# ConneXium

## TCSEFEC Industrial Firewall
## Configuration User Manual

S1B64663.00

www.schneider-electric.com

Schneider Electric

# Contents

# Safety instructions

## 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.


## Usage

The device may only be employed for the purposes described in the catalog, technical description, and manuals.

# 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 TCSEFEC Industrial Firewall Configuration User Manual | S1B64663 |
| ConneXium TCSEFEC Industrial Firewall Command Line Interface Reference Manual | S1B64695 |
| ConneXium TCSEFEC Industrial Firewall Web-based Interface Reference Manual | S1B64648 |
| ConneXium TCSEFEC Industrial Firewall Installation User Manual | S1B64656 |

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

Perform the following steps to install and configure the Firewall:

- Select operating mode depending on area of application,
  - Transparent - Bridging
  - Router - Different subnets
  - PPPoE - Internet access via DSL
- Configure the operating mode selected,
- Create firewall rules / set up VPN.

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

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

The “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.

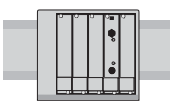
# Key

The designations used in this manual have the following meanings:

| | |
|---|---|
| ▶ | List |
| ☐ | Work step |
| ■ | Subheading |
| Link | Cross-reference with link |
| **Note:** | A note emphasizes an important fact or draws your attention to a dependency. |
| `Courier` | ASCII representation in 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 -<br>Programmable logic controller |
|  | I/O -<br>Robot |

# 1 Introduction

Today, machines and production units such as printing machines or robotic lines require the real-time transfer of production information. This necessitates the option to access the machine directly from the office level, and exposes the production plant to the potential risk of deliberate or accidental manipulation.

The Schneider Electric Industrial Firewall TCSEFEC assists you in establishing security for anywhere that process and production data flows into cross-area data recording systems, or where systems are aligned. The segmentation of individual production cells and the assistance in securing remote maintenance accessing helps prevent manipulation and helps provide the required data security and the smooth operation of the plant.

These times in which Ethernet is being used beyond office applications, and increasingly on the machine level, are seeing an increase in the security requirements:

- assistance in the protection of sensitive subareas of production
- long-term integration of office IT and industrial IT networks as a comprehensive solution.

In addition, the Schneider Electric Industrial Firewall TCSEFEC provides you with three access options for remote maintenance:

- modem access with firewall rules
- Internet access with firewall rules
- access via a virtual private network (VPN).

To increase availability, the Schneider Electric Industrial Firewall TCSEFEC provides you with two redundancy mechanisms:

- virtual router redundancy
- layer 2 redundancy for redundant ring/network coupling.

# 1.1 Security Concept

A Firewall helps make a closed internal network secure. A number of main factors affect this security:

- Access within the internal network
  The potential risks within an internal network are often underestimated. Usually unintentionally, virulent programs are introduced into the internal network by the company's own employees or service providers, who connect to the internal network with their own computers. USB sticks or other memory media can also contain virulent programs.
- Access to the Firewall
  Take measures to help protect the access to the management of the Firewall. Because whoever has access to the Firewall determines which data can pass through the Firewall and which cannot.
- Firewall settings
  A Firewall helps protect your internal network from unpermitted data traffic across the dividing line of internal/external network.
  You use the Firewall rules to define which data is permitted to cross this dividing line.
- Protective measures against viruses
  An effective way to help protect your network from viruses is to help prevent communication with nonsecure devices. This is effective, because it removes the need for the work-intensive checking of data package contents. Another advantage of this method is that you define exactly who may communicate with whom.

# 1.2 Typical applications

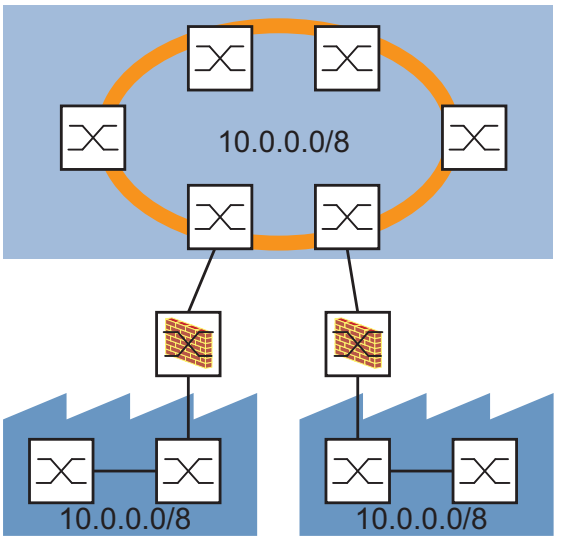
The Industrial Firewall is used everywhere that security-sensitive network cells require a connection from the internal network into an external network. The Industrial Firewall is the link between the internal network and the external network from which unauthorized accesses are to be expected. In its function as a link, the Industrial Firewall helps protect the internal network from undesired data traffic along the connection to the external network.

Typical uses are:

- Helping protect individual production cells in a flat company network
- Helping protect individual production cells in a routed company network
- Coupling identical production cells to a company network
- Connecting a production cell with the office network via a public network
- Helping provide protected service access
- Separation of machine common parts

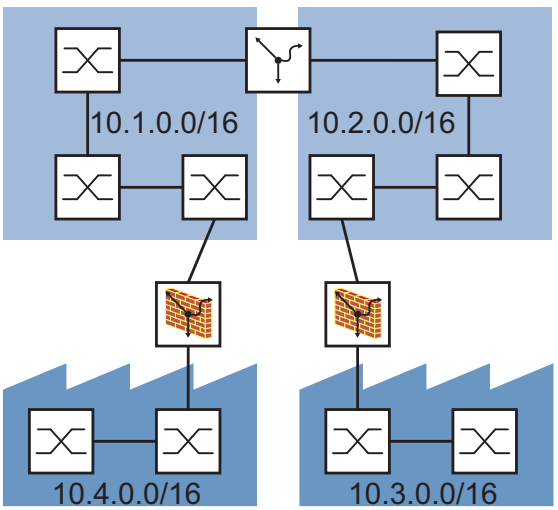
### Helping protect individual production cells in a flat company network

Individual production cells exchange information with devices in the company network. The company network and the production cells are located in the same layer 2 network. The TCSEFEC works like a switch with an integrated firewall.



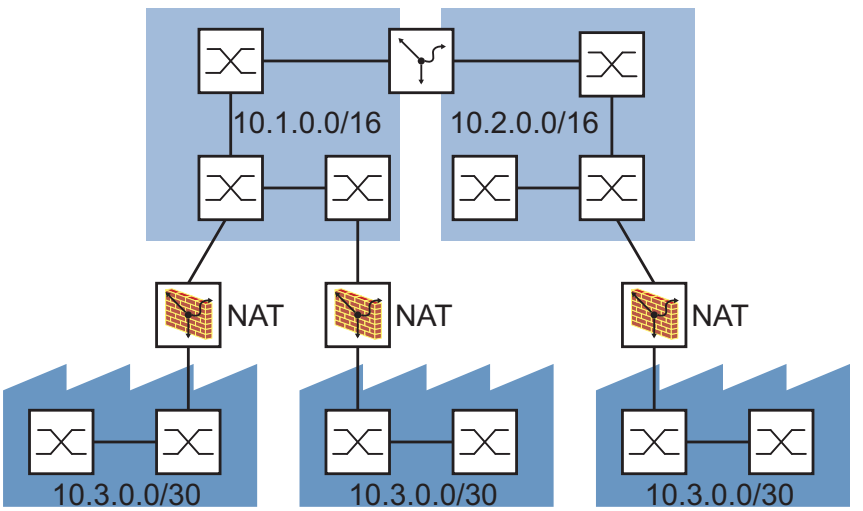
### Helping protect individual production cells in a routed company network

Individual production cells exchange information with devices in the company network. The company network and the production cells are located in different subnetworks. The TCSEFEC works like a router with an integrated firewall.



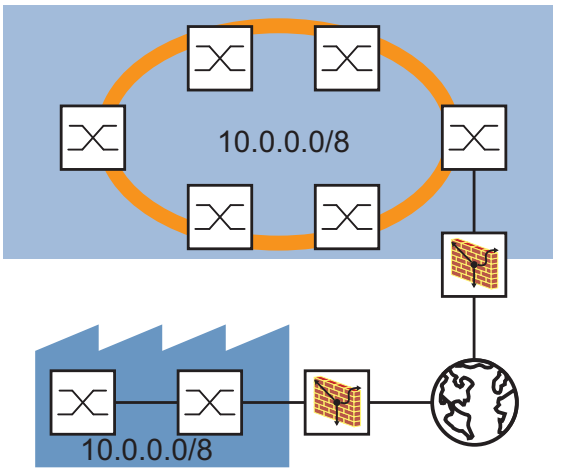
**Coupling identical production cells to a company network**

Individual, identically structured production cells exchange information with devices in the company network. The company network and the production cells are located in different subnetworks. The TCSEFEC works like a router with an integrated firewall.
The NAT function enables the identically structured production cells to communicate with the company network, even though the devices have the same IP address in the different production cells.



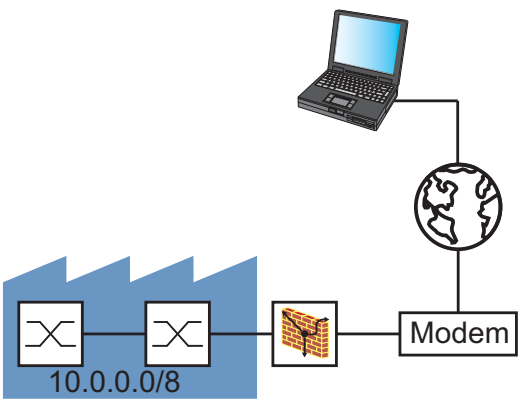
## Connecting a production cell with the office network via a public network

A production cell exchanges information with devices in the company network via the public Internet. A virtual information tunnel (virtual private network, VPN) through the public Internet helps protect the communication.




## Helping provide protected service access

A service technician exchanges information with devices in the production cell via the public Internet. A virtual information tunnel (virtual private network, VPN) through the public Internet helps protect the communication.



# 1.3 Configuring the application

The Industrial Firewall has 3 operating modes:

- Transparent mode
- Router mode
- PPPoE mode

Your choice of operating mode depends on your application case.
The table below helps you when choosing the operating mode.

| Application | Characteristic | Operating mode |
|---|---|---|
| Helping protect individual production cells in a flat company network | Transmission on level 2 of the ISO/OSI layer model. The IP address ranges before and after the Firewall are located in the same subnetwork. | Transparent |
| Helping protect individual production cells in a routed company network | Transmission on level 3 of the ISO/OSI layer model. The IP address ranges before and after the Firewall are located in different subnetworks. | Router |
| Coupling identical production cells to a company network | Transmission on level 3 of the ISO/OSI layer model. The IP address ranges before and after the Firewall are located in different subnetworks.<br>The Nat function is used to map IP addresses onto a different IP address range. | Router |
| Connecting a production cell with the office network via a public network | Transmission on level 3 of the ISO/OSI layer model. The IP address ranges before and after the Firewall are located in different subnetworks.<br>Data transfer in a protected tunnel through the public Internet (VPN). | Router |
| Helping provide protected service access | Service access via the public telephone network. | PPPoE |

*Table 1: Choosing the operating mode*

Depending on the operating mode you choose, there are different procedures for the further configuration of the Industrial Firewall.

### 1.3.1 Configuration steps in the transparent mode

In the state on delivery, the Industrial Firewall is in the transparent mode. The default settings enable you to start operating the Industrial Firewall immediately. In the state on delivery, the Industrial Firewall helps prevent a communication link from being set up if it is initiated externally. Internal devices can set up a communication link to the outside.

The following proceedings assist you in controlling the access to the Industrial Firewall and in making further settings:

- ☐ Make connection to Firewall(see on page 25 “Access to the user interfaces”)
- ☐ Select the transparent operating mode (see on page 46 “IP parameters in Transparent Mode”)
- ☐ Enter IP parameters for the device (see on page 46 “IP parameters in Transparent Mode”)
- ☐ Take measures to help protect Industrial Firewall from unauthorized access (see on page 93 “Assistance in the Protection from Unauthorized Access”)
- ☐ Create rules for authorized and unauthorized data traffic (see on page 117 “Controlling the Data Traffic”)

### 1.3.2 Configuration steps in router mode

In the state on delivery, the Industrial Firewall is in the transparent mode.

