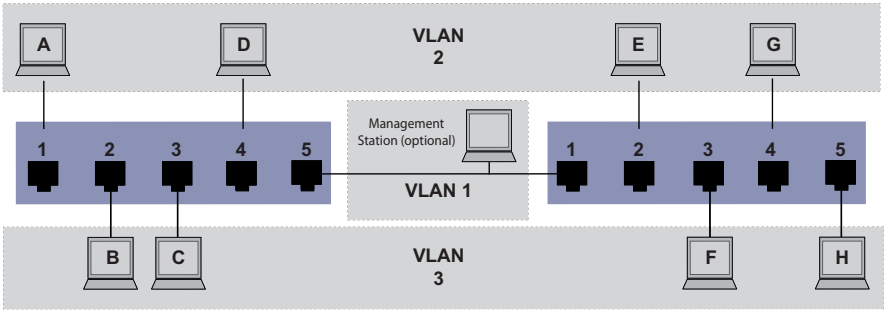


Figure 39: Example of a more complex VLAN constellation

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 144 “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 15: 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 16: 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 17: 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 18: 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.

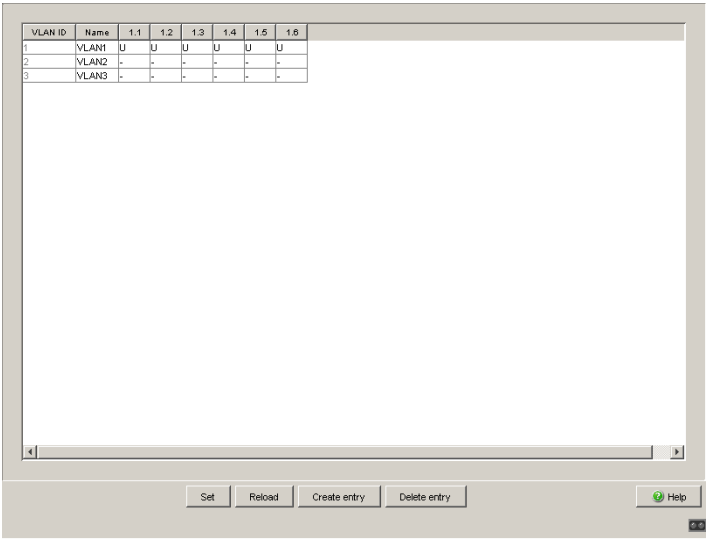


Figure 40: Creating and naming new VLANs

- ☐ 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

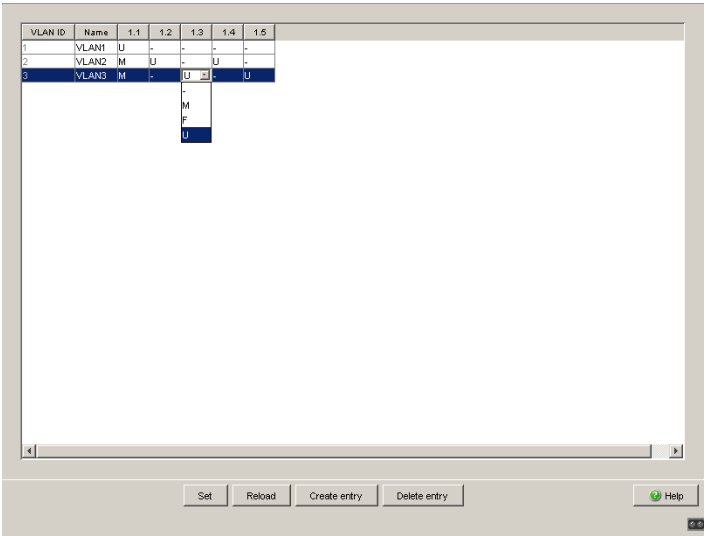


Figure 41: Defining the VLAN membership of the ports.

☐ 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.

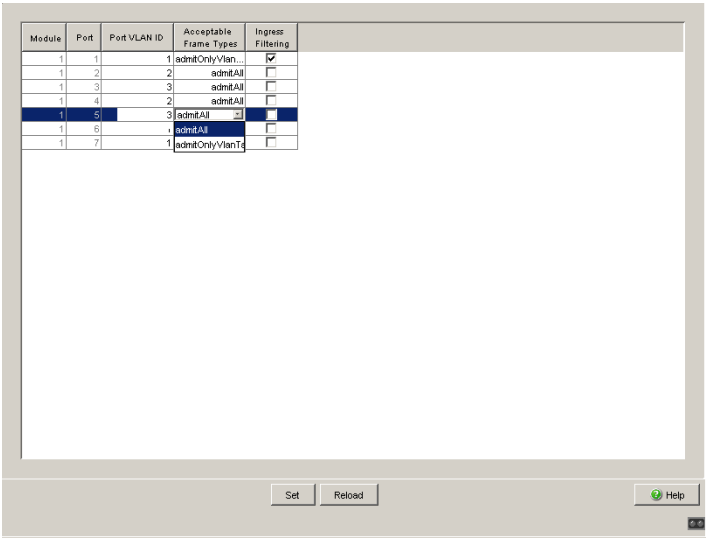


Figure 42: Assign and save Port VLAN ID, Acceptable Frame Types and Ingress Filtering

☐ 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 for
                              interface 1/2.
vlan participation include 2  Port 1/2 becomes member untagged in VLAN 2.
vlan pvid 2                   Port 1/2 is assigned the port VLAN ID 2.
exit                          Switch to the Configuration mode.
interface 1/3                 Switch to the Interface Configuration mode of
                              Interface 1/3.
vlan participation include 3  Port 1/3 becomes member untagged in VLAN 3.
vlan pvid 3                   Port 1/3 is assigned the port VLAN ID 3.
exit                          Switch to the Configuration mode.
interface 1/4                 Switch to the interface configuration mode of
                              interface 1/4.
vlan participation include 2  Port 1/4 becomes member untagged in VLAN 2.
vlan pvid 2                   Port 1/4 is assigned the port VLAN ID 2.
exit                          Switch to the Configuration mode.
interface 1/5                 Switch to the interface configuration mode for port
                              1.5.
vlan participation include 3  Port 1/5 becomes member untagged in VLAN 3.
vlan pvid 3                   Port 1/5 is assigned the port VLAN ID 3.
exit                          Switch to the Configuration mode.
exit                          Switch to the privileged EXEC mode.
show vlan 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 the device status
- Out-of-band signaling via signal contact
- Port status indication
- Event counter at port level
- Detecting non-matching duplex modes
- SFP status display
- Twisted pair cable diagnosis
- Topology Discovery
- Detecting IP address conflicts
- Detecting loops
- Reports
- Monitoring data traffic at a port (port mirroring)
- Syslog
- Event log

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 sent.

☐ In the column "Password", enter the community name that the device uses to identify itself as the trap's source.

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

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

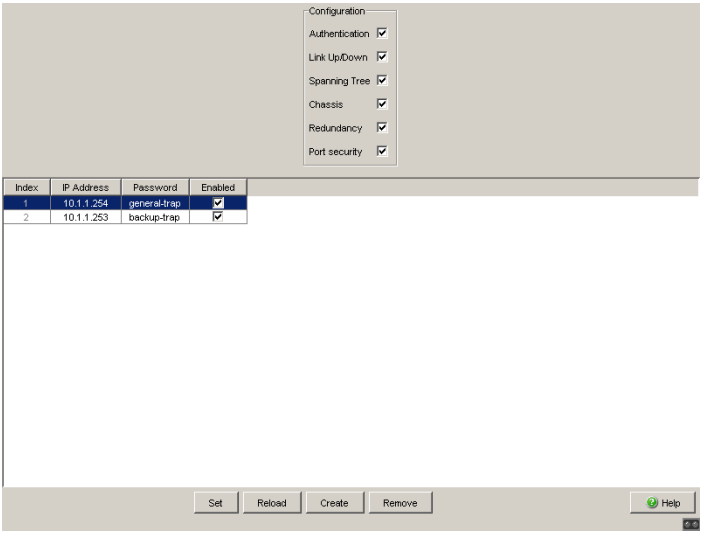


Figure 43: Alarms dialog

The events which can be selected are:

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

Table 19: Trap categories

9.2 Monitoring the Device Status

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

- signal the device status out-of-band via a signal contact (see on page 181 “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 configuration on the Memory Backup Adapter does not match that in the device.
- 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 84 “Displaying detected loss of connection”). 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 181 “Monitoring the Device Status via the Signal Contact”).

9.2.1 Configuring the Device Status

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

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

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

9.2.2 Displaying the Device Status

- ☐ Select the `Basics:System` dialog.

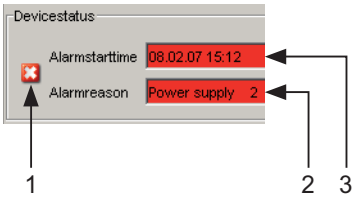


Figure 44: Device status and alarm display
1 - The symbol displays the device status
2 - Cause of the oldest existing alarm
3 - Start of the oldest existing alarm

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

9.3 Out-of-band Signaling

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

- Incorrect supply voltage,
  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 configuration on the Memory Backup Adapter does not match that in the device.
- 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 84 “Displaying detected loss of connection”). 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 181 “Monitoring the Device Status via the Signal Contact”).

9.3.1 Controlling the Signal Contact

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

Application options:

- Simulation of an error as an input for process control monitoring equipment.
- Remote control of a device via SNMP, such as switching on a camera.

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

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

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

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

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

9.3.2 Monitoring the Device Status via the Signal Contact

The "Device Status" option enables you, like in the operation monitoring, to monitor the device state (see on page 177 “Monitoring the Device Status”) via the signal contact.

9.3.3 Monitoring the Device Functions via the Signal Contact

Configuring the operation monitoring

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

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

Displaying the signal contact's status

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

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

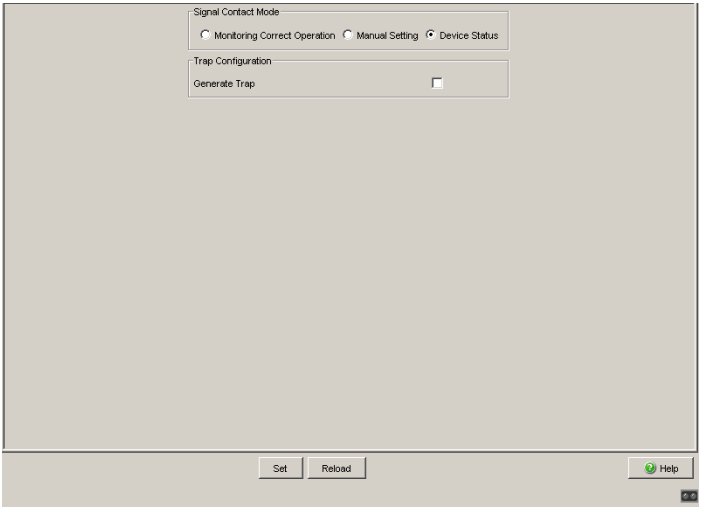


Figure 45: Signal Contact dialog

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

9.4 Port Status Indication

☐ Select the `Basics:System` dialog.