The following proceedings assist you in controlling the access to the Industrial Firewall and in making further settings:

- ☐ Make connection to Firewall (see on page 25 “Access to the user interfaces”)
- ☐ Select the router operating mode (see on page 47 “IP Parameters in Router Mode”)
- ☐ Enter IP parameter for the internal port (see on page 47 “Internal interface”)
- ☐ Enter IP parameter for the external port (see on page 48 “External Interface”)
- ☐ Take measures to help protect Industrial Firewall from unauthorized access (see on page 93 “Assistance in the Protection from Unauthorized Access”)
- ☐ Create rules for authorized and unauthorized data traffic (see on page 117 “Controlling the Data Traffic”)
- ☐ Make NAT settings (see on page 137 “NAT – Network Address Translation”)
- ☐ Set up VPN connection (see on page 155 “VPN – Virtual Private Network”)

### 1.3.3 Configuration steps in PPPoE mode

In the state on delivery, the Industrial Firewall is in the transparent mode.

The following proceedings assist you in controlling the access to the Industrial Firewall and in making further settings:

- ☐ Make connection to Firewall (see on page 25 “Access to the user interfaces”)
- ☐ Select the PPPoE operating mode (see on page 49 “Connection parameters in PPPoE Mode”)
- ☐ Enter IP parameter for the internal port (see on page 47 “Internal interface”)
- ☐ Enter connection parameters for the external port (see on page 48 “External Interface”)
- ☐ Switch the automatic interruption of the PPPoE connection on or off (see page 48 “External Interface”)
- ☐ Take measures to help protect Industrial Firewall from unauthorized access (see on page 93 “Assistance in the Protection from Unauthorized Access”)
- ☐ Create rules for authorized and unauthorized data traffic (see on page 117 “Controlling the Data Traffic”)
- ☐ Make NAT settings (see on page 137 “NAT – Network Address Translation”)
- ☐ Set up VPN connection (see on page 155 “VPN – Virtual Private Network”)

# 2 Access to the user interfaces

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

- System monitor via the V.24 interface (out-of-band)
- Command Line Interface (CLI)
  - via the V.24 connection (out-of-band)
  - via SSH (in-band)
- Web-based interface via Ethernet (SNMPv3, in-band).

# 2.1 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 2: 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.

```
< TCSEFEC  (Boot) Release: 05.2.xx Build: 2012-02-17 08:08 HW: 1.00 >

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

*Figure 1: Screen display during the boot process*

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

```
   System Monitor 1

   (Selected OS: L3S-05.2.xx (2012-02-17 08:08))


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



sysMon1>
```

*Figure 2: System monitor 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.

# 2.2 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.

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)
- SSH (in-band).
  In the state on delivery,
  – the firewall setting allows SSH access via the INTERNAL port.
  – the firewall setting helps prevent SSH access via the EXTERNAL port.

**Note:** To facilitate making entries, CLI gives you the option of abbreviating keywords. Type in the beginning of a keyword. If the characters entered identify a keyword, CLI will complete the keyword when you press the tab key or the space key.

**Note:** You can configure the V.24 interface either as a modem interface or a terminal/CLI interface.
However, to be able to have at least limited access to the CLI interface in modem mode, you connect your terminal (setting on terminal: 9,600 baud) to the V.24 interface.
Press any key on your terminal keyboard a number of times until the login screen indicates the CLI mode.

## Opening the Command Line Interface

☐ Connect the device to a terminal or to a “COM” port of a PC using terminal emulation based on VT100, and press any key (see on page 26 “Opening the system monitor”) or
call up the Command Line Interface via SSH.
A window for entering the user name appears on the screen.
Up to five users can access the Command Line Interface.

The TCSEFEC is a **S**ecurity **D**evice with **V**PN function (SDV).

```
                Copyright (c) 2011-2012 Schneider Electric

                     All rights reserved

                  TCSEFEC Release L3S-05.2.0x

                  (Build date 2012-02-17 08:08)

               System Name:  TCSEFEC-000000
               Netw. Mode :  transparent
               Mgmt-IP    :  a.b.c.d
               Base-MAC   :  00:11:22:33:44:55
               System Time:  FRI FEB 17 08:08:08 2012


(Schneider Electric TCSEFEC)
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.
These entries are case-sensitive.

The start screen appears.

```
NOTE: Enter '?' for Command Help.  Command help displays all options
      that are valid for the particular mode.
      For the syntax of a particular command form, please
      consult the documentation.

(Schneider Electric TCSEFEC) >
```

*Figure 4: CLI screen after login*

# 2.3 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.

In the state on delivery,
– the firewall setting allows Web access via the internal interface.
– the firewall setting helps prevent Web access via the external interface, for security reasons.

### Opening the Web-based Interface via the internal port

To open the Web-based interface, you will need a Web browser (a program that can read hypertext), for example Mozilla Firefox version 2 or later, or Microsoft Internet Explorer version 6 or later.

**Note:** The Web-based interface uses Java software 6 (“Java™ Runtime Environment Version 1.6.x”).

For Windows users: If you do not have access to the internet, cancel the installation. Install the software from the enclosed CD-ROM. To do this, browse the directory of this CD under "ConneXium".

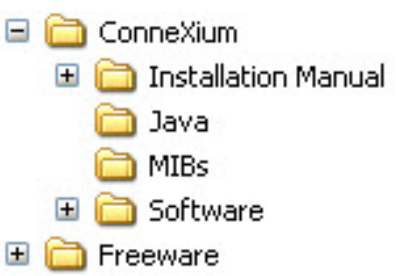



*Figure 5: ConneXium Resource CD Windows Explorer view*

☐ Open the "Java" folder.
☐ Start the installation program.

Upon the execution of Autorun on the CD the following Welcome screen will appear:


*Figure 6: ConneXium Resource CD Welcome screen*

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

The login window appears on the screen.

The TCSEFEC is a **S**ecurity **D**evice with **V**PN function (SDV).


*Figure 7: Login window*

☐ Select the desired language.
☐ In the `Login` drop-down menu, select
  – `user` to have read access to the device
  – `admin` to have read/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).
☐ In the `Login Type` drop-down menu, select
  – Administration if you want to manage the device, or
  – User Firewall if you want to login for the user firewall function (prerequisite: the user selected in the `Login` drop-down menu has already been created in the user firewall).
☐ Click on OK.

The website of the device appears on the screen.

**Note:** For security reasons, change the factory setting password. You thus help prevent the device from being accessed with this password. If the password is the factory setting password, the device displays the message “Default Password” in every dialog‘s header line.

**Note:** The changes you make in the dialogs are copied to the volatile memory of the device when you click on “Write”. Click on “Load” to update the display.

### Opening the Web-based Interface via the external port

In the state on delivery, the firewall setting helps prevent Web access via the external port, for security reasons. You can access the device via the external port if you create and activate for your PC a rule for the Web access and the SNMP access. First open the Web-based Interface via the internal port (see on page 31 “Opening the Web-based Interface via the internal port”). After creating the access rules at the external port, you can open the Web-based interface via the external port in the same way as via the internal port.

- ☐ In the `Security:Web Access` menu, create a new entry with the IP address of your PC as the source address. Select “Accept” in the “Action” column and activate the table entry.
- ☐ In the `Security:SNMP Access` menu, create a new entry with the IP address of your PC as the source address. Select “Accept” in the “Action” column and activate the table entry.
- ☐ Proceed in the same way as for opening the internal port.

# 3 Entering the IP Parameters

## Choosing the operating mode

The entries for the IP parameters depend on the operating mode selected.

– In Transparent Mode, the local IP address is also the IP address of the management of the Industrial Firewall.
– In Router/PPPoE Mode, the IP address of the internal interface is also the IP address of the management of the Industrial Firewall. Depending on the firewall settings, you can also access the management via the IP address of the external interface.

☐ Choose an operating mode that meets your requirements.

In the state on delivery, the Transparent Mode is active.

## Options for entering the IP parameters for the management of the Industrial Firewall

Enter the IP parameters when the device is installed for the first time so that you can access the device management for further configuration.

During the first installation, the device provides you with 5 options for entering the local IP parameters in Transparent Mode, or the IP parameters of the internal interface in the Router/PPPoE mode:

- Entry using the Command Line Interface (CLI).
  You choose this “out of band” method if
  - you preconfigure your device outside its operating environment
  - you do not have network access (“in-band”) to the device

  (see page 44 “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 page 52 “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 page 55 “Loading the System Configuration from the EAM”).
- 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 IP parameters to the device using its MAC address or its system name (see page 57 “System Configuration via DHCP”).
- 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.

# 3.1 IP Parameter Basics

## 3.1.1 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 3: 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

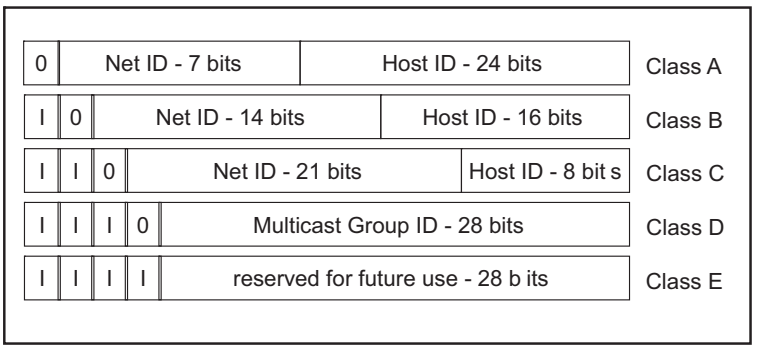



*Figure 8: Bit representation of the IP address*

The IP addresses belong to class A when their 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.

## 3.1.2 Private IP addresses

If the IP address range assigned to you is not large enough for your requirements, or for whatever other reason, you can use the IP addresses of the private IP address range. IANA has defined three private IP address ranges in RFC 1918. Each of the three ranges is located in a different class. Internet routers block data packets with private IP addresses. Thus, the private addresses are only intended for use in internal networks. The Network Address Translation Protocol (see on page 137 “NAT – Network Address Translation”) enables you to allow devices with a private IP address in an internal network with devices in other networks.

| IP address range | CIDR notation | Network class |
|---|---|---|
| 10.0.0.0 - 10.255.255.255 | 10.0.0.0/8 | A |
| 172.16.0.0 - 172.31.255.255 | 172.16.0.0/12 | B |
| 192.168.0.0 - 192.168.255.255 | 192.168.0.0/16 | C |

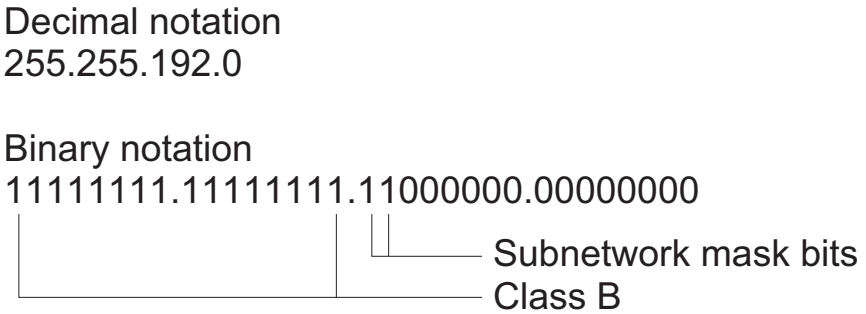
*Table 4: Private address ranges*

## 3.1.3 Netmask

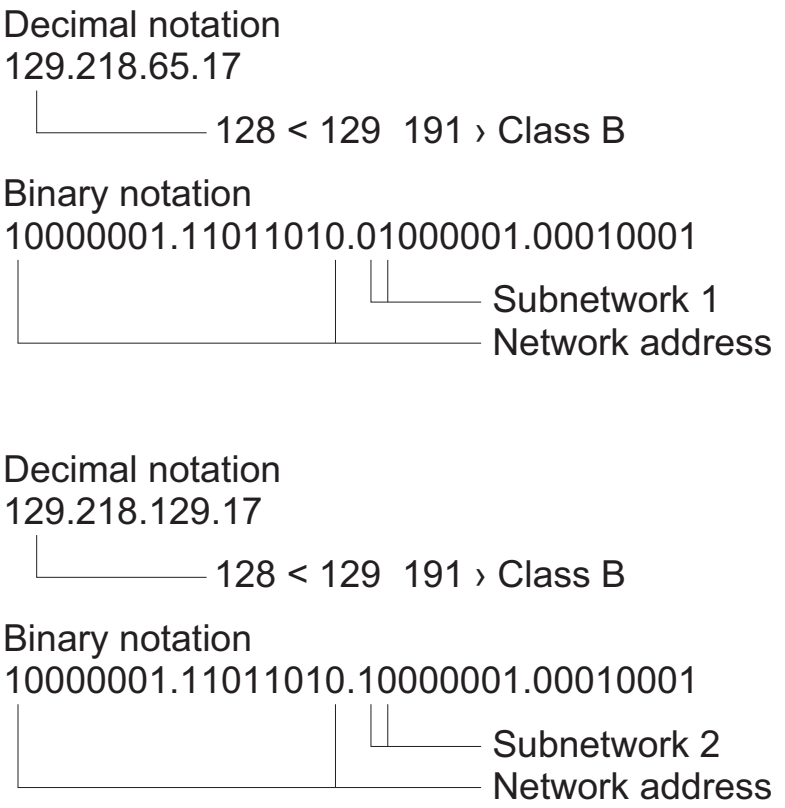
Routers and gateways subdivide large networks into subnetworks. The netmask assigns the IP addresses of the individual devices to a particular subnetwork.