The device view shows the device with the current configuration. The status of the individual ports is indicated by one of the symbols listed below. You will get a full description of the port's status by positioning the mouse pointer over the port's symbol.

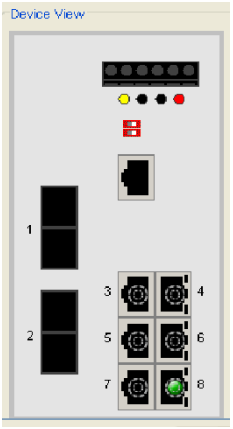


Figure 46: Device View

Meaning of the symbols:

The port (10, 100 Mbit/s, 1 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 (100 Mbit/s) is in the discarding mode of a redundancy protocol like e.g. Spanning Tree or HIPER-Ring.

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

Table 20: 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.

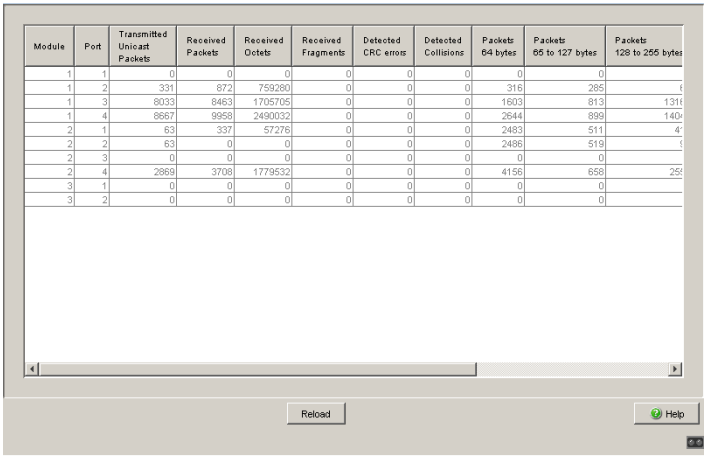


Figure 47: Port Statistics dialog

9.5.1 Detecting Non-matching Duplex Modes

If the duplex modes of 2 ports directly connected to each other do not match, this can cause problems that are difficult to track down. The automatic detection and reporting of this situation has the benefit of recognizing it before problems occur.

This situation can arise from an incorrect configuration, e.g. if you deactivate the automatic configuration at the remote port.

A typical effect of this non-matching is that at a low data rate, the connection seems to be functioning, but at a higher bi-directional traffic level the local device records a lot of CRC errors, and the connection falls significantly below its nominal capacity.

The device allows you to detect this situation and report it to the network management station. In the process, the device evaluates the error counters of the port in the context of the port settings.

Possible Causes of Port Error Events

The following table lists the duplex operating modes for TX ports together with the possible error events. The terms in the table mean:

- Collisions: In half-duplex mode, collisions mean normal operation.
- Duplex problem: Duplex modes do not match.
- EMI: Electromagnetic interference.
- Network extension: The network extension too great, or too many hubs are cascaded.
- Collisions, late collisions: In full-duplex mode, the port does not count collisions or late collisions.
- CRC error: The device only evaluates these errors as duplex mismatches in the manual full duplex mode.

No.	Autonegotiation	Current duplex mode	Detected error events (≥ 10)	Evaluation of duplex situation by device	Possible causes
1	On	Half duplex	None	OK	
2	On	Half duplex	Collisions	OK	
3	On	Half duplex	Late collisions	Duplex problem detected	Duplex problem, EMI, network extension
4	On	Half duplex	CRC error	OK	EMI
5	On	Full duplex	None	OK	
6	On	Full duplex	Collisions	OK	EMI
7	On	Full duplex	Late collisions	OK	EMI
8	On	Full duplex	CRC error	OK	EMI
9	Off	Half duplex	None	OK	
10	Off	Half duplex	Collisions	OK	
11	Off	Half duplex	Late collisions	Duplex problem detected	Duplex problem, EMI, network extension
12	Off	Half duplex	CRC error	OK	EMI
13	Off	Full duplex	None	OK	
14	Off	Full duplex	Collisions	OK	EMI
15	Off	Full duplex	Late collisions	OK	EMI
16	Off	Full duplex	CRC error	Duplex problem detected	Duplex problem, EMI

Table 21: Evaluation of non-matching of the duplex mode

Activating the detection

- ☐ Select the `Switching:Switching Global` dialog.
- ☐ Select “Activate Duplex Mismatch Detection”. The device then checks whether the duplex mode of a port might not match that of the remote port.
  If the device detects a potential mismatch, it creates an entry in the event log and sends an alarm (trap).

`enable`	Switch to the Privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`bridge duplex-mismatch-detect operation enable`	Activates the detection and reporting of non-matching duplex modes.
`bridge duplex-mismatch-detect operation disable`	Deactivates the detection and reporting of non-matching duplex modes.

9.5.2 TP Cable Diagnosis

The TP cable diagnosis allows you to check the connected cables for short-circuits or interruptions.

Note: While the check is running, the data traffic at this port is suspended.

The check takes a few seconds. After the check, the "Result" row contains the result of the cable diagnosis. If the result of the check detects a cable problem, then the "Distance" row contains the detected problem location’s distance from the port.

Result	Meaning
normal	The cable is okay.
open	The cable is interrupted.
short circuit	There is a short-circuit in the cable.
unknown	No cable check was performed yet, or it is currently running

Table 22: Meaning of the possible results

Prerequisites for correct TP cable diagnosis:
- 1000BASE-T port, connected to a 1000BASE-T port via 8-core cable or
- 10BASE-T/100BASE-TX port, connected to a 10BASE-T/100BASE-TX port.

9.5.3 Port Monitor

When you enable this feature the device monitors the port states. The device offers you the ability to disable individual ports or send a trap when user-defined conditions occur.

Definable port conditions are:
- Link Flap
- CRC/Fragments
- Overload Detection
- Speed and duplex combination

In the "Global" dialog, you activate the configurations defined in the "Link Flap", "CRC/Fragments" and "Overload Detection" tabs. The device detects these conditions when you activate the functions. If the device detects the user defined condition on a port, it produces the response defined for that port.

Link Flapping occurs when a link alternately advertises its link state as up and down. You configure the device to detect this condition and then define whether to send a trap or shut the port off.

Using the Cyclical Redundancy Check (CRC) the device detects data packets modified during the transmission based on the checksum. The device detects the total number of packets received that were less than 64 octets in length, excluding framing bits, but including FCS octets, and had either a FCS error or an Alignment Error.
- A FCS error is a bad Frame Check Sequence (FCS) with an integral number of octets.
- An Alignment Error is a bad FCS with a non-integral number of octets.

The device monitors both criteria if you enable the function in the "Global" tab. If the number of occurred CRC/fragment errors exceeds the specified threshold, the device executes the user-specified action.

Overload Detection helps prevent a broadcast, multicast, or unicast storm from disrupting traffic on a port. The Overload Detection function monitors packets passing from a port to the switching bus to determine if the packet is unicast, multicast, or broadcast. The switch counts the number of user-defined packets received within the "Sampling Interval " and compares the measurement with a user-defined threshold. The port blocks traffic after reaching the "Upper Threshold". When you activate the recovery function for Overload Detection, the port remains blocked until the traffic rate drops below the "Lower Threshold" and then forwards traffic as normal.

The device allows you to specify which duplex mode is allowed for which speed for a specific port. The monitoring of the combination of speed and duplex mode helps prevent any undesired connections.

- ☐ Open the "Diagnositics:Ports:Port Monitor" dialog.

- ☐ Open the "Link Flap" tab.
- ☐ Define the number of times that a port cycles between link up and link down before the function disables the port, in the "Link Flap Count" text box, in the "Parameter" frame.
- ☐ Define the elapse time in the "Sample Interval [s]" text box in the "Parameter" frame.

- ☐ Open the "CRC/Fragments" tab.
- ☐ Define the number of packets received containing changes in raw data or fragment packets received before the function disables the port, in the "CRC/Fragments count [ppm]" text box, in the "Parameter" frame.
- ☐ Define the elapse time in the "Sample Interval [s]" text box in the "Parameter" frame.

- ☐ Open the "Overload Detection" tab.
- ☐ Define the elapse time in the "Sample Interval [s]" text box in the "Parameter" frame.
- ☐ For each port, define the type of traffic to monitor in the "Traffic Type" column.
- ☐ For each port, define the type of threshold to use in the "Threshold Type" column.
- ☐ For each port, define the threshold at which the device enables the port in the "Lower Threshold" column.
- ☐ For each port, define the threshold at which the device disables the port in the "Upper Threshold" column.

- ☐ Open the "Speed Duplex" tab.

☐ You define for each port which duplex mode is allowed for which speed.
- "hdx" = half duplex
- "fdx" = full duplex
- "10" = 10 Mbit/s
- "100" = 100 Mbit/s

etc.

☐ Open the "Global" tab.
☐ In the "Port Monitor on" column of the "Global" tab, select the ports to monitor.
☐ To activate the Port Monitor function, click `On` in the "Operation" frame.

9.5.4 Auto Disable

If the configuration shows a port as enabled, but the device detects an error, the software shuts down that port. In other words, the device software disables the port because of a detected error condition.

When a port is auto-disabled, the device effectively shuts down the port and the port blocks traffic. The port LED blinks green 3 times per period and identifies the reason for the shutdown. In addition, the device generates a log entry listing the reason for the auto-disable. When you enable the port after a timeout by auto-disable, the device generates a log entry.

This feature provides a recovery function which automatically enables an auto-disabled port after a user-defined time. When this function enables a port, the device sends a trap with the port number and an empty "Reason" entry.

The auto-disable function serves the following purposes:
- It assists the network administrator in port analysis.
- It helps eliminate the possibility that this port causes other ports on the module (or the entire module) to shut down.

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

So that the device enables the ports again that were disabled because of a detected error state, complete the following steps:

- ☐ Open the `Diagnostics > Ports > Auto Disable` dialog.
- ☐ To enable ports again that the device has disabled due to link flaps, in the "Configuration" frame mark the "Link Flap" checkbox.
  You define the parameters that cause the ports to be disabled due to link flaps in the "Diagnostics:Ports:Port Monitor" dialog, on the "Link Flap" tab.

- ☐ To enable ports again that the device has disabled due to CRC or fragment errors, on the "Configuration" frame mark the "CRC Error" checkbox.
  You define the parameters that cause the ports to be disabled due to CRC or fragment errors in the "Diagnostics:Ports:Port Monitor" dialog, on the "CRC/Fragments" tab.
- ☐ To enable ports again that the device has disabled due to an overload, in the "Configuration" frame mark the "Overload Detection" checkbox.
  You define the parameters that cause the ports to be disabled due to an overload in the "Diagnostics:Ports:Port Monitor" dialog, on the "Overload Detection" tab.
- ☐ To enable ports again that the device disabled due to an incorrect speed and duplex combination, in the "Configuration" frame mark the "Speed Duplex" checkbox.
  You define the parameters that cause the ports to be disabled due to an incorrect speed and duplex combination in the "Diagnostics:Ports:Port Monitor" dialog, on the "Speed Duplex" tab.
- ☐ To enable ports again that the device disabled due to an unauthorized access to the port, in the "Configuration" frame you mark the "Port Security" checkbox.
  You define the parameters that cause the ports to be disabled due to unauthorized access in the "Security:Port Security" dialog.
- ☐ You define the time until each port is automatically enabled again in the "Reset Timer [s]" column in the table.

9.6 Topology Discovery

9.6.1 Description of Topology Discovery

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

A device with active LLDP

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

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

- Chassis ID (its MAC address)
- Port ID (its port MAC address)
- Description of the port
- System Name
- System description
- Supported system capabilities
- Currently activated system capabilities
- Interface ID of the management address
- Port VLAN ID of the port
- Status of the autonegotiation at the port
- Medium, half and full duplex settings and speed setting of the port

- Information about whether a redundancy protocol is switched on at the port, and which one (for example, RSTP, HIPER-Ring, Fast-HIPER-Ring, MRP, Ring Coupling).
- Information about the VLANs which are set up in the switch (VLAN ID and VLAN name, regardless of whether the port is a VLAN member).

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. When a non-LLDP-capable device is placed between 2 LLDP-capable devices, it inhibits the LLDP information exchange between these two devices. To get around this, Schneider Electric devices send and receive additional LLDP packets with the Schneider Electric Multicast MAC address 01:80:63:2F:FF:0B. Schneider Electric devices with the LLDP function are thus also able to exchange LLDP information with each other via devices that are not LLDP-capable.

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

9.6.2 Displaying the Topology Discovery Results

☐ Select the `Diagnostics:Topology Discovery` dialog.
The table on the “LLDP” tab page shows you the collected LLDP information for neighboring devices. This information enables the network management station to map the structure of your network.

Activating “Display FDB entries” below the table allows you to add entries for devices without active LLDP support to the table. In this case, the device also includes information from its FDB (forwarding database).

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

then
- the topology table hides the devices without active topology discovery.

If
- only devices without active topology discovery are connected to a port

then
- the table will contain one line for this port to represent all devices. This line contains the number of connected devices.
  MAC addresses of devices that the topology table hides for the sake of clarity, are located in the address table (FDB), (see on page 126 “Entering Static Addresses”).

9.7 Detecting IP Address Conflicts

9.7.1 Description of IP Address Conflicts

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

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

Table 23: 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 23).

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.

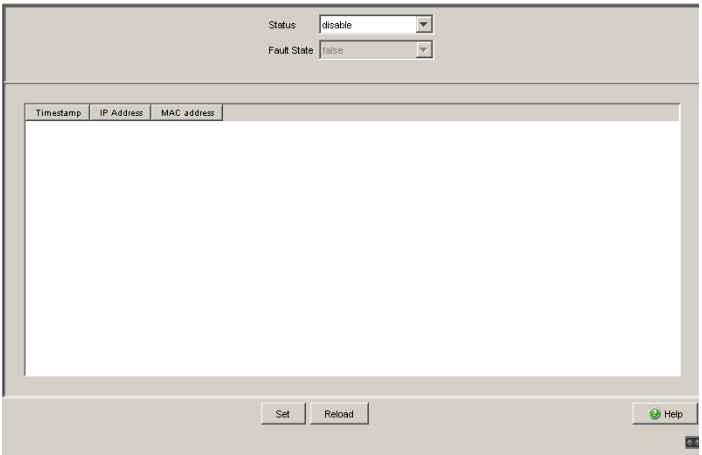


Figure 48: IP Address Conflict Detection dialog

9.8 Detecting Loops

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

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

To avoid loops during the configuration phase, configure all the devices of the ring individually. Before you connect the redundant line, you must complete the configuration of all the devices of the ring.

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

An incorrect configuration can cause a loop, for example, if you deactivate Spanning Tree.

The device allows you to detect the effects typically caused by loops and report this situation automatically to the network management station. You have the option here to specify the magnitude of the loop effects that triggers the device to send a report.

A typical effect of a loop is that frames from multiple different MAC source addresses can be received at different ports of the device within a short time. The device evaluates how many of the same MAC source addresses it has learned at different ports within a time period. This process detects loops when the same MAC address is received at different ports.
Conversely, the same MAC address being received at different ports can also have other causes than a loop.

☐ Select the `Switching:Switching Global` dialog.
☐ Select “Enable address relearn detection”. Enter the desired threshold value in the “Address relearn threshold” field.

If the address relearn detection is enabled, the device checks whether it has repeatedly learned the same MAC source addresses at different ports. This process very probably indicates a loop situation.
If the device detects that the threshold value set for the MAC addresses has been exceeded at its ports during the evaluation period (a few seconds), the device creates an entry in the log file and sends an alarm (trap). The preset threshold value is 1.

9.9 Reports

The following reports and buttons are available for the diagnostics:

- Log file.
  The log file is an HTML file in which the device writes all the important device-internal events.
- System information.
  The system information is an HTML file containing all system-relevant data.
- Download Switch-Dump.
  This button allows you to download system information as files in a ZIP archive.

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

The following button is available as an alternative for operating the Web-based interface:

- Download JAR file.
  This button allows you to download the applet of the Web-based interface as a JAR file. Then you have the option to start the applet outside of a browser.
  This facilitates the device administration even when you have disabled its web server for security reasons.

☐ To display the HTML file with system-relevant data, select the dialog `Diagnosis:Report:System Information`.
☐ To view the log file with important device-internal events, select the dialog `Diagnosis:Report:Event Log`.

☐ Select the `Diagnosis:Report` dialog.

☐ Click “Download Switch Dump”.

☐ Select the directory in which you want to save the switch dump.

☐ Click “Save”.

The device creates the file name of the switch dumps automatically in the format <IP address>_<system name>.zip, e.g. for a device of the type TCSESM-E: “10.0.1.112_TCSESM063F2CU1.zip”.

☐ Click “Download JAR-File”.

☐ Select the directory in which you want to save the applet.

☐ Click “Save”.

The device creates the file name of the applet automatically in the format <device type><software version)>_<software revision of applet>.jar, e.g. for a device of type TCSESM-E: “tcsesm_e06000_00.jar”.

9.10 Monitoring Data Traffic at Ports (Port Mirroring)

The port mirroring function enables you to review the data traffic at up to 8 ports of the device for diagnostic purposes. The device additionally forwards (mirrors) the data for these ports to another port. This process is also called port mirroring.
The ports to be reviewed are known as source ports. The port to which the data to be reviewed is copied is called the destination port. You can only use physical ports as source or destination ports.

In port mirroring, the device copies valid data packets of the source port to the destination port. The device does not affect the data traffic on the source ports during port mirroring.
A management tool connected at the destination port, e.g. an RMON probe, can thus monitor the data traffic of the source ports in the sending and receiving directions.

When selecting "RX" as the monitoring direction on a source port, only frames received on the source port will be copied/mirrored to the destination port (monitoring ingress).
When selecting "TX" as the monitoring direction on a source port, only frames transmitted on the source port will be copied/mirrored to the destination port (monitoring egress).

With port mirroring active, the device copies the traffic received and/or forwarded on a source port to the destination port.

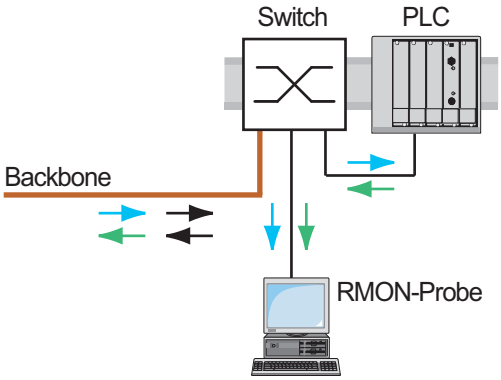


Figure 49: Port mirroring

☐ Select the `Diagnostics:Port Mirroring` dialog.

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

☐ Select the source ports whose data traffic you want to review from the list of physical ports by checkmarking the relevant boxes.
You can select a maximum of 8 source ports. Ports that cannot be selected are displayed as inactive by the device, e.g. the port currently being used as the destination port, or if you have already selected 8 ports. Default setting: no source ports.

☐ Select the destination port to which you have connected your management tool from the list element in the “Destination Port” frame.
The device does not display ports that cannot be selected in the list, e.g. the ports currently being used as source ports. Default setting: port 0.0 (no destination port).

☐ Select “On” in the “Function” frame to switch on the function. Default setting: “Off”.

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

Note: When port mirroring is active, the specified destination port is used solely for reviewing, and does not participate in the normal data traffic.

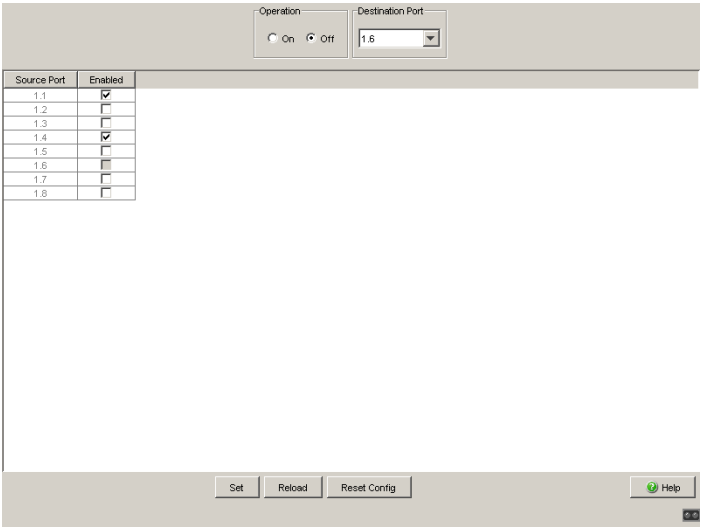


Figure 50: Dialog Port Mirroring

9.11 Syslog

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

Note: You will find the actual events that the device has logged in the "Event Log" (see on page 211 “Trap log”) and in the log file (see on page 203 “Reports”), a HTML page with the title "Event Log".