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?

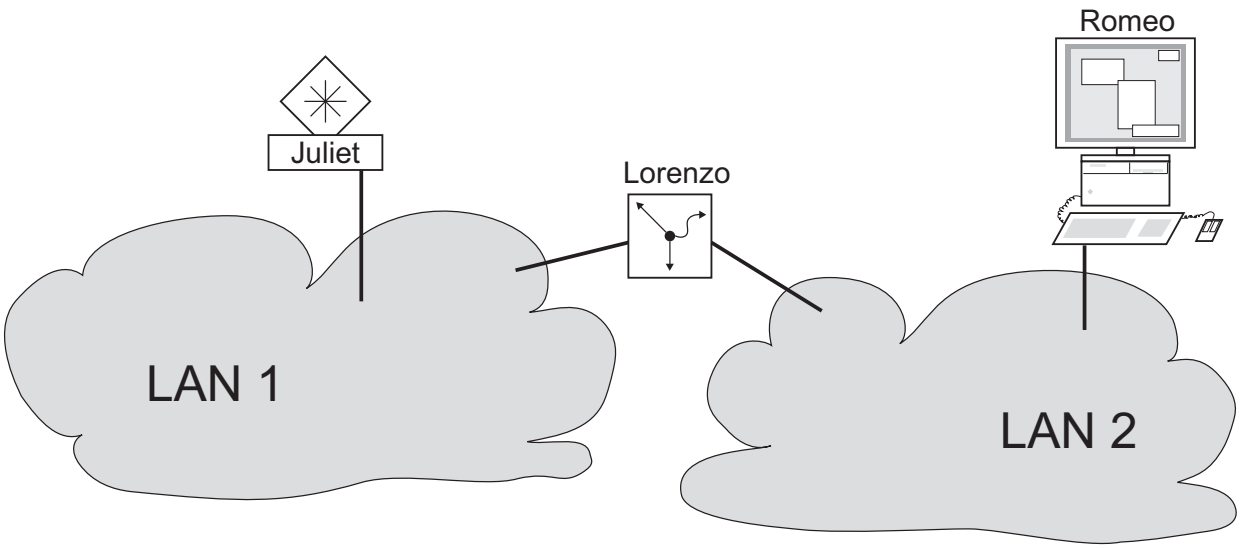



*Figure 9: Management agent that is separated from its management station by a router*

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.

### 3.1.4 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 the IP addresses in a given address range. Example:

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

25 mask bits

CIDR notation: 149.218.112.0/25

Mask bits

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

# 3.2 Entering IP parameters via CLI

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

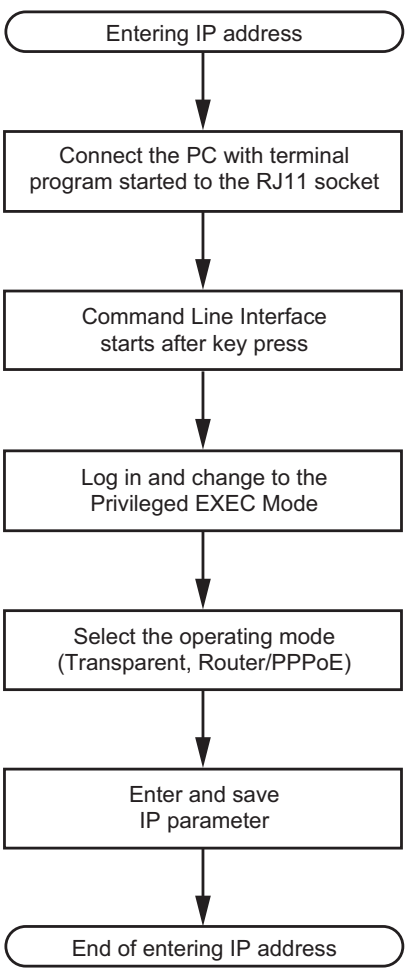



*Figure 10: Flow chart for entering IP addresses*

**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 28 “Command Line Interface”).

The start screen appears.

```
NOTE: Enter '?' for Command Help.  Command help displays all options
      that are valid for the particular mode.
      For the syntax of a particular command form, please
      consult the documentation.


(Schneider Electric TCSEFEC) >
```

### 3.2.1 IP parameters in Transparent Mode

☐ Activate the transparent mode (state on delivery: transparent mode).

☐ If DCHP is switched on, switch it off (state on delivery: DHCP is switched off).

☐ Enter the IP parameters.

- Local IP Address
  On delivery, the device has the local IP address 192.168.1.1.
- 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 255.255.255.0.
- IP address of the gateway
  This entry is required if the device and the management station or the DHCP server are located in different subnetworks (see page 41 “Example of how the network mask is used”).
  Enter the IP address of the gateway that connects the local subnet with the management station’s subnet.
  The default setting of the IP address is 0.0.0.0.

☐ Save the configuration entered.

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `network mode transparent` | Select the Transparent Mode (state of delivery: Transparent Mode). |
| `network transparent proto none` | Deactivate DHCP (state on delivery: disabled). |
| `network transparent ip-address 172.16.1.100` | Allocate the IP address 172.16.1.100 to the device in transparent mode. |
| `network transparent netmask 255.255.255.0` | Allocate the netmask 255.255.255.0 to the device in transparent mode. |
| `network transparent gateway 176.16.1.1` | Allocate the gateway address 176.16.1.1 to the device in transparent mode. |
| `copy config running-config nv` | 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).

### 3.2.2 IP Parameters in Router Mode

**Internal interface**

☐ Activate the router mode (state on delivery: transparent mode).

☐ If DCHP is switched on, switch it off (state on delivery: DHCP is switched off).

☐ Enter the IP parameters.

- Internal IP address
  On delivery, the device has the local IP address 192.168.1.3.
- 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 255.255.255.0.

☐ Save the configuration entered with
`copy config running-config nv` or
`save`.

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `network mode router` | Select the Router Mode (state of delivery: Transparent Mode). |
| `network router proto int none` | Deactivate the DHCP on the internal router interface (state on delivery: disabled). |
| `network router param int ip-address 172.17.1.100` | Allocate the IP address 172.17.1.100 to the internal router interface. |
| `network router param int netmask 255.255.255.0` | Allocate the netmask 255.255.255.0 to the internal router interface. |
| `copy config running-config nv` | 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).

## External Interface

☐ If DCHP is switched on, switch it off (state on delivery: DHCP is switched off).

☐ Enter the IP parameters.

- External IP Address
  On delivery, the device has the local IP address 10.0.0.10.
- 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 255.255.255.0.
- IP address of the gateway
  This entry is required if the device and the management station or the DHCP server are located in different subnetworks (see page 41 “Example of how the network mask is used”).
  Enter the IP address of the gateway that connects the local subnet with the management station’s subnet.
  The default setting of the IP address is 0.0.0.0.

☐ Save the configuration entered with
`copy config running-config nv` or
`save`.

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `network router proto ext none` | Deactivate the DHCP on the external router interface (state on delivery: disabled). |
| `network router param ext ip-address 10.0.1.100` | Allocate the IP address 10.0.1.100 to the external router interface. |
| `network router param ext netmask 255.255.240.0` | Allocate the netmask 255.255.240.0 to the external router interface. |
| `network router gateway 10.0.1.1` | Allocate the gateway address 10.0.1.1 to the device. The gateway must be located in the network of one of the router interfaces. |
| `copy config running-config nv` | Save the current configuration to the non-volatile memory. |

## 3.2.3 Connection parameters in PPPoE Mode

### Internal interface

☐ Activate the PPPoE mode (state on delivery: transparent mode).

☐ If DCHP is switched on, switch it off (state on delivery: DHCP is switched off).

☐ Enter the IP parameters.

- Internal IP address
  On delivery, the device has the local IP address 192.168.1.3.
- 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 255.255.255.0.

☐ Save the configuration entered with `copy config running-config nv` or `save`.

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `network mode pppoe` | Select the PPPoE Mode (state on delivery: Transparent Mode). |
| `network router proto int none` | Deactivate DHCP (state on delivery: disabled). |
| `network router param int ip-address 172.17.1.100` | Allocate the IP address 172.17.1.100 to the internal interface. |
| `network router param int netmask 255.255.255.0` | Allocate the netmask 255.255.255.0 to the device in transparent mode. |
| `copy config running-config nv` | 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).

## External Interface

☐ Enter the connection parameters that you got from your provider for the connection.

- Username
- Password
- MTU (Maximum Transmission Unit).
  The MTU specifies the maximum frame size that this connection can transmit. If larger data packets are to be transmitted, the Firewall fragments the larger data packet into multiple small data packets.

☐ Save the configuration entered with
`copy config running-config nv` or
`save`.

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `network pppoe username Peter` | Enter the user name “Peter”. |
| `network pppoe password Holidays` | Enter the password “Holidays”. |
| `network pppoe mtu-size 1492` | Enter the maximum frame size as 1492. |
| `copy config running-config nv` | Save the current configuration to the non-volatile memory. |

**Note:** Normally, you can skip the setting of the maximum frame size. Set the maximum frame size if you know that your Internet Service Provider uses a different value.

The external interface gets its IP address from the connection provider via PPPoE.

The TCSEFEC device allows you to automatically interrupt the PPPoE connection every day. To activate this function, you proceed as follows:

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `network pppoe disconnect admin-state enable` | Specify that the device automatically interrupts the PPPoE connection at the specified time every day. |
| `network pppoe disconnect hour 2` | Set the time (hour) at which the device automatically interrupts the PPPoE connection every day. Value range: 0 to 23. |
| `copy config running-config nv` | Save the current configuration to the non-volatile memory. |

# 3.3 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 connection.
You can easily configure other parameters via the Web-based interface (see the "Web-based Interface" reference manual).

In the state on delivery, the Ethernet Switch Configurator function of the device is

- activated at the internal port,
- deactivated at the external port.

**Note:** The device offers the configuration with Ethernet Switch Configurator exclusively in and for transparent mode. The transparent mode is activated in the as-delivered condition.

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

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

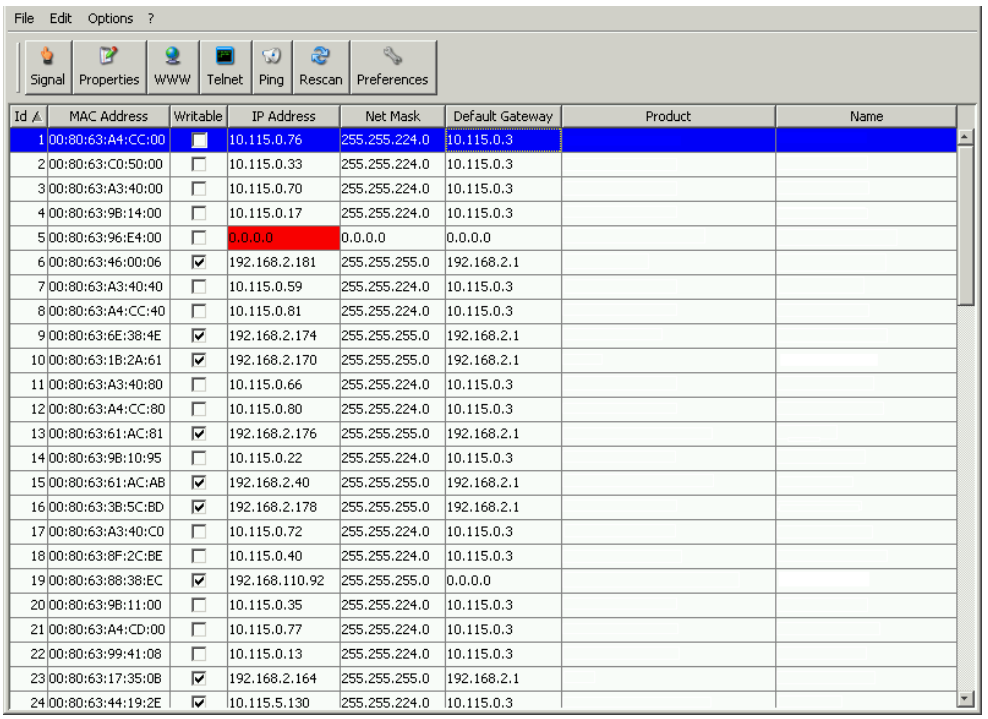



*Figure 11: Ethernet Switch Configurator*

When Ethernet Switch Configurator is started, Ethernet Switch Configurator automatically searches the network for those devices which support the Ethernet Switch Configurator protocol.
Ethernet Switch Configurator uses the first network interface found for the PC. If your computer has several network cards, you can select the one you desire in the Ethernet Switch Configurator toolbar.