- ☐ Select the "Diagnostics:Syslog" dialog.

- ☐ Activate the Syslog function in the "Operation" frame.
- ☐ Click on "Create".
- ☐ In the "IP Address" column, enter the IP address of the syslog server to which the log entries should be sent.
- ☐ In the "Port" column, enter the UDP port of the syslog server at which the syslog receives log entries. The default setting is 514.
- ☐ In the "Minimum level to report" column, confirm that you enter the minimum level of seriousness required for an event to attain for the device to send a log entry to this syslog server.
- ☐ In the "Active" column, you select the syslog servers that the device takes into account when it is sending logs.

“SNMP Logging” frame:

- ☐ Activate “Log SNMP Get Request” if you want to send reading SNMP requests to the device as events to the syslog server.
- ☐ Select the level to report at which the device creates the events from reading SNMP requests.
- ☐ Activate “Log SNMP Set Request” if you want to send writing SNMP requests to the device as events to the syslog server.
- ☐ Activate “Log SNMP Set Request” if you want to send writing SNMP requests to the device as events to the syslog server.

Note: For more details on setting the SNMP logging, see the “Syslog” chapter in the “GUI” (Graphical User Interface / Web-based Interface) reference manual.

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`logging host 10.0.1.159 514 3`	Select the recipient of the log messages and its port 514. The “3” indicates the seriousness of the message sent by the device. “3” means “error”.
`logging syslog`	Enable the Syslog function.
`exit`	Switch to the privileged EXEC mode.
`show logging hosts`	Display the syslog host settings.

```
Index     IP Address       Severity   Port     Status
-----  -----------------  ----------  ----  -------------
1      10.0.1.159         error       514   Active
```

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

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

9.12 Trap log

The device allows you to call up a log of the system events. The table of the “Trap Log” dialog lists the logged events with a time stamp.

- ☐ Click “Reload” to update the content of the trap log.
- ☐ Click “Clear” to delete the content of the trap log.

Note: You have the option to also send the logged events to one or more syslog servers (see on page 208 “Syslog”).

10 EtherNet/IP

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

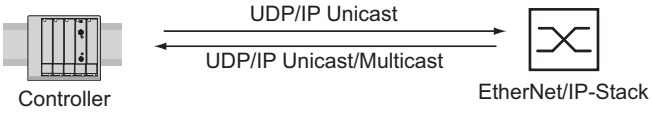


Figure 51: Communication between the controller (PLC) and the Switch

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

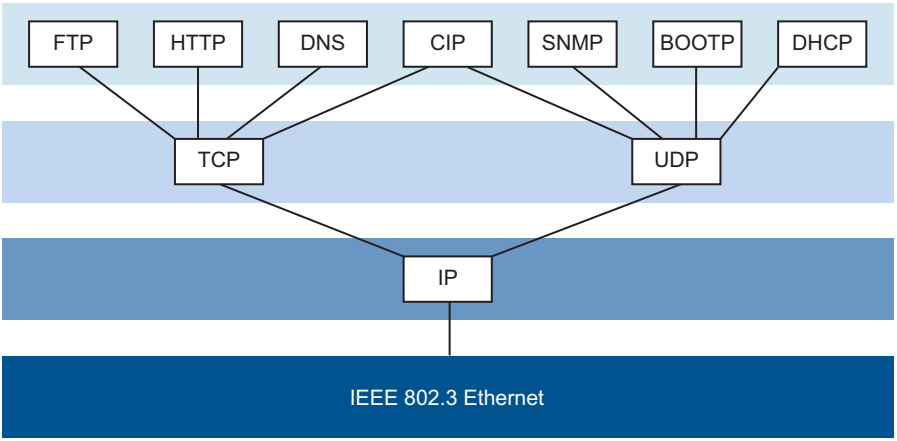


Figure 52: EtherNet/IP (CIP) in the ISO/OSI reference model

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 theSwitch, you configure it according to the “Basic Configuration” user manual. Then:

☐ Use the Web-based interface in the `Switching:Multicasts:IGMP` dialog to check whether the IGMP Snooping is activated.

☐ Use the Web-based interface in the `Advanced:Industry Protocols` dialog to check whether EtherNet/IP is activated.

☐ Use the Web-based interface in the `Advanced:Industry Protocols` dialog to download the EDS (EtherNet/IP configuration file) and the icon to 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 24: 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.

Table 25: TCP/IP Interface Object

Id	Attribute	Access rule	Data type	Description
5	Interface Configuration	Set/Get	Structure: UDINT IP address UDINT Netmask 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 25: 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 unsuccessful, 2: unsuccessful 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 Jeweils UDINT	InOctets, InUcastPackets, InNUcastPackets, InDiscards, InErrors, InUnknownProtos, OutOctets, OutUcastPackets, OutNUcastPackets, OutDiscards, OutErrors.
5	Media Counters	Get	Struct Ethernet MIB Counters Jeweils 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.
7	Interface Type	Get	USINT	Value 0: Unknown interface type, Value 1: The interface is internal, Value 2: Twisted-pair, Value 3: Optical fiber.

Table 26: Ethernet Link Object

Id	Attribute	Access rule	Data type	Description
8	Interface State	Get	USINT	Value 0: Unknown interface state, Value 1: The interface is enabled, Value 2: The interface is disabled, Value 3: The interface is testing,
9	Admin State	Set	USINT	Value 1: Enable the interface, Value 2: Disable the interface.
10	Interface Label	Get	SHORT_ STRING	Interface name. The content of the string is vendor-specific.

Table 26: 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 hmIfaceUtilization 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 hmIfaceUtilizationAlarmUpperThreshold 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 hmIfaceUtilizationAlarmLowerThreshold can be accessed. Utilization in percentage[a]. RX Interface Utilization Lower Limit.

Table 27: Schneider Electric extensions for the Ethernet Link Object

Id	Attribute	Access rule	Data type	Description
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 27: 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 $95_{H,}$ 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: failed) Like the signal contact.
	Bit 1	Power Supply 1 (0: ok, 1: failed or does not exist)
	Bit 2	Power Supply 2 (0: ok, 1: failed or does not exist)
	Bit 3	Power Supply 3 (0: ok or not possible on this platform, 1: failed or does not exist)
	Bit 4	Power Supply 4 (0: ok or not possible on this platform, 1: failed or does not exist)
	Bit 5	Power Supply 5 (0: ok or not possible on this platform, 1: failed or does not exist)
	Bit 6	Power Supply 6 (0: ok or not possible on this platform, 1: failed or does not exist)
	Bit 7	Power Supply 7 (0: ok or not possible on this platform, 1: failed or does not exist)
	Bit 8	Power Supply 8 (0: ok or not possible on this platform, 1: failed or does not exist)
	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 ports 1&2, 1: module 2, ports 1&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 Error (1: link inoperable)
Switch Temperature	ID 02	Struct{INT RO Temperature °F, INT RO Temperature °C}

Table 28: Schneider Electric Ethernet Switch Agent Object

Attribute	ID/Bit No.	Description
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)
	Bit 8-10 RW	Treatment of Unknown Multicasts: 0: Send To All Ports, 1: Send To Query Ports, 2: Discard
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 to 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 to 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 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 28: 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 RSTP Bridge Object

For the device TCSESM-E.
RSTP is a layer 2 protocol that enables the use of a redundant Ethernet topology (e.g., a ring topology). RSTP is specified in Chapter 17 of IEEE 802.1D-2004.

The Switch supports the Schneider Electric-specific RSTP Bridge Object (class code $64_{H,}$ 100) for the Switch configuration and information parameters.

The device supports 2 instances:
- Instance 1 represents the bridge‘s primary RSTP instance, and
- instance 2 represents the secondary (Dual) RSTP instance.

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

Id	Attribute	Access rule	Data type	Description
1	Bridge Identifier Priority	Set	UDINT	Range: 0 to 61,440 in steps of 4,096, default: 32,768 (refer to IEEE, 802.1D-2004, § 17.13.7)
2	Transmit Hold Count	Set	UINT	Range: 1 to 40, default: 10 (refer to IEEE 802.1D-2004, §17.13.12)
3	Force Protocol Version	Set	UINT	Default:2 (refer to IEEE 802.1D-2004, §17.13.4 and dot1dStpVersion in RFC 4318)
4	Bridge Hello Time	Set	UDINT	Range: 100 to 200, unit: centi-seconds (1/100 of a second), default: 200 (refer to IEEE 802.1D-2004, §17.13.6 and dot1dStpHoldTime in RFC 4188)
5	Bridge Forward Delay	Set	UDINT	Range: 400 to 3000, unit: centi-seconds, default: 2100 (refer to IEEE 802.1D-2004, §17.13.5 and dot1dStpForwardDelay in RFC 4188)
6	Bridge Max. Age	Set	UINT	Range: 600 to 4000, unit: centi-seconds, default: 4000 (refer to IEEE 802.1D-2004, §17.13.8 and dot1dStpBridgeMaxAge in RFC 4188)
7	Time Since Topology Change	Get	UDINT	Unit: centi-seconds (refer to dot1dStpTimeSinceTopologyChange in RFC 4188)

Table 29: Schneider Electric RSTP Bridge Object

Id	Attribute	Access rule	Data type	Description
8	Topology Change	Get	UDINT	Refer to dot1dStpTopChanges in RFC 4188
100	InnerPort	Get	UINT	Schneider Electric-specific object. ▶ For instance 1, it holds the port number of the DRSTP Primary instance's inner port. ▶ For instance 2, it holds the port number of the DRSTP Secondary instance's inner port.
101	OuterPort	Get	UINT	Schneider Electric-specific object. ▶ For instance 1, it holds the port number of the DRSTP Primary instance's outer port. ▶ For instance 2, it holds the port number of the DRSTP Secondary instance's outer port.

Table 29: Schneider Electric RSTP Bridge Object

10.2.6 RSTP Port Object

For the device TCSESM-E.
The Switch supports the Schneider Electric-specific RSTP Port Object (class code $65_{H,}$ 101) for the RSTP port configuration and information parameters with at least one instance.
Instance 1 represents the CPU's Ethernet Interface, instance 2 represents the 1st physical port, instance 3 the 2nd physical port, and so on.

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

Id	Attribute	Access rule	Data type	Description
1	Port Identifier Priority	Set	UDINT	Range: 0 to 240 in steps of 16, default: 128 (refer to IEEE, 802.1D-2004, § 17.13.10).
2	mcheck	Set	BOOL	True (1), False (2) (refer to IEEE 802.1D-2004, §17.19.13 and dot1dStpPortProtocolMigration in RFC 4318).
3	Port Path Cost	Set	UDINT	Range: 1 to 200,00,000, default:auto (0) (refer to IEEE 802.1D-2004, §17.13.11 and dot1dStpPortAdminPathCost in RFC 4318).
4	Port Admin Edge Port	Set	BOOL	True (1), False (2) (refer to IEEE 802.1D-2004, §17.13.1 and dot1dStpPortAdminEdgePort in RFC 4318).
5	Port Oper Edge Port	Get	BOOL	True (1), False (2) (refer to dot1dStpPortOperEdgePort in RFC 4318).
6	Port Admin PointToPoint	Set	UINT	forceTrue (0), forceFalse (1), auto (2) (refer to dot1dStpPortAdminPointToPoint in RFC 4318).
7	Port Oper PointToPoint	Get	UINT	True (1), False (2) (refer to dot1dStpPortOperPointToPoint in RFC 4318).
8	Port Enable	Set	UINT	Enabled (1), Disabled (2) (Refer to dot1dStpPortEnable in RFC 4188).
9	Port State	Get	UINT	Disabled (1), Blocking (2), Listening (3), Learning (4), Forwarding (5), Broken (6) (refer to dot1dStpPortState in RFC 4188).

Table 30: Schneider Electric RSTP Port Object

Id	Attribute	Access rule	Data type	Description
10	Port Role	Get	UNT	Unknown (0), Alternate/Backup (1), Root (2), Designated (3) (refer to dot1dStpTopChanges in RFC 4188).
100	DRSTP	Get	UINT	Schneider Electric-specific object. True (1), False (2).

Table 30: Schneider Electric RSTP Port Object

10.2.7 I/O Data

You will find the exact meaning of the individual bits of the device status in the I/O data in “Ethernet Switch Agent Object” on page 222.

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 31: I/O Data

10.2.8 Assignment of the Ethernet Link Object Instances

The table shows the assignment of the Switch ports to the Ethernet Link Object Instances.

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 32: Assignment of the Switch ports to the Ethernet Link Object Instances

10.2.9 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 Interface Object	Ethernet Link Object	Switch Agent Object
Get Attribute All (01H)	All Attributes	All Attributes	All Attributes	All Attributes
Set Attribute All (02H)	-	Settable Attributes (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 Configuration (35H) Vendor-specific	Parameter (0,1)	-	-	Save Switch Configuration

Table 33: Supported Services

10.3 TCSESM/TCSESM-E in a Premium System

The section describes the configuration of a TCSESM/TCSESM-E 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.

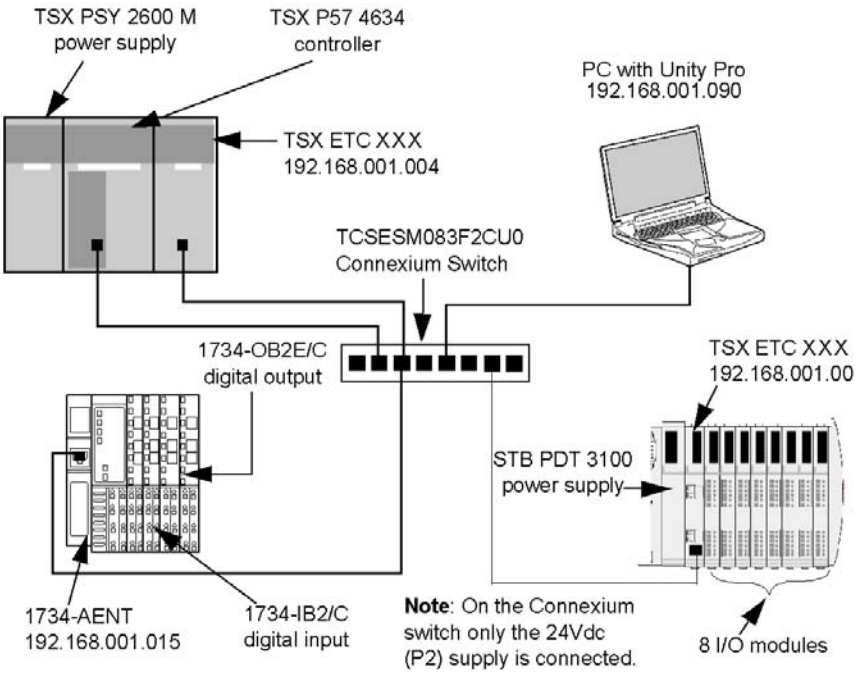


Figure 53: Required hardware and the connections involved to develop a network topology

To re-create this example, confirm that you:
- use the IP addresses for your own configurations
  - PC
  - STB NIC 2212 EtherNet/IP network interface module
  - 1734-AENT Point IO 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 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.

10.3.1 Adding EDS Files

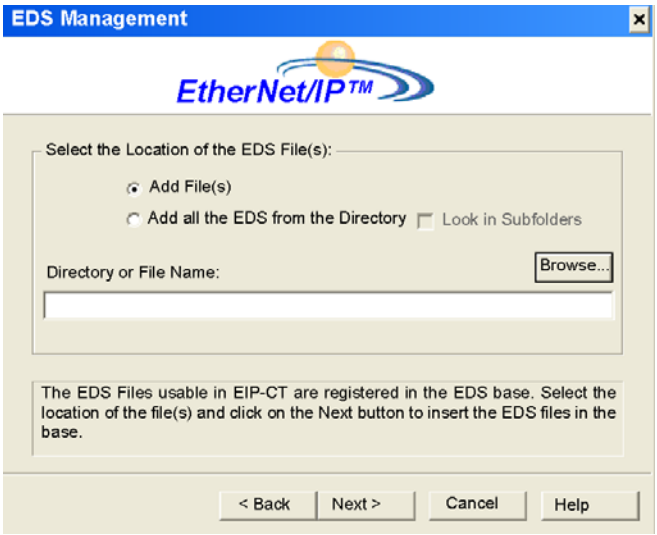
Before the TCSESM switch can be configured in a Premium system, the TCSESM EDS file has to be added to the Unity Pro EtherNet/IP Device Library. Unity Pro includes an EDS Management wizard that you can use to add one or more EDS files to the Device Library.

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.

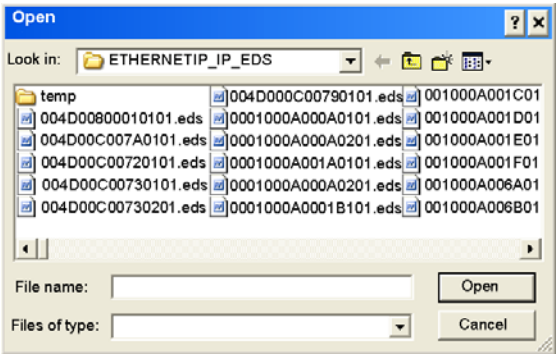
10.3.2 Adding one or more EDS files to the Device Library

☐ 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.



☐ 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.

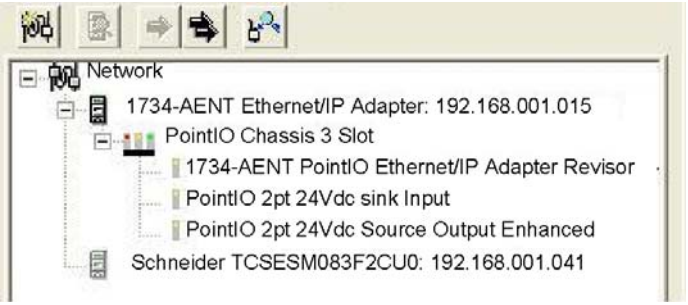
10.3.3 Automatically Detect and Add the TCSESM Switch

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: Confirm that the TCSESM is 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.



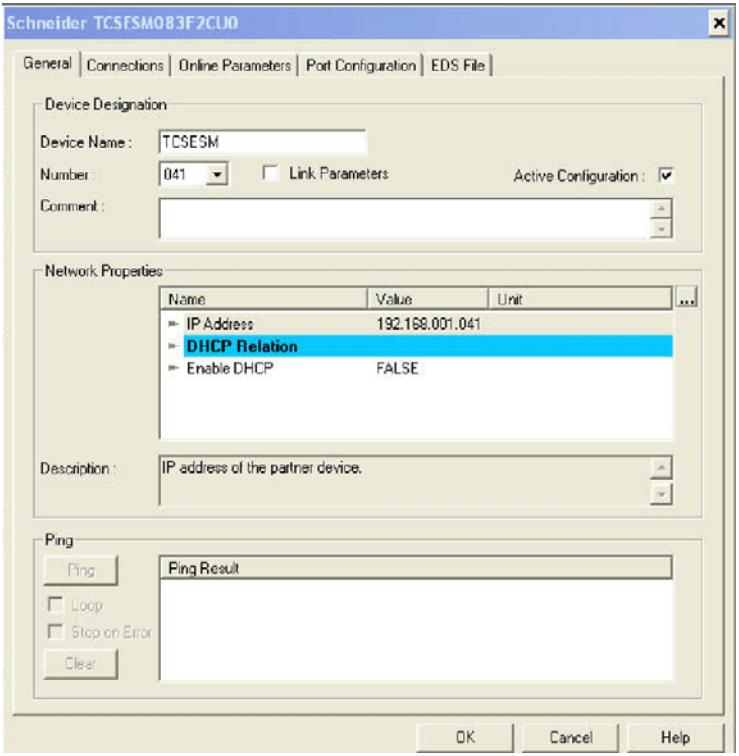
- ☐ Select the "1734-AENT PointIO Ethernet/IP Adapter Revisor" in the "Network Detection" window.
- ☐ Click the "Insert in Configuration" button ➡ to open the "Properties" window.