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

**Note:** When the IP address is entered, the device copies the local configuration settings (see on page 68 “Editing and managing Configurations”).

**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 61 “Web-based IP Configuration”).

**Note:** Save the settings so that you will still have the entries after a restart (see on page 68 “Editing and managing Configurations”).

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.

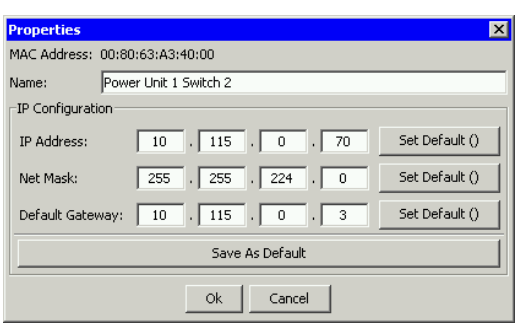



*Figure 12: Ethernet Switch Configurator – assigning IP parameters*

# 3.4 Loading the System Configuration from the EAM

The Memory Backup Adapter (EAM) is a device for

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

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

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

The password is valid if

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

To save the configuration data in the EAM (see on page 70 “Saving the Configuration”).

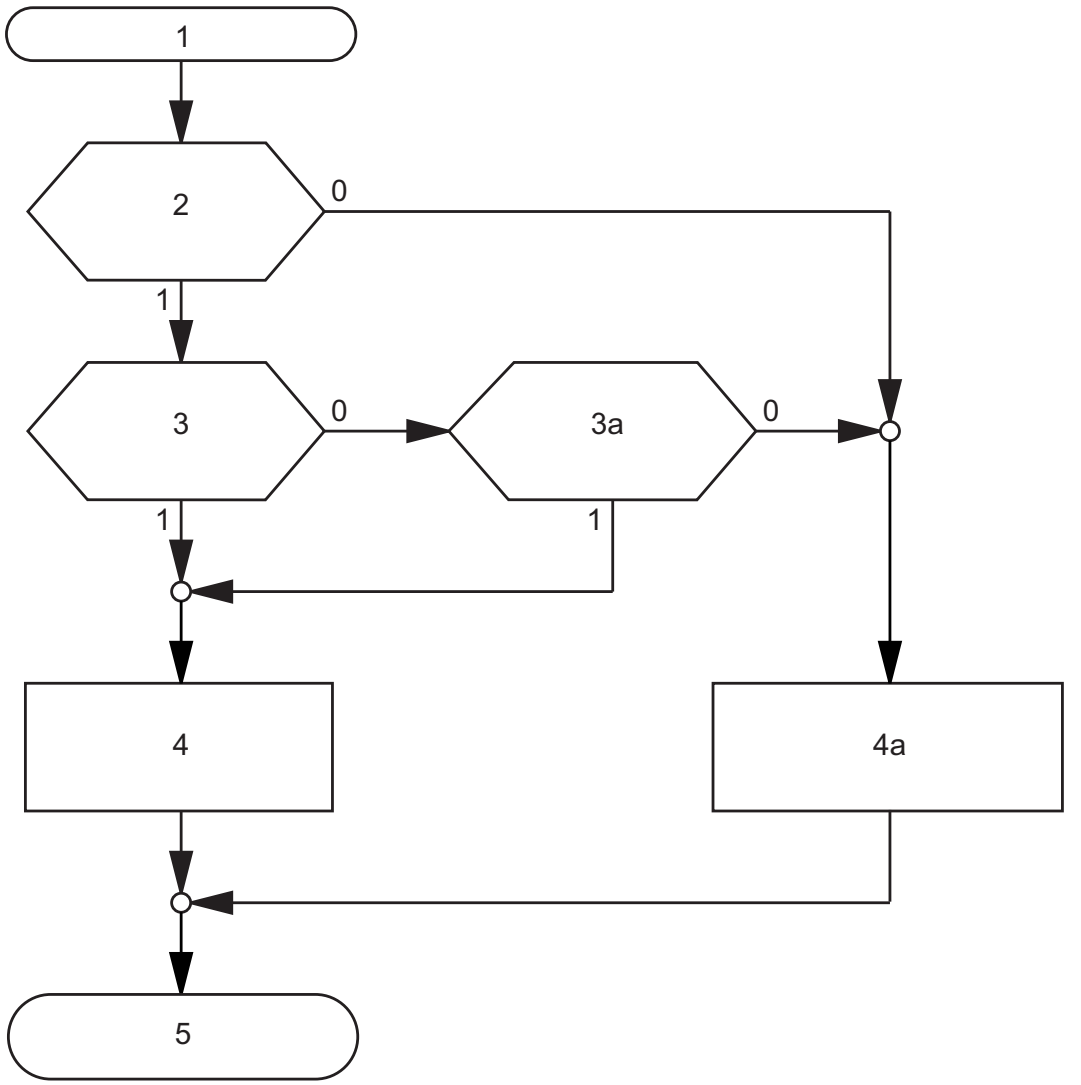



*Figure 13: Flow chart of loading configuration data from the EAM*

*1 – Device start-up*
*2 – EAM plugged-in?*
*3 – Password in device and EAM identical?*
*3a – Default passwort in device?*
*4 – Load configuration from the EAM, EAM-LEDs flashing sychronously*
*4a –Load configuration from local memory, EAM-LEDs flashing alternately*
*5 – Configuration data loade*

# 3.5 System Configuration via DHCP

When it is started up via DHCP (dynamic host configuration protocol), a device receives its configuration data in accordance with the flow chart. DHCP enables the configuration of the device (DHCP Client) via a name. 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 IP parameters according to the “DHCP process” flowchart (see fig. 14).

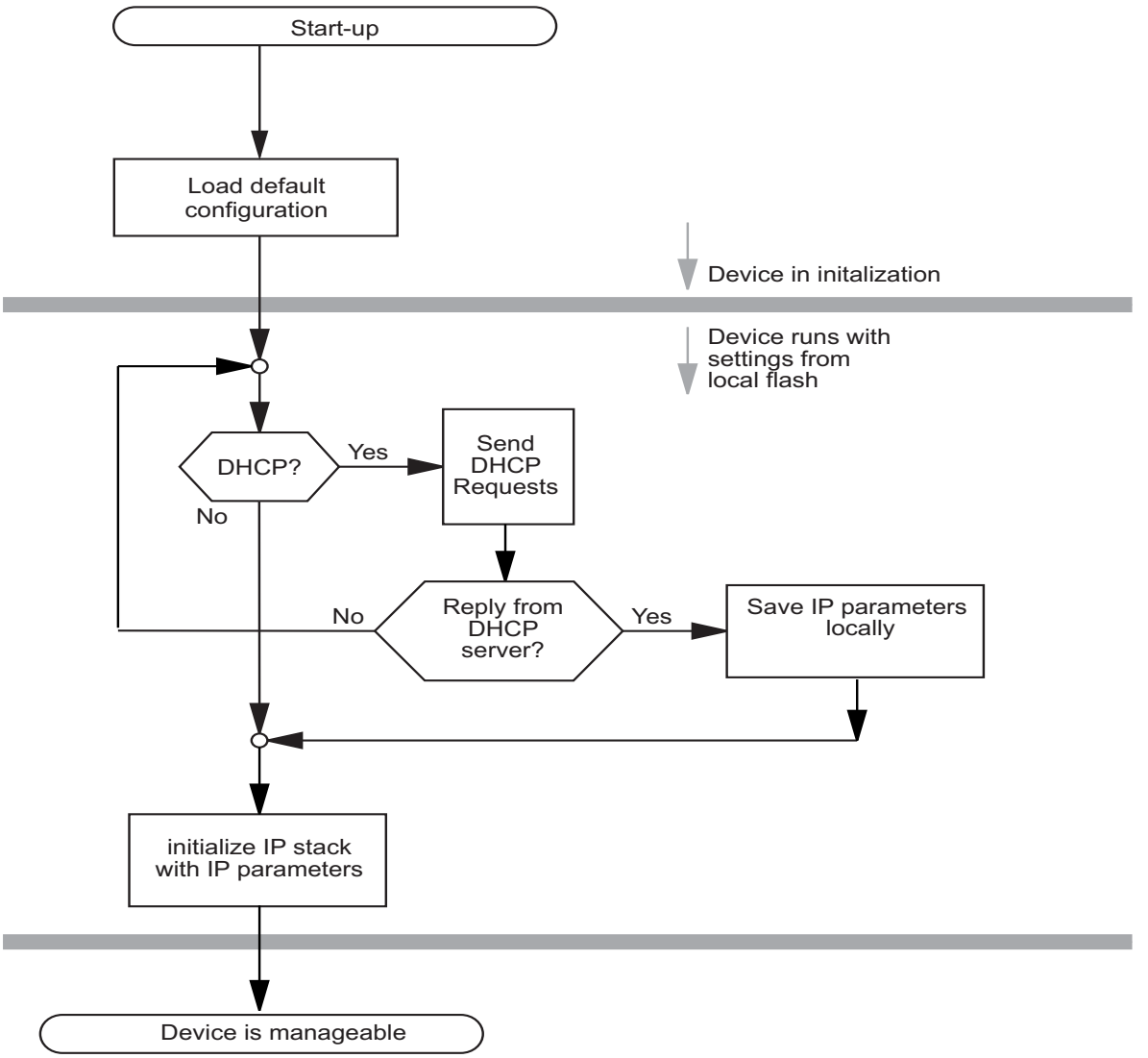



*Figure 14: Flow chart for the DHCP process*

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.
The device accepts this data as configuration parameters (see on page 61 “Web-based IP Configuration”).
If an IP address was assigned by a DHCP server, it will be saved locally

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

*Table 5: DHCP Options requested by the device*

The DHCP server provides (“leases”) the configuration parameters for a specific time period.
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 inactive.
If 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 61 “Web-based IP Configuration”).

Example of a DHCP-configuration file:

```
# /etc/dhcpd.conf for DHCP Daemon
#
subnet 10.1.112.0 netmask 255.255.240.0 {
option subnet-mask 255.255.240.0;
option routers 10.1.112.96;
}
#
# Host berta requests IP configuration
# with her MAC address
#
host berta {
hardware ethernet 00:80:63:08:65:42;
fixed-address 10.1.112.82;
}
#
# Host hugo requests IP configuration
# with his client identifier.
#
```

```
host hugo {
#
option dhcp-client-identifier "hugo";
option dhcp-client-identifier 00:68:75:67:6f;
fixed-address 10.1.112.83;
server-name "10.1.112.11";
filename "/agent/config.dat";
}
```

Lines that begin with the #-character contain comments.
The lines that precede the individual devices indicate settings that apply to the following device.
The fixed-address line assigns a fixed IP address to the device.
Please refer to your DHCP-Server manual for more details.

# 3.6 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, define the handling of the VLAN ID and configure the Ethernet Switch Configurator access.

☐ Choose the operating mode (see on page 20 “Configuring the application”).

## 3.6.1 IP configuration in Transparent Mode

☐ In the “Protocol” frame, you enter where the device is to obtain its IP parameters:
- ▶ Select “DHCP” if the configuration is to be performed by a DHCP server on the basis of the MAC address or the name of the device (see page 57 “System Configuration via DHCP”).
- ▶ If “DHCP” is not selected, the device uses the network parameters in its local memory.

☐ Select “Use VLAN Tag” if you want the device to evaluate the VLAN tag of the data packets received. If this function is active, you can only access the management of the device VLAN entered in “Management VLAN ID” (see below).