10.3.4 Configuration of the TCSESM properties

The "TCSESM switch properties" window provides the following tab pages. In the following example, you only need to edit a few of these pages:

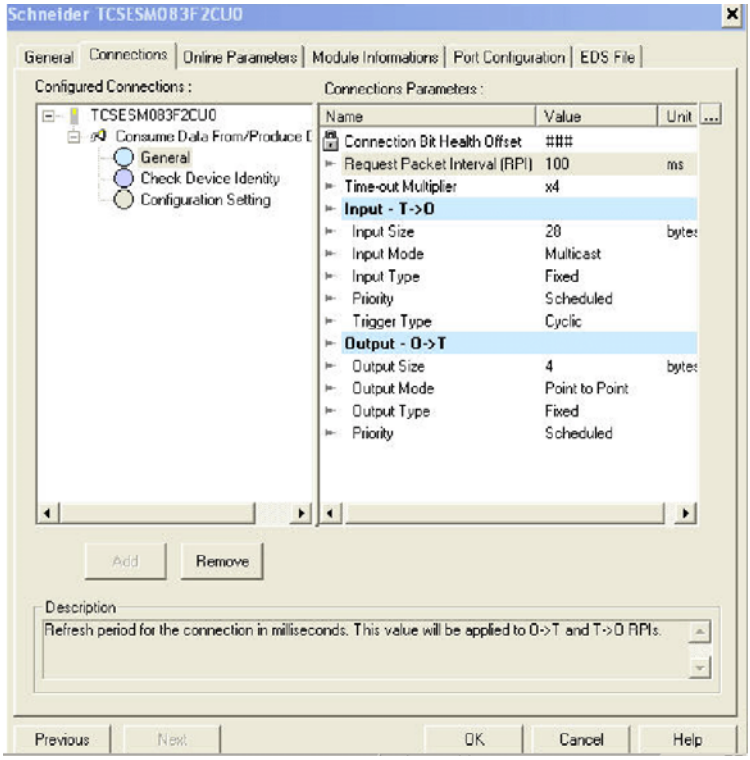
On this page	Perform the following
General	- Name of the input device - Configure IP address - Add the device to the project configuration
Connections	Apply the standard settings.
Online Parameters	Apply the standard settings (if available).
Module information	(Read-only page – no configuration required)
Connection configuration	(Read-only page – no configuration required)
EDS File	(Read-only page – no configuration required)

The following settings are used for the configuration example:
☐ Click the "General" page:



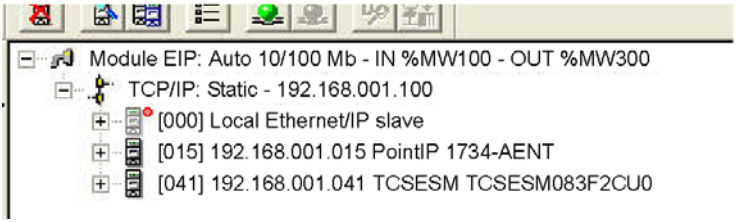
☐ On the "General" page, edit the following settings:
- Device Designation: TCSESM
- Number: The position of the device in the "Device" window - in this example, enter 041.
- Active Configuration: Confirm that this checkbox is selected.
- IP Address: 192.168.001.041

☐ Click the "Connections" 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 "TCSESM switch properties" window.
A node is added to the project configuration in the "Devices" window:



The next step involves monitoring the inputs and outputs of the external device.

10.3.5 Viewing the TCSESM Switch Data

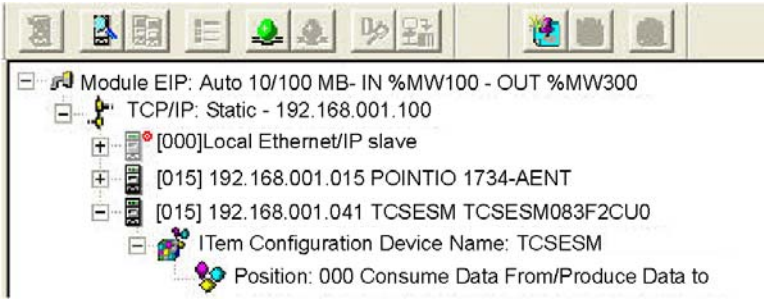
Because the Device Library includes EDS files for the TCSESM switch PointIO adapter and its discrete input and output modules, the Unity Pro EtherNet/IP configuration tool automatically:

- 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, confirm that each analog module is connected to the TCSESM using a separate connection.

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

☐ Navigate to the "Protocol" window 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
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

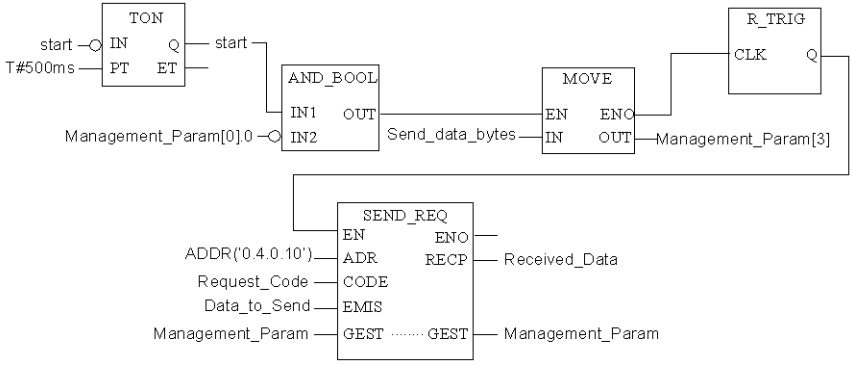
Output Item Name	Data Type	Offset/Device	Offset/Connection	Position in the Byte	Address
Link_Admin_States	Output dword	0	0		%MW306

10.3.6 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 34: 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 35: 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 36: 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 37: 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 38: 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 39: 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 deice. 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 40: Create and Configure the Send_data_bytes Variable

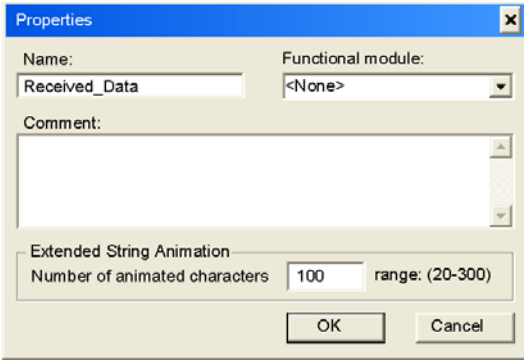
Viewing the Response

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.

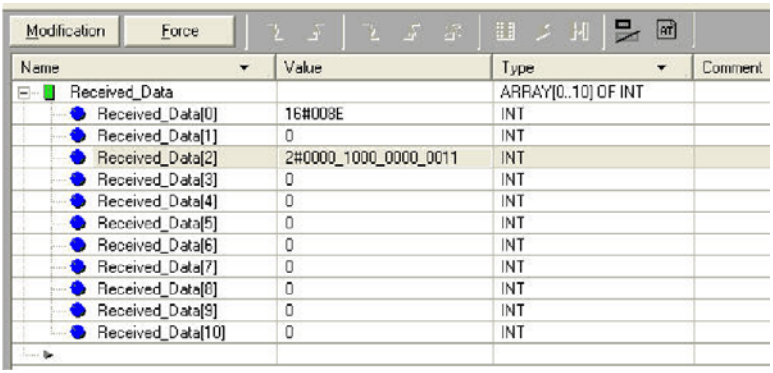
☐ The completed Properties dialog looks like this:



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):



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/TCSESM-E in a Quantum System

This section describes the configuration of a TCSESM/TCSESM-E 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.

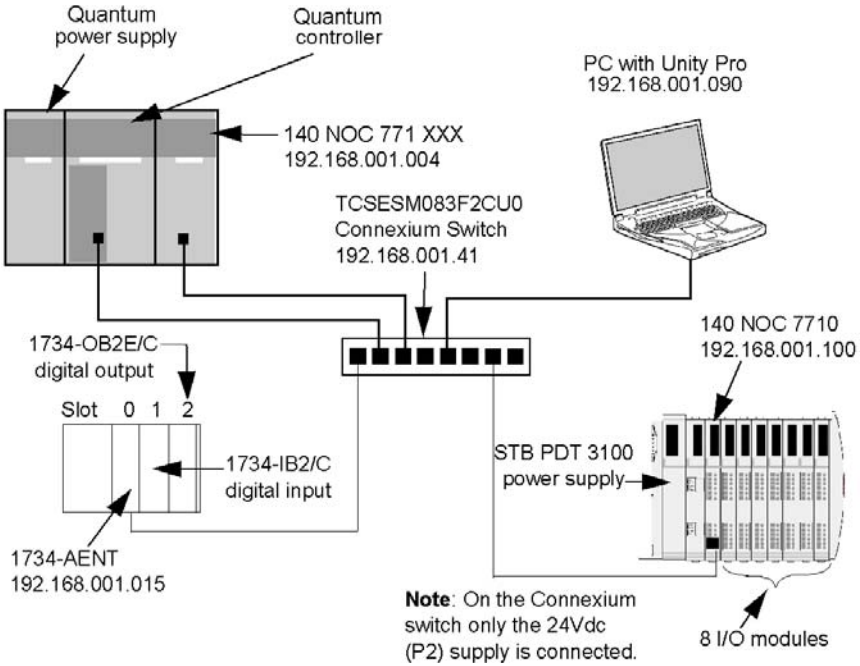


Figure 54: Required hardware and the connections involved to develop a network topology

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

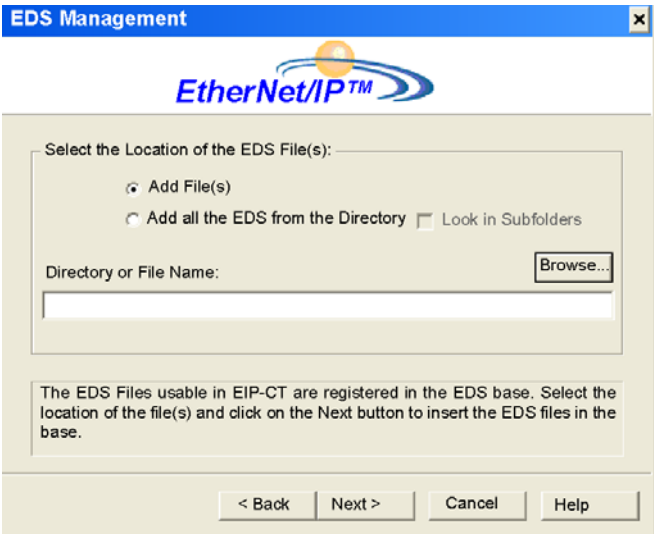
Before the TCSESM switch can be configured in a Quantum system, the TCSESM EDS file has to be added to the Unity Pro EtherNet/IP Device Library. Unity Pro includes an EDS Management wizard that you can use to add one or more EDS files to the Device Library.

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

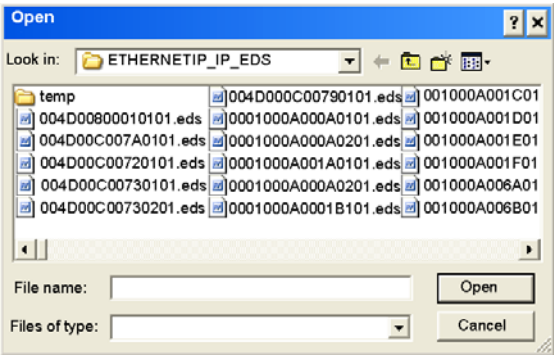
Note: During the following procedure, you can select `Devices:Options...` to open the Display Options window, where you can enable/disable messages indicating the EDS file you are adding is a duplicate—or a different version—of an existing EDS file.

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.

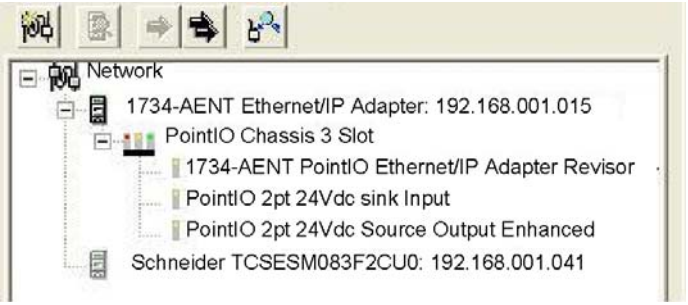
10.4.3 Finding and adding the TCSESM automatically

Use the Unity Pros network detection function to find the TCSESM automatically. As soon as it has been found, you can include it in your project.

Note: Confirm that the TCSESM is actively online with a valid IP address before you can find it and add it to your project.

The following 3 steps are necessary to detect and add a device:
☐ Go online and connect your PC to the network.
☐ Start the network detection.
☐ From the devices displayed by your computer, select those that you would like to add to your device.

You can find more details in 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.

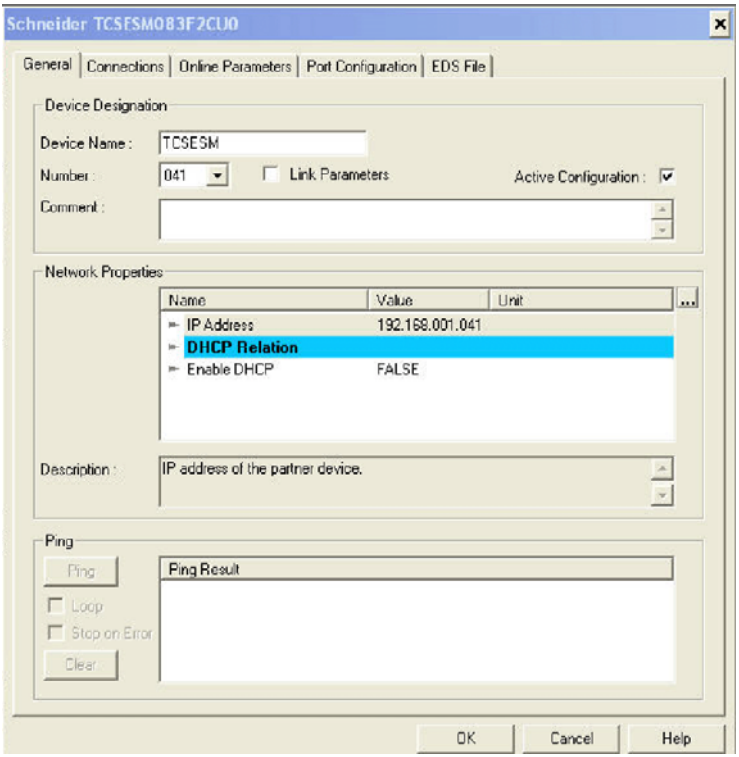
10.4.4 Configuration of the TCSESM properties

The "TCSESM switch properties" window provides the following tab pages. In the following example, you only need to edit a few of these pages:

On this page	Perform the following
General	- Name of the input device - Configure IP address - Add the device to the project configuration
Connections	Apply the standard settings.
Online Parameters	Apply the standard settings (if available).
Module information	(Read-only page – no configuration required)

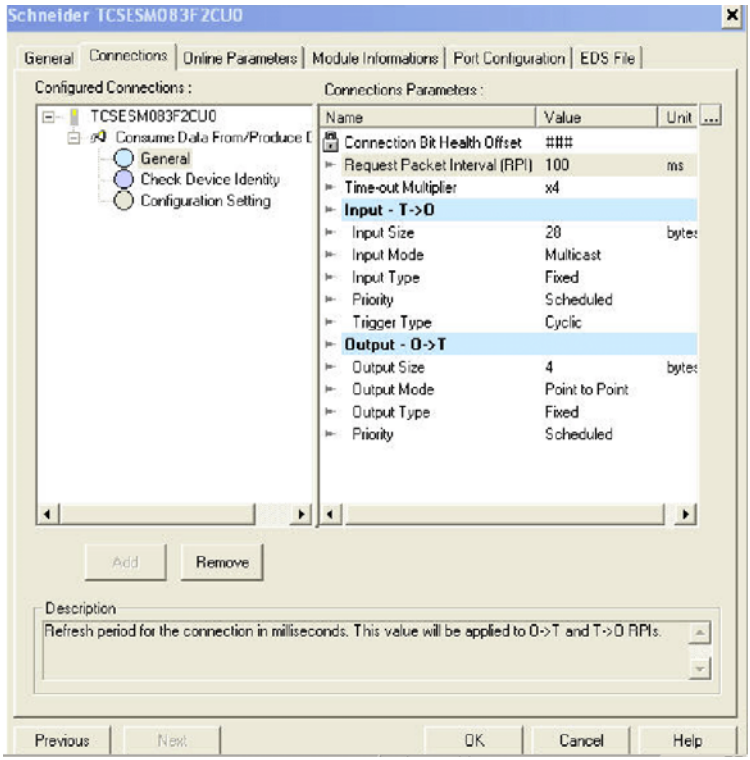
On this page	Perform the following
Connection configuration	(Read-only page – no configuration required)
EDS File	(Read-only page – no configuration required)

The following settings are used for the configuration example:
☐ Click the "General" page:



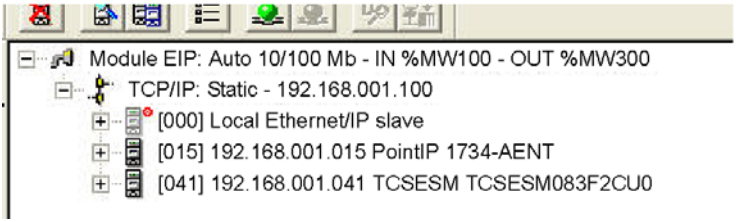
☐ On the "General" page, edit the following settings:
- Device Designation: TCSESM
- Number: The position of the device in the "Device" window - in this example, enter 041.
- Active Configuration: Confirm that this checkbox is selected.
- IP Address: 192.168.001.041

☐ Click the "Connections" 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 "TCSESM switch properties" window.
A node is added to the project configuration in the "Devices" window:



The next step involves monitoring the inputs and outputs of the external device.

10.4.5 Monitoring the TCSESM data

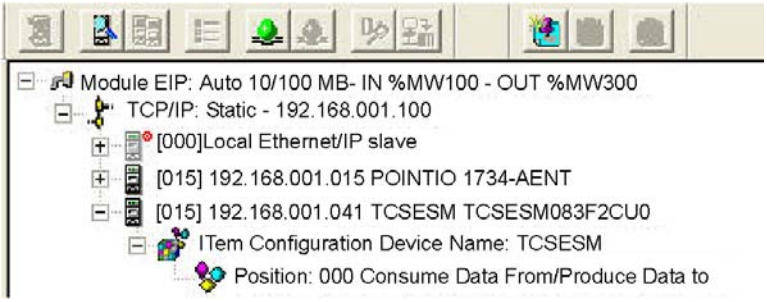
As the device library contains EDS files for the PointIO adapter of the TCSESM and its individual input and output modules, the Unity Pro EtherNet/IP configuration tool automatically performs the following:

- It creates a CIP connection from the EtherNet/IP communication module of the TCSESM to the 1734-AENT that is optimized for the rack and
- It configures every input and output by assigning:
  - a position name
  - an address location
  - a size assignment based on its data type

Note: In this example, the configuration tool has created a connection optimized for an individual rack, thus using the CIP connections more efficiently. A rack-optimized connection can only be used with discreet (digital) I/O modules. With analog I/O modules, confirm that each analog module is connected with the TCSESM using a separate connection.

To monitor the automatically created CIP connection and the I/O parts in Unity Pro:

☐ Navigate to the "Protocol" window 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
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

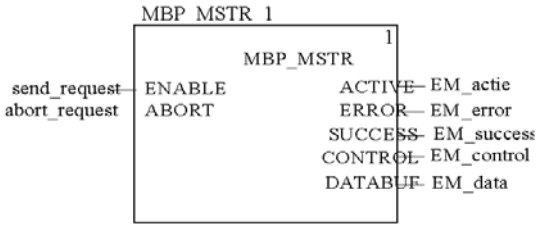
Output Item Name	Data Type	Offset/Device	Offset/Connection	Position in the Byte	Address
Link_Admin_States	Output dword	0	0		%MW306

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 41: 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	Adress
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 42: 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	Seting (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 43: 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 44: 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#OE
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 45: 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 46: 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:

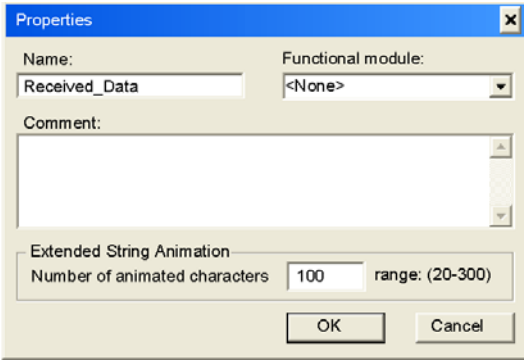
☐ In Unity Pro, select `Tools:Project Browser` to open the Project Browser.

☐ 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.