☐ The “Management VLAN ID” line enables you to assign a VLAN to the interface for the management of the device (see “Use VLAN Tag” above).

### Entering local IP parameters

- ☐ Enter the IP address of the device in the “IP Address” field.
- ☐ In the “Gateway IP Address” field, enter the IP address of the gateway to which the device is to forward data packets whose destination address is outside its own subnetwork.
- ☐ Enter the netmask in the “Netmask” field.

### Getting IP Parameters via DHCP

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

### Configuring 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. Activate the Ethernet Switch Configurator protocol if you want to transfer an IP address to the device from your PC with the enclosed Ethernet Switch Configurator software (setting on delivery: active).

### Save IP configuration

Save the settings so that you will still have the entries after a restart (see page 68 “Editing and managing Configurations”).

## 3.6.2 IP configuration in Router Mode

In Router Mode, the device requires the IP parameters to be entered on the internal and external interfaces.

☐ In the “Protocol” frame, you enter where the device is to obtain its IP parameters:
- ▶ Select “DHCP” if the configuration is to be performed by a DHCP server on the basis of the MAC address or the name of the device (see page 57 “System Configuration via DHCP”).
- ▶ If “DHCP” is not selected, the device uses the network parameters in its local memory.

☐ Select “Use VLAN Tag” if you want the device to evaluate the VLAN tag of the data packets received. When this function is active, the device drops those data packets received whose VLAN tag contains a VLAN ID different to the one entered in this dialog.

☐ The “VLAN ID” line enables you to allocate a VLAN to the interface.

### Entering local IP parameters

☐ Enter the IP address of the device in the “IP Address” field.
☐ Enter the netmask in the “Netmask” field.
☐ In the “Gateway IP Address” field, enter the IP address of the gateway to which the device is to forward data packets whose destination address is outside its own subnetwork.
☐ If you want to allocate more than one IP address to an interface, you can press “Create” to enter additional IP parameters in the table below.
You require multiple IP addresses on an interface if you want to connect large flat networks with different subnetworks at one port.

### Getting IP Parameters via DHCP

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

### Save IP configuration

Save the settings so that you will still have the entries after a restart (see page 68 “Editing and managing Configurations”).

## 3.6.3 IP configuration in PPPoE Mode

In Router Mode, the device requires the IP parameters to be entered on the internal interface. The device gets the IP parameters for the external interface from the connection provider.

☐ In the “Protocol” frame, you enter where the device is to obtain its IP parameters:
- ▶ Select “DHCP” if the configuration is to be performed by a DHCP server on the basis of the MAC address or the name of the device (see page 57 “System Configuration via DHCP”).
- ▶ If “DHCP” is not selected, the device uses the network parameters in its local memory.

☐ Select “Use VLAN Tag” if you want the device to evaluate the VLAN tag of the data packets received. When this function is active, the device drops those data packets received whose VLAN tag contains a VLAN ID different to the one entered in this dialog.

☐ The “VLAN ID” line enables you to allocate a VLAN to the interface.

## Entering local IP parameters

☐ Enter the IP address of the device in the “IP Address” field.
☐ Enter the netmask in the “Netmask” field.
☐ In the “Gateway IP Address” field, enter the IP address of the gateway to which the device is to forward data packets whose destination address is outside its own subnetwork.
☐ If you want to allocate more than one IP address to an interface, you can press “Create” to enter additional IP parameters in the table below.
You require multiple IP addresses on an interface if you want to connect large flat networks with different subnetworks at one port.

## Getting IP Parameters via DHCP

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

## Entering PPPoE connection parameters

☐ Enter the connection parameters that you got from your provider for the connection.

- Username
- Password
- MTU (Maximum Transmission Unit).
The MTU specifies the maximum frame size that this connection can transmit. If larger data packets are to be transmitted, the Firewall fragments the larger data packet into multiple small data packets.

## Save IP configuration

Save the settings so that you will still have the entries after a restart (see page 68 “Editing and managing Configurations”).

# 3.7 Faulty Device Replacement

The device provides a plug-and-play solution 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 55 “Loading the System Configuration from the EAM”).

When the new device is started, it is given the same configuration data that the faulty device had.

# 4 Basic Settings

The basic settings of the device include:

- Editing and managing configurations (device settings)
- Loading the latest device software
- Configuring the ports of the device
- Synchronizing the system time in the network

# 4.1 Editing and managing Configurations

When it is restarted, the device loads its configuration (settings) from its non-volatile memory, once you have not activated DHCP and no EAM is connected to the device.

During operation, the device allows you to load configurations (settings) from the following sources:
- from its non-volatile memory (NVM),
- from the Memory Backup Adapter. If an EAM is connected to the device, the device loads its configuration from the EAM if the configuration safed on the EAM differs from the confiuration safed locally.

The device saves configurations (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 allows you to do the following with configurations (settings):
- activate them,
- save them,
- reset them to the state on delivery,
- load them from the non-volatile memory (NVM),
- copy them,
- display them,
- delete them.

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.

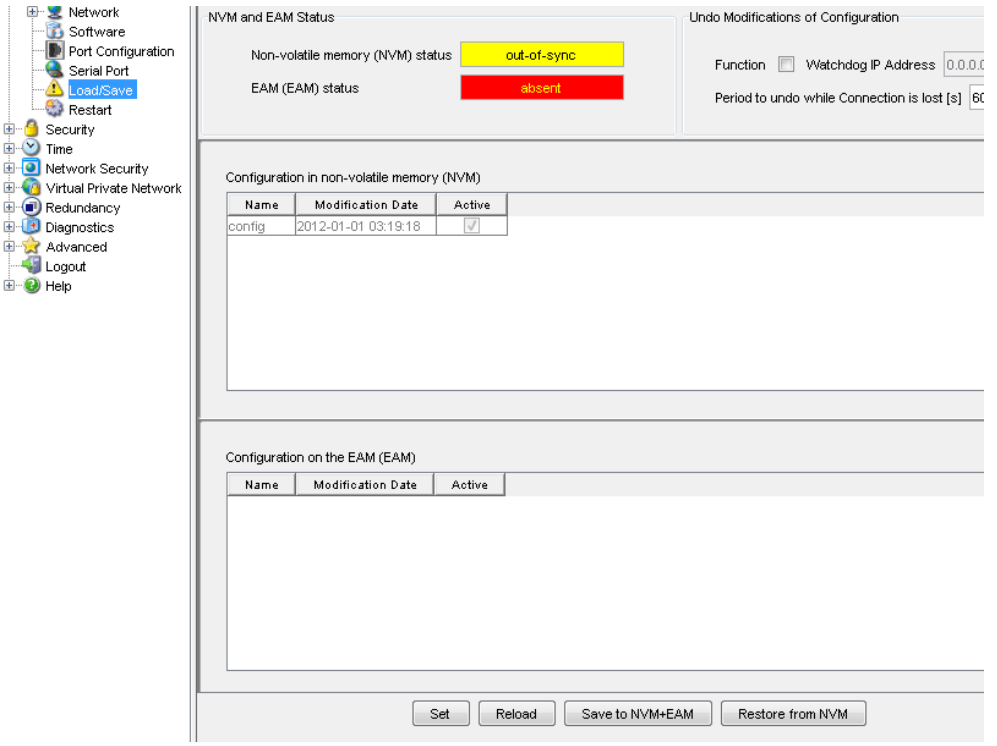



*Figure 15: Load/Save dialog*

## 4.1.1 Activating a Configuration

The device allows you to activate a stored configuration from the table “Configuration in the non-volatile memory (NVM)”.

☐ Select the dialog `Basic Settings:Load/Save`.
☐ Select a non-active configuration file in the NVM configuration table.
☐ Click on “Activate”.

In the “Active” column, the device shows you the active configuration. If an EAM with the same configuration file is connected, the device activates the configuration file on the EAM and grays out the display of the activation in the NVM table.

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `show config profiles nv` | Display the configurations stored in the NVM. |
| `copy config nv profile <name> running-config` | The device loads configuration data “Name” from the local non-volatile memory. |

**Note:** If you mark a configuration as active using the alternative CLI command `profile activate nv <id>`, it will only take effect after you issue the CLI command `copy config nv running-config`.

**Note:** When loading (activating) 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 can take several seconds. Wait until the device selects the new configuration in the “Active” column.

## 4.1.2 Saving the Configuration

The device allows you to do the following with the current configuration (setting) on the device and the EAM

- save it in a new configuraton file,
- save it in the active configuration file.

## Saving a configuration in a new configuration file

- ☐ Select the `Basics: Load/Save` dialog.
- ☐ Click on “Create” to open a window for entering a new row in the table.
- ☐ Enter a name in “Configuration name” in the file window.
- ☐ Click on “OK”.

The device saves the configuration in a new file in the NVM and on the EAM.

**Note:** Do not use space characters in filenames. The maximum length is 32 characters.

## Saving a configuration in an active configuration file

The device allows you to replace the active configuration with the current configuration.
Note than you overwrite the active configuration file when you save the current configuration in it.

- ☐ Select the dialog `Basic Settings:Load/Save`.
- ☐ Click on “Save to NVM + EAM” when you want to replace the active configuration with the current configuration in the non-volatile memory and on the EAM.

**Note:** If you want to load the active configuration file from the local non-volatile memory, click on „Restore from NVM“.

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `copy config running-config nv` | The device saves the current configuration data in the local non-volatile memory and, if an EAM is connected, also on the EAM. |

### 4.1.3 Resetting the Configuration to the State on Delivery

The device allows you to reset the configuration to the state on delivery.

☐ Select the `Basic Settings:Restart` dialog.
☐ Click on “Reset to factory”.

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `clear factory` | Reset NVM and EAM to the factory settings. |
| `clear config` | Delete the current configuration, including the IP parameters. |

Setting in the system monitor:

☐ Select `5` “Erase main configuration file”
This menu item allows you to reset the configuration of the device to its state on delivery.
☐ Press the Enter key to restore the configuration of the state on delivery.

**Note:** The device deletes the tables, settings and files on the device and on a connected EAM.

**Note:** The command “clear config” does not clear the name of the active configuration profile. Use the command “save profile” to store the cleared configuration under a new name.

### 4.1.4 Loading the active Configuration

The device allows you to load the active configuration.

☐ Select the dialog `Basic Settings:Load/Save`.
☐ Click on “Restore from NVM” if you want to load the active configuration file from the non-volatile memory.

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `copy config nv running-config` | Load the active configuration. |

### 4.1.5 Copying Configuration Files

**Copying from a PC to the device**

The device allows you to copy a configuration file from a PC to the device.

☐ Select the `Basics: Load/Save` dialog.
☐ Click on “Copy from PC” beside the NVM configuration table.
☐ In the file selection frame, click on “...”.
☐ In the file selection window, select the configuration file (*.cfg) and click on “Set”.
☐ In the file selection frame, click on “Copy from PC”.

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

▶ Update completed successfully.
▶ File not found. Reason: File name not found or does not exist.

## Copying from a PC to the EAM

The device allows you to copy a configuration file from a PC to the EAM.

- ☐ Select the `Basics: Load/Save` dialog.
- ☐ Click on “Copy from PC” beside the EAM configuration table.
- ☐ In the file selection frame, click on “...”.
- ☐ In the file selection window, select the configuration file (*.cfg) and click on “Set”.
- ☐ In the file selection frame, click on “Copy from PC”.

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

- ▶ Update completed successfully.
- ▶ File not found. Reason: File name not found or does not exist.

When you restart, the device adopts the configuration data of the EAM and saves it in the flash memory. If the connected EAM does not contain any valid data, for example, if it is in the delivery state, the device loads the data from the flash memory.

Before loading the configuration data from the EAM, the device compares the password in the device with the password in the EAM configuration data.

The device loads the configuration data if

- ▶ the admin password matches or
- ▶ there is no password stored locally or
- ▶ the local password is the delivery state password or
- ▶ no configuration is saved locally.

## Copying from the device or the EAM to a PC

The device allows you to save a configuration file of the device or the EAM on a PC.

- ☐ Select the `Basics: Load/Save` dialog.
- ☐ Select a table entry
  - – of the device (configuration in the non-volatile memory (NVM)) or
  - – of the EAM (configuration on the Memory Backup Adapter (EAM))
- ☐ Click on “Copy to PC”.
- ☐ In the file selection window, select the desired directory and click on “Set”.

### Copying from the EAM to the device

The device allows you to store a configuration file from the EAM on the device.

- ☐ Select the `Basics: Load/Save` dialog.
- ☐ Select a table entry of the EAM (configuration on the Memory Backup Adapter (EAM)).
- ☐ Click on “Copy to NVM”.

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `copy config eam profile <name> nv` | Load configuration “Name” onto the device. |

## 4.1.6 Displaying a Configuration File

The device allows you to display a configuration file on the device and on the EAM.

- ☐ Select the `Basics: Load/Save` dialog.
- ☐ Select a table entry
  - – of the device (configuration in the non-volatile memory (NVM)) or
  - – of the EAM (configuration on the Memory Backup Adapter (EAM))
- ☐ Click on “Show”.

## 4.1.7 Deleting a Configuration File

The device allows you to delete a non-active configuration file on the device and on the EAM.

☐ Select the `Basics: Load/Save` dialog.
☐ Select a non-active table entry
– of the device (configuration in the non-volatile memory (NVM)) or
– of the EAM (configuration on the Memory Backup Adapter (EAM))
☐ Click on “Delete”.

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `show config profiles nv` | Display the configurations stored in the NVM. |
| `profile delete nv <index>` | Delete the configuration with the specified index in the NVM. |
| `show config profiles eam` | Display the configurations stored in the EAM. |
| `profile delete eam <index>` | Delete the configuration with the specified index in the EAM. |

## 4.1.8 SFTP Access to Device Files

The device allows you to use SFTP to access device files such as configuration files or the EAM, or to load a firmware update or VPN certificates onto the device. To do this, use an SFTP client, such as WinSCP. For the SFTP access, you must have SSH access to the device.

To do this, enable the SSH access to the device (see on page 102 “Configuring the CLI Access”).

### 4.1.9 Cancelling a Configuration Change

The device allows you to automatically cancel a configuration change if the device loses its network connection with the management station from which you configure the device. An example is the inadvertent changing of the device's IP address.

You can use this function during remote maintenance.

When the function is active, the device constantly checks if it is periodically accessed from the management station’s IP address. If these accesses are not received within a certain time, the device replaces its current configuration with the most recently saved configuration.

This function is useful for administrators when the device is far removed or difficult to access.

State on delivery: Operation: Off, Waiting time: 600 s.

**Note:** Deactivate the function after you have successfully saved the configuration. In this way you help prevent the device from reloading the configuration after you close the web interface.

- ☐ Select the `Basics: Load/Save` dialog.
- ☐ To activate the function, select “Function” in the “Configuration change” frame.
- ☐ Enter the waiting time at “Period until cancellation when connection is interrupted”.
- ☐ Click “Set” to temporarily save the entry in the configuration.
- ☐ Click “Load” to display the IP address of your management station in the “Watchdog IP address” field.

- ☐ To deactivate the function, deselect “Function” in the “Configuration change” frame.
- ☐ Click “Set” to temporarily save the entry in the configuration.
- ☐ Then click on “Load”. The “Watchdog IP address” field now shows 0.0.0.0.

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `show config-watchdog` | Display of settings for the automatic cancellation of a configuration change during a connection interruption. |
| `configure` | Switch to the Configuration mode. |
| `config-watchdog admin-state enable` | Activation of the automatic cancellation of a configuration change during a connection interruption. |
| `config-watchdog admin-state disable` | Deactivation of the automatic cancellation of a configuration change during a connection interruption. |
| `config-watchdog timeout 300` | Timeout settings for automatic cancellation of a configuration change during a connection interruption at 300 s. |

# 4.2 Loading Software Updates

## 4.2.1 Checking the installed Software Release

☐ Select the `Basics:Software` dialog.

☐ This dialog shows you the variant, the release number and the date of the software saved on the device.

- "Stored Version": the software in the non-volatile memory
- "Running Version": the software currently being used
- "Backup Version": the backup software in the non-volatile memory

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `show system info` | Display the system information. |

```
System information
------------------
System Description..... TCSEFEC23F3F20_ConneXium Industrial
   Firewall TX/TX
System Name.................. TCSEFEC23F3F20
System Location..............
System Contact................. www.schneider-electric.com
System Uptime................. 0 days 0 hours 2 minutes 42 seconds
System Date and Time (local time zone)... FRI FEB 17 08:08:08 2012
OS Software Release........... L3S-05.2.0x 2012-02-17 08:08
OOS Software Release (ROM).... L3S-05.2.0x 2012-02-17 08:08
Software Release (BAK)........ L3S-05.2.0x 2012-02-17 08:08
Device Hardware Revision...... 1.13
Device Hardware Description... TCSEFEC23F3F20
Serial Number................. 943987001000201358
Network Operation Mode........ Transparent Mode
IP address (management)....... 192.168.154.87
MAC address (management)...... 00:80:63:95:ef:8d
Configuration state (running to NV)..... ok
Configuration state (NV to EAM)......... ok
Memory Backup Adapter, Serial Num.. 943271001020201583
Power Supply P1, State.................. ok
Power Supply P2, State.................. ok
Temperature (°C)........................ 49
```

### 4.2.2 Loading the Software

The device gives you two options for loading the software:

- from the TCSEAM0100-Adapter (out-of-band)
- via a file selection dialog from your PC.

**Note:** The existing configuration of the device is kept after the new software is installed.

### 4.2.3 Loading the Software from the EAM

You can connect the TCSEAM0100-Adapter to a USB port of your PC like a conventional USB stick and copy the device software into the main directory of the TCSEAM0100-Adapter.

☐ Connect the TCSEAM0100-Adapter with the device software to the device's USB port.

#### Loading with the system monitor

☐ Open the system monitor (see page 26 "System Monitor").
☐ Select 2 and press the Enter key to copy the software from the TCSEAM0100-Adapter into the local memory of the device.
☐ Enter the file name of the firmware and confirm your entry with the Enter key.
☐ Press the Enter key to start the loading procedure.
At the end of the loading procedure, 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:

- Select the software to be loaded
- Start the software
- Perform a cold start

#### Loading with the Command Line Interface

☐ Open the Command Line Interface (see on page 28 "Command Line Interface").

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `copy firmware eam filename tcsefec.bin nv` | Load the firmware with the file name "tcsefec.bin" in the non-volatile memory. |
| `Are you sure (Y/N) ? Y` | Confirm the operation with "Y". |

### Performing a cold start

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `reboot` | Perform a cold start. |

In the System Monitor:
The “End (reset and reboot)” menu item of the system monitor allows you to reset the hardware of the device and perform a restart.

## 4.2.4 Loading the Software via File Selection

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

- ☐ In the file selection frame, click on “...”.
- ☐ In the file selection window, select the device software (tcsefec.bin) and click on “Open”.
- ☐ Click on “HTTPS 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.

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

# 4.3 Configuring the Ports

The port configuration consists of:

- Entering the port name
- Switching the port on and off
- Selecting the operating mode
- Activating the display of detected connection errors

### Entering the port name

The “Name” table column allows you to give the port any name you want.

### Switching the port on and off

In the state on delivery, the ports are switched on.

☐ 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, 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 connection errors

In the state on delivery, 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.

# 4.4 Synchronizing the System Time in the Network

The device allows you to synchronize the time in your network.
The actual meaning of the term “real time” depends on the time requirements of the application.

By using NTP, the device is able to determine the time more precisely than by using SNTP. Therefore, as an NTP server it is also able to offer a more precise time.

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

## 4.4.1 Entering the Time

If no reference clock is available, you have the option of adopting the system time from the PC. The device resets the time during a restart.

**Note:** When setting the time in zones with summer and winter times, make an adjustment for the local offset, if applicable.
The SNTP client can also get the SNTP server IP address and the local offset from a DHCP server.
The NTP client gets its NTP server IP address exclusively from the configuration that you set.

☐ Select the `Time:Basic Settings` dialog.

With this dialog you can enter time-related settings.

- The “System time (UTC)” displays the time with reference to the coordinated world time scale UTC (Universal Time Coordinated). The display is the same worldwide. Local time differences are not taken into account.
  Possible sources of the system time (UTC) are: `local`, `sntp` and `ntp`, see “Time source”.
- The devices calculates the “system time” from the “system time (UTC)” and the “local offset” (the local time difference from UTC).
  “System time” = “System time (UTC)” + “Local offset”.
- “Time Source” displays the source of the system time (UTC). The device automatically selects the available source based on accuracy.
  Possible sources are: `local`, `sntp` and `ntp`.
  - The source is initially `local`. This is the system clock of the device.
  - If you have activated the SNTP client and if the device receives a valid SNTP packet, the device sets its time source to `sntp`.
  - If you have activated the NTP client and if the client has synchronized itself, the device sets its time source to `ntp`.

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

☐ The “local offset” is for displaying/entering the time difference between the local time and the “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 “SNTP time”. |

## 4.4.2 SNTP

### 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.

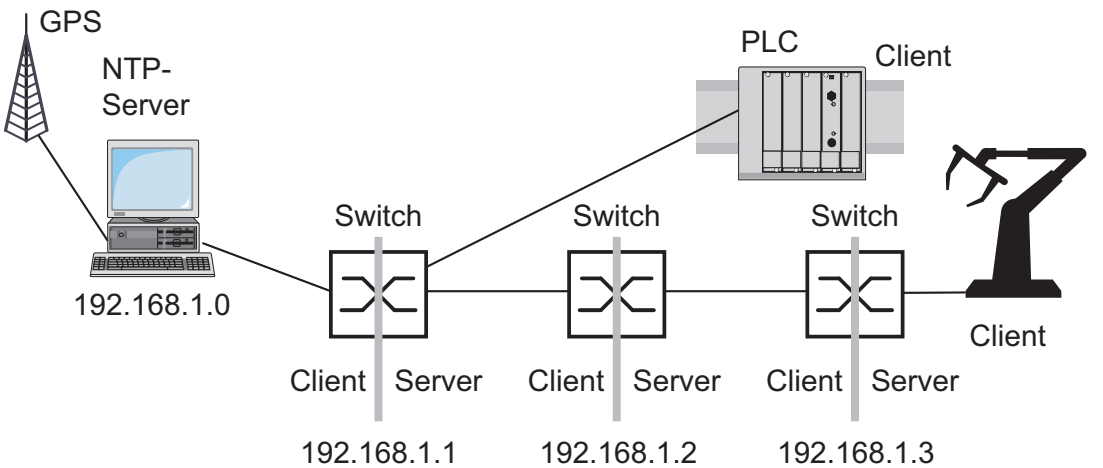



*Figure 16: SNTP cascade*

## Preparing the SNTP Configuration

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

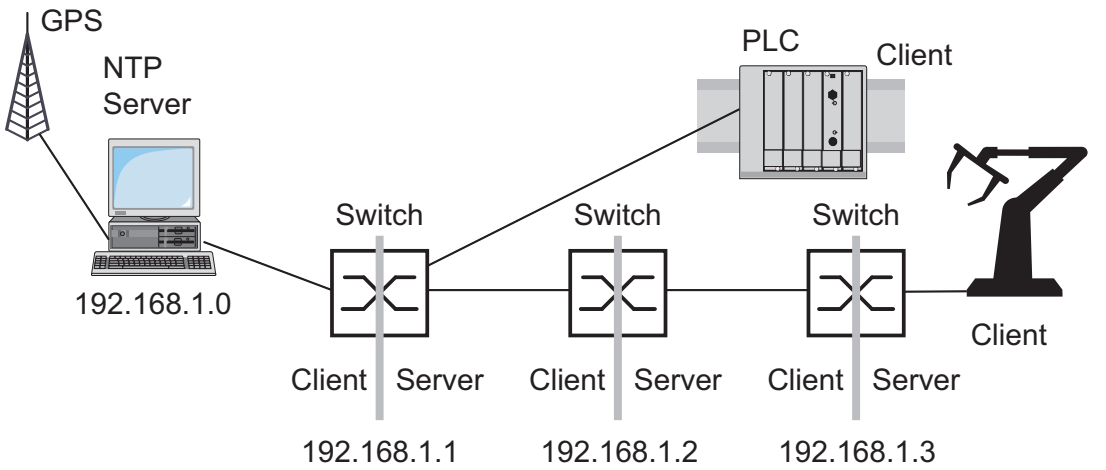



*Figure 17: Example of SNTP cascade*

☐ Enable the SNTP function on the 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.

## Configuring SNTP

☐ Select the `Time:SNTP` dialog.

▶ Operation

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

**Note:** If you switch SNTP on when NTP is already active on the device, the device reports a detected error.
To switch SNTP on, first deactivate NTP.
On delivery, NTP is switched off.