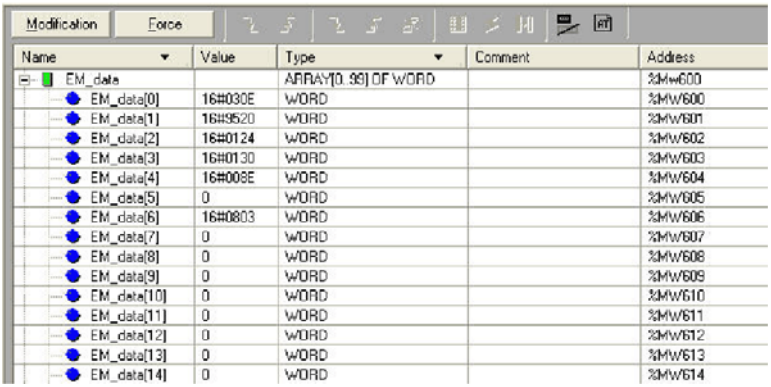
☐ The completed Properties dialog looks like this:



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):



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 figure 55) and whether the status of this process is "IW":

SunOS

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

HP

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

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

SunOS

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

HP

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

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

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

Special steps for HP workstations:

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

For example:

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

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

☐ Test the tftp process with, for example:`cd /tftpboot/device`

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

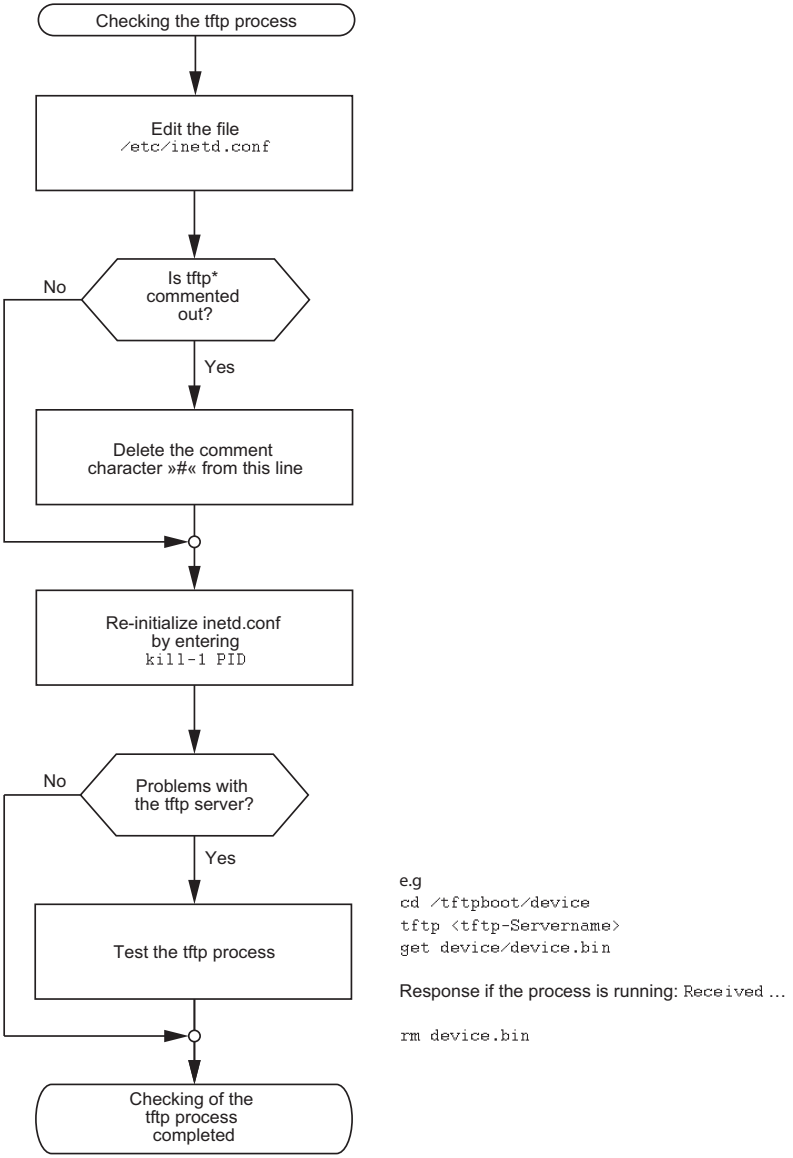


Figure 55: Flow chart for setting up tftp server with SunOS and HP

A.1.2 Software Access Rights

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

Example of a UNIX tftp Server

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

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

Table 47: 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.

A.2 Preparing access via SSH

To be able to access the device via SSH, perform the following steps:

- Generate a key (SSH host key).
- Install the key on the device.
- Enable access via SSH on the device.
- Install a program for executing the SSH protocol (SSH client) on your computer.

A.2.1 Generating a key

The device gives you the option to use your own self-generated keys for the SSH server. If there is no SSH key on the device, the device generates the required keys automatically when the SSH server is switched on for the first time.

The PuTTYgen program allows you to generate the key. This program is located on the product CD.

☐ Start the program by double-clicking on it.
☐ In the “Parameters” frame you select the type of key to be generated.
  ☐ To generate a key for SSH version 2, you select "SSH-2 (RSA)" or "SSH-2 (DSA)".
  ☐ To generate a key for SSH version 1, you select "SSH-1 (RSA)".
☐ Confirm that the field "Number of bits in a generated key" in the "Parameters" frame is showing the value `1024`.
☐ In the "Actions" box, click on "Generate". Move the mouse pointer over the PuTTYgen-window, so that PuTTYgen can create the key using random numbers.
☐ Leave the "Key passphrase" and "Confirm passphrase" input boxes empty.

- ☐ Save the key:
  - ☐ To save a key for SSH version 2, click the "Conversions:Export OpenSSH key" menu.
  - ☐ To save a key for SSH version 1, click the "Save private key" button in the "Actions" frame.
- ☐ Answer the question about saving the key without a passphrase with "Yes".
- ☐ Select the Save location and enter a file name for the key file.
- ☐ Note down the key fingerprint, so that you can check it when establishing a connection.
- ☐ You should also store the key in a location separate from the device so that, if the device is being replaced, the key can be transferred to the new device.

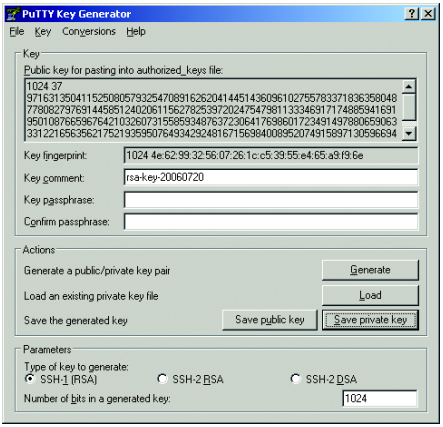


Figure 56: PuTTY key generator

For experienced network administrators, another way of creating the key is with the OpenSSH Suite. To generate the key, enter the following command:

```
ssh-keygen(.exe) -q -t rsa1 -f rsa1.key -C '' -N ''
```

A.2.2 Loading a key onto the device

You load the SSH key onto the device with the Command Line Interface via TFTP.

SSH version 1 works with an RSA key. However, SSH version 2 works with an RSA key and a DSA key. For SSH version 2, confirm that you load both keys to the device.

☐ Store the keys on your tftp server.

☐ Load the keys from the tftp server onto the device.

`enable`	Switch to the privileged EXEC mode.
`no ip ssh`	Deactivates the SSH server.
`copy tftp://ip/filepath/key nvram:sshkey-rsa2`	Loads the key to the non-volatile memory of the device. ▶ `nvram:sshkey-rsa2` is the storage location of the RSA key for SSH version 2. ▶ `nvram:sshkey-dsa` is the storage location of the DSA key for SSH version 2. ▶ `nvram:sshkey-rsa1` is the storage location of the RSA key for SSH version 1.
`copy tftp://ip/filepath/key nvram:sshkey-dsa`	
`copy tftp://ip/filepath/key nvram:sshkey-rsa1`	
`ip ssh`	Activates the SSH server.

A.2.3 Access through an SSH

One way of accessing your device through an SSH is by using the PuTTY program. This program is provided on the product-CD.

☐ Start the program by double-clicking on it.
☐ Enter the IP address of your device.
☐ Select "SSH".

☐ Click on "Open" to set up the connection to your device.

Depending on the device and the time at which SSH was configured, it can take up to a minute to set up the connection.

Just before the connection is established, the PuTTY program displays a security alarm message and gives you the option of checking the key fingerprint.

Figure 57: Security alert prompt for the fingerprint

☐ Check the fingerprint of the key to help ensure that you have actually connected to the desired device. You will find the fingerprint of your key in the "Key fingerprint" field of the PuTTY key generator.
☐ If the fingerprint matches your key, click on "Yes".

PuTTY also displays another security alarm message at the defined detected threshold.

Figure 58: Security query at the defined detected threshold

☐ Click on "Yes" in the security alarm message.

To suppress this message when establishing subsequent connections, select "SSH" in the "Category" box in the PuTTY program before opening the connection. In the "Encryption options" box, select "DES" and click on "Up" until "DES" comes above the line "-- warn below here --". In the "Category" box, switch back to "Session" and establish the connection as usual.

For experienced network administrators, another way of accessing your device through an SSH is by using the OpenSSH Suite. To open the connection, enter the following command:

```
ssh admin@10.0.112.53 -cdes
```

- `admin` for the user name.
- `10.0.112.53` is the IP address of your device.
- `-cdes` sets the encryption type for SSHv1.

A.3 HTTPS Certificate

The encryption of HTTPS connections requires an X.509 certificate. The device allows you to use your own X.509 certificate. If there is no X.509 certificate on the device, the device generates this automatically when the HTTPS server is switched on for the first time.

You load your own X.509 certificate onto the device with the Command Line Interface via TFTP.

☐ Store the certificate on your tftp server.

☐ Load the certificate from the tftp server onto the device.

`enable`	Switch to the privileged EXEC mode.
`no ip https`	Deactivates the HTTPS function before transferring the certificate to the device.
`copy tftp://ip/filepath/cert nvram:httpscert`	Loads the certificate to the non-volatile memory of the device. `nvram:httpscert` is the storage location of the X.509 certificate.
`ip https`	Activates the HTTPS function after transferring the certificate to the device.

A.4 Service Shell

When you need assistance with your device, then the service personnel use the Service Shell function to monitor internal conditions, for example switch or CPU registers.

The CLI Reference Manual contains a description of deactivating the Service Shell.

Note: When you deactivate the Service Shell, then you are still able to configure the device, but you limit the service personnel to system diagnostics. In order to reactivate the Service Shell function, the device requires disassembly by the manufacturer.

B General Information

B.1 Abbreviations used

EAM	Memory Backup Adapter
ACL	Access Control List
BOOTP	Bootstrap Protocol
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
FDB	Forwarding Database
GARP	General Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocoll
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocol
F/O	Optical Fiber
MAC	Media Access Control
MSTP	Multiple Spanning Tree Protocol
NTP	Network Time Protocol
PC	Personal Computer
PTP	Precision Time Protocol
QoS	Quality of Service
RFC	Request For Comment
RM	Redundancy Manager
RSTP	Rapid Spanning Tree Protocol
SFP	Small Form-factor Pluggable
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TP	Twisted Pair
UDP	User Datagramm Protocol
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network

B.2 Technical Data

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

C Index

T

U

V

W