▶ 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 “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 an additional SNTP server. The device periodically requests from this server the system time if it does not receive a response from the server to a request from the “External server address” within 1 second.

**Note:** If you are receiving the system time from an external/ redundant server address, you do not accept any SNTP Broadcast packets (see below). You thus help ensure that the device uses the time of the server entered.

☐ In “Server request interval” you specify the interval at which the device requests SNTP packets (valid entries: 1 s to 3,600 s, on delivery: 30 s).

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

▶ Configuration SNTP Server

☐ In “Anycast destination address” you enter the IP address to which the SNTP server of the device sends its SNTP packets (see table 6).

☐ 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:Basic Settings` 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 6: Destination address classes for SNTP and NTP packets*

| 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 7: Settings for the example (see fig. 17)*

### 4.4.3 NTP

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

With NTP, the device can determine the time more accurately than with SNTP. Thus, as an NTP server it can also provide a more accurate time.

The NTP and SNTP packet formats are identical.
In contrast to the SNTP client, the NTP client uses multiple NTP servers and a more complex algorithm for the synchronization. It can thus determine the time more accurately. Therefore, the synchronization of the NTP client can take longer than an SNTP client.
Only use NTP if you require this increased accuracy.

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

**Note:** To obtain as accurate a system time distribution as possible, use multiple NTP servers for an NTP client.

**Note:** If you switch NTP on (set any value other than `off`) when SNTP is already active on the device, the device reports a detected error.
To switch NTP on, first deactivate SNTP.
On delivery, SNTP is switched off.

# 5 Assistance in the Protection from Unauthorized Access

The device assists against unauthorized access with the following functions:

- Password-protected Web access
- Password-protected CLI access
- Password-protected network management access
- Ethernet Switch Configurator function
- User authentication

**Note:** For security reasons, change the factory setting password. You thus help prevent the device from being accessed with this password. If the password is the factory setting password, the device displays the message “Default Password” in every dialog‘s header line.

**Note:** Choose your password so that you can remember it.

When creating your password, do not use

- short words and character sequences,
- words and character sequences that have a meaning (e.g. names, years, birthdays),
- quotations,
- sequences of simple words.

When creating your password, use

- long words and character sequences,
- words and character sequences that do not seem to have a meaning (e.g. first letters of the words in a sentence),
- unusual words,
- invented words,
- combinations of letters, numbers and special characters. (When selecting special characters, note that these may not be available on foreign keyboards.),
- altered and corrupted spelling (e.g. “pLue PiRD” instead of “Blue bird”).

**Note:** In the state on delivery, SNMPv1 and SNMPv2 access is deactivated. As SNMPv1 and SNMPv2 transfer data unencrypted, using SNMPv1 and SNMPv2 creates a potential security risk. Only allow SNMPv1 or SNMPv2 access if you want to use an application that requires this.

**Note:** In the state on delivery, the device allows SSH, SNMPv3 and HTTPS access.

# 5.1 Web-based Interface Access

You access the Web-based interface with the Hypertext Transfer Protocol Secure (HTTPS).
HTTPS contains an authentication and an encryption of the data to be transmitted. Both are based on a certificate.
In the state on delivery, the device provides a Schneider Electric certificate. When you start the Web-based interface via the browser, your browser will ask you whether you trust the certificate, no matter what the browser's default settings are.
In the `Security:Web Access` dialog, you can load a different certificate from your PC onto the device.

### 5.1.1 Description of Web-based Interface Access

The device helps you protect the access to the Web-based interface in a number of ways:

- Password
- Selection of the SNMP port
  To access the Web-based interface, your browser uses a Java application that it downloads from the device. This Java application communicates with the device via SNMPv3.
  Applications use the standard port 161 for an SNMP connection.
  The device allows you to use a different port
- Alternatively, the device allows you to tunnel the SNMP access of the Web-based Interface to the device via HTTPS. Thus only HTTPS connections to the device are necessary. The factory setting for the function SNMP over HTTPS (Tunnel) is inactive.
- Activate/deactivate
- Selection of the HTTPS port
  To access the Web-based interface, your browser sets up an HTTPS connection to the device. Applications use the standard port 443 for an HTTPS connection.
  The device allows you to use a different port
- Restrictions for IP addresses permitted access for each port
  In the state on delivery, you can access the device with every IP address via the internal port. The device allows you to specify for each port from which IP address the device allows or denies access.
- Automatic logout after inactivity

## 5.1.2 Configuring the Web-based Interface Access

To help protect the access, use the options the device provides you with. The figure shows a typical example for accessing the internal port of the Firewall.
The following table contains examples of the parameters for the subsequent configuration example.

| Parameter | Value |
|---|---|
| Read password | Heinrich5 |
| Write/read password | Ludwig14 |
| SNMP port | 9223 |
| SNMP source address of internal port | 10.0.1.17/24 |
| Web server active | Yes |
| HTTPS port | 9027 |
| HTTPS source address of internal port | 10.0.1.17/24 |

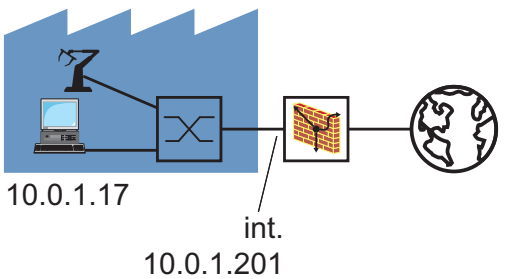



*Figure 18: Application example of Web-based interface access*

☐ Enter new passwords.

☐ Select the `Security:Password` dialog.
☐ 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.

**Note:** If you do not know a password with “read/write” access, you will have no write access to the device.

**Note:** For security reasons, the dialog shows the passwords as asterisks. Make a note of every change. You cannot access the device without a valid password.

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

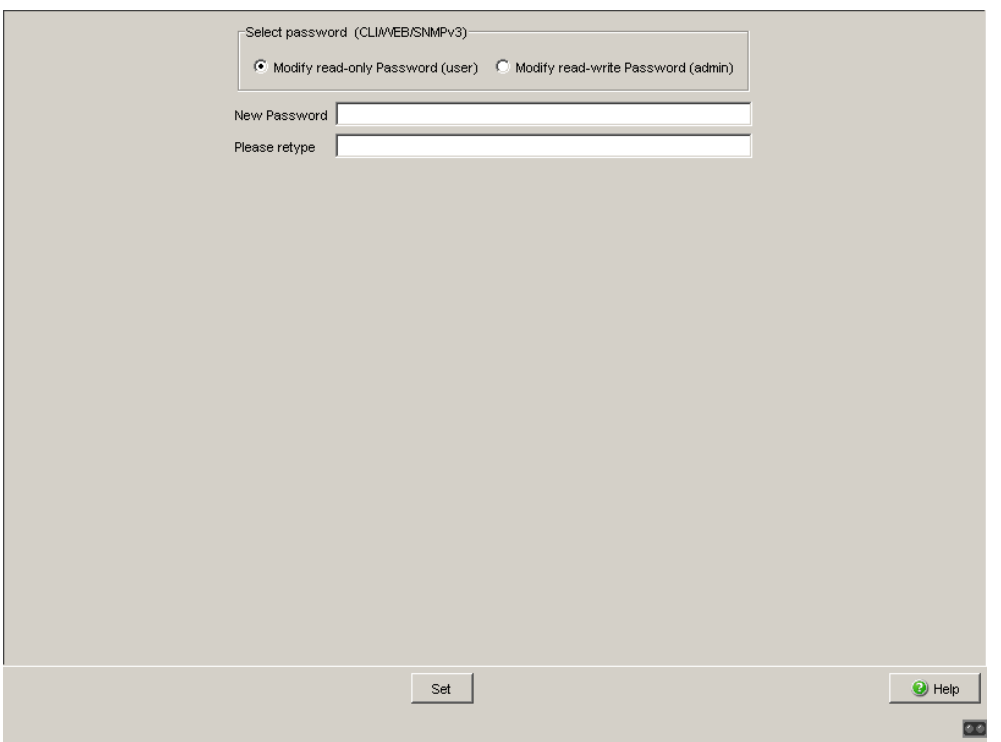



*Figure 19: Password Dialog*

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

☐ Configure the SNMP access.

☐ Select the `Security:SNMP Access` dialog.
☐ Change the SNMP port to `9223`, for example.
Restrict the IP address which are permitted access via SNMP:
☐ Click on “Create Entry”.
☐ In the “Port” cell of the new entry in the table, select `int`.
☐ Double-click in the “Source IP (CIDR)” cell and enter the source address, e.g. `10.0.1.17`.
If this is the only active entry in this table, then only the PC with this IP address can access via this protocol.
☐ Click on the “Active” field of this entry to activate the entry.
☐ Click “Set” to temporarily save the entry in the configuration.

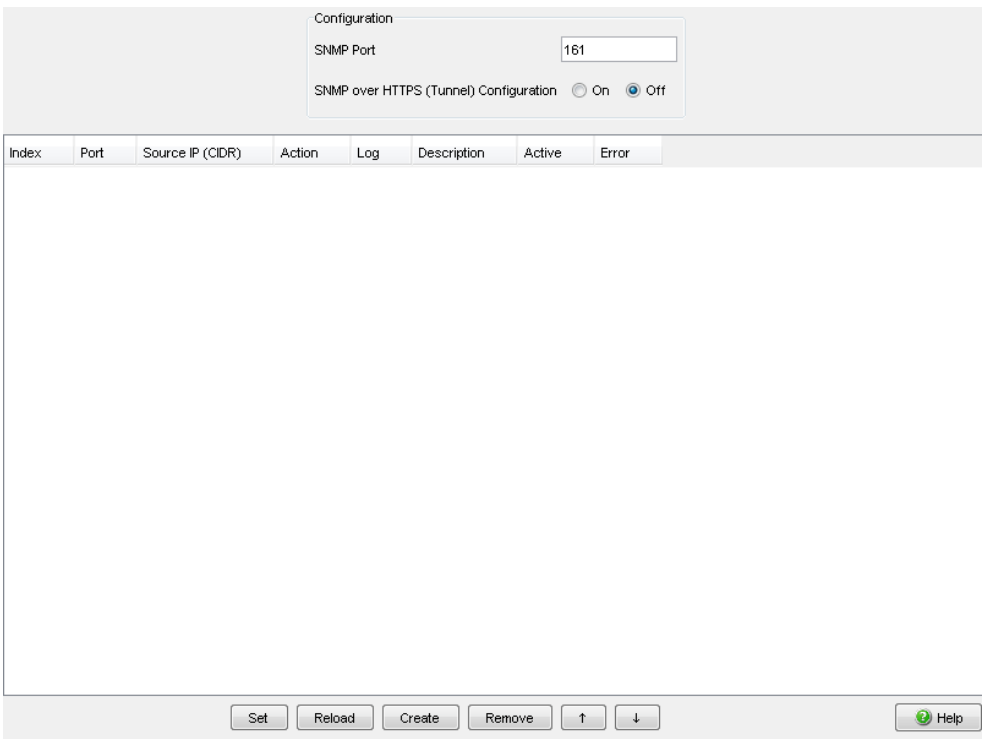



*Figure 20: SNMP Access dialog*

☐ Configure the Web access.

☐ Select the `Security:Web Access` dialog.
☐ Change the HTTPS port to `9027`, for example.

Restrict the IP address which are permitted access via HTTPS:

☐ Click on “Create Entry”.
☐ In the “Port” cell of the new entry in the table, select `int`.
☐ Double-click in the “Source IP (CIDR)” cell and enter the source address, e.g. `10.0.1.17`.
If this is the only active entry in this table, then only the PC with this IP address can access via this protocol.
☐ Click on the “Active” field of this entry to activate the entry.
☐ Click “Set” to temporarily save the entry in the configuration.

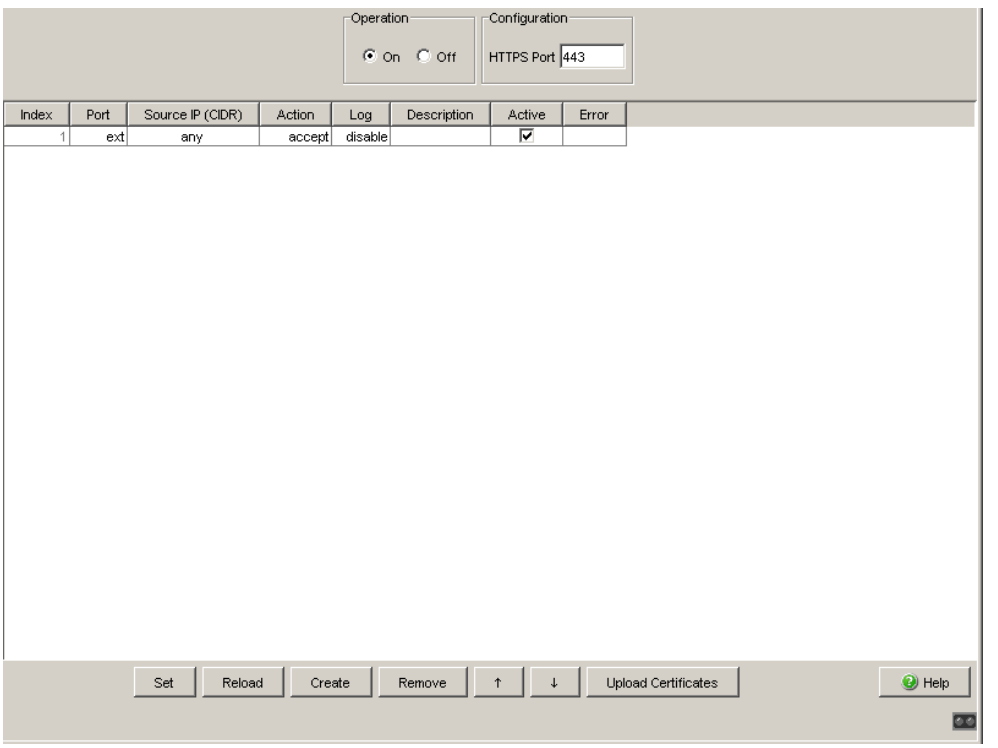



*Figure 21: Web Access dialog*

☐ Configure the automatic logout.

☐ Select the `Logout` dialog.
☐ In the “Automatically” line in the “Web-based Interface” frame, click “On”.
☐ In the “After [min]” line, enter the number of minutes of inactivity after which the device automatically terminates the HTTPS connection.
☐ Click “Set” to temporarily save the entry in the configuration.

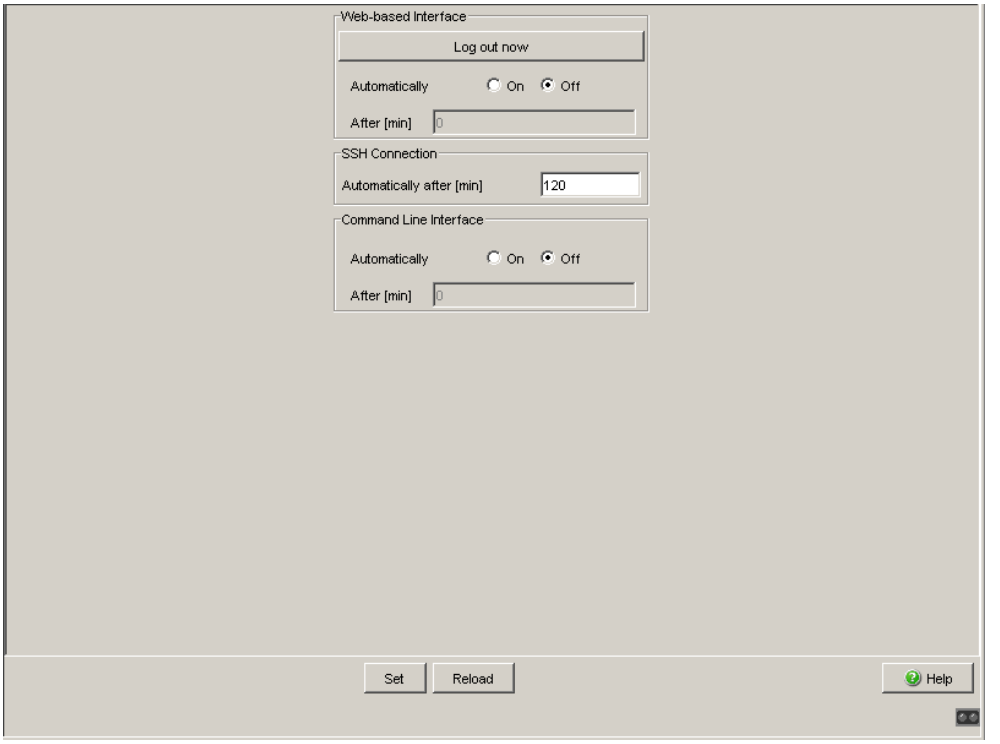



*Figure 22: Logout dialog*

☐ Save the settings in the non-volatile memory.

☐ Select the dialog `Basic Settings:Load/Save`.
☐ Click on “Save to NVM + EAM” to save the configuration in the active configuration.

# 5.2 CLI Access

To access the Command Line Interface (CLI), you need a direct connection from your PC to the serial port or a Secure Shell (SSH) connection to your device (see on page 220 “Access via SSH”).

## 5.2.1 Description of CLI Access

The device helps you protect the access to the CLI in a number of ways:

- Password
- Activate/deactivate
  After the SSH server has been deactivated, the device helps prevent renewed access via a new SSH connection. If an SSH connection already exists, it is kept.
- Selection of the SSH port
  Applications use the standard port 22 for an SSH connection.
  The device allows you to use a different port
- Restrictions for IP addresses permitted access for each port
  In the state on delivery, you can access the device with every IP address via the internal port. The device allows you to specify for each port from which IP address the device allows or denies access.
- Automatic logout after inactivity

## 5.2.2 Configuring the CLI Access

To help protect the access, use the options the device provides you with. The figure shows a typical example for accessing the internal port of the Firewall.

The following table contains examples of the parameters for the subsequent configuration example.

| Parameter | Value |
|---|---|
| Read password | Heinrich5 |
| Write/read password | Ludwig14 |
| SSH access active | Yes |
| SSH Port | 9234 |
| SSH source address of internal port | 10.0.1.17/24 |

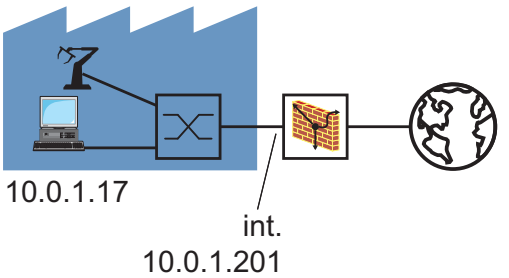



*Figure 23: Application example of Command Line Interface access*

☐ Enter new passwords.

☐ Select the `Security:Password` dialog.
☐ 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.

**Note:** If you do not know a password with “read/write” access, you will have no write access to the device.

**Note:** For security reasons, the dialog shows the passwords as asterisks. Make a note of every change. You cannot access the device without a valid password.

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

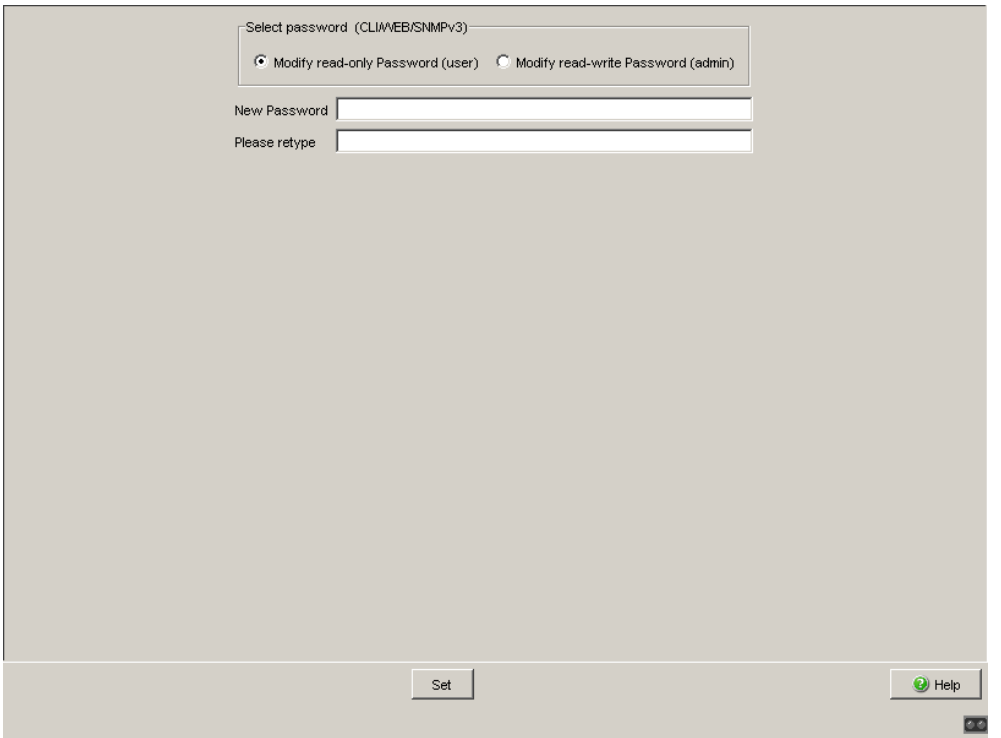



*Figure 24: Password Dialog*

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

☐ Configure the SSH access.

☐ Select the `Security:SSH Access` dialog.
☐ Change the SSH port to `9243`, for example.
Restrict the IP address which are permitted access via SSH:
☐ Click on “Create Entry”.
☐ In the “Port” cell of the new entry in the table, select `int`.
☐ Double-click in the “Source IP (CIDR)” cell and enter the source address, e.g. `10.0.1.17`.
If this is the only active entry in this table, then only the PC with this IP address can access via this protocol.
☐ Click on the “Active” field of this entry to activate the entry.
☐ Click “Set” to temporarily save the entry in the configuration.

**Note:** The device allows you to use SFTP to access device files such as configuration files or the EAM, or to load a firmware update or VPN certificates onto the device. To do this, use an SFTP client, such as WinSCP. For the SFTP access, you must have SSH access to the device.

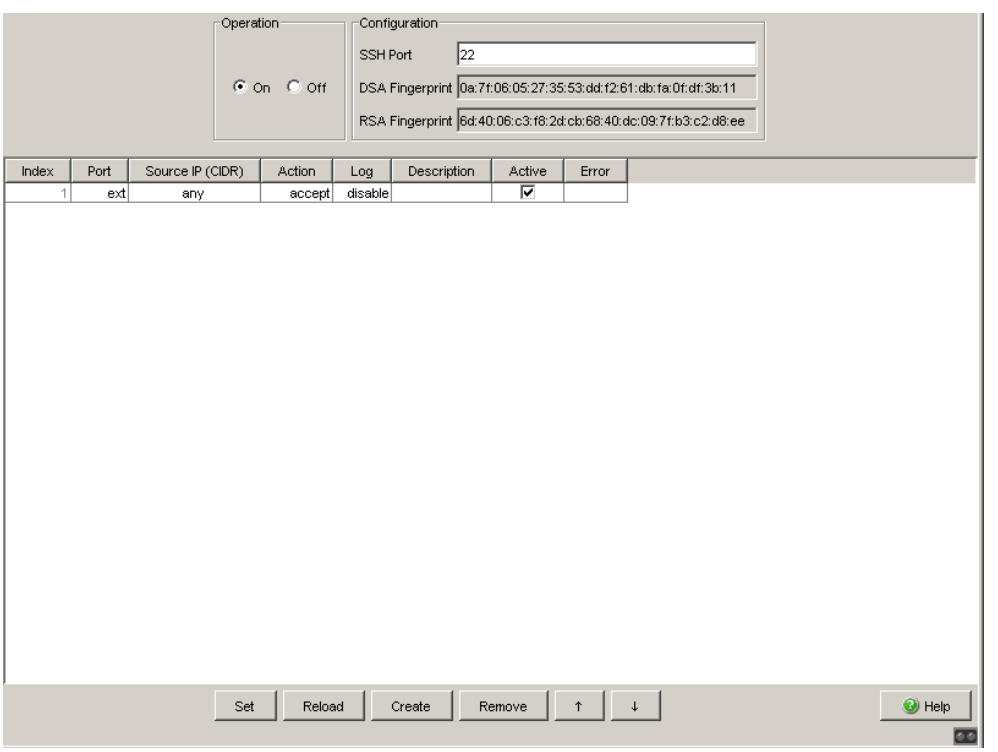



*Figure 25: SSH Access dialog*

☐ Configure the automatic logout.

☐ Select the `Logout` dialog.
☐ In the “SSH connection” frame, in the “After [min]” line, enter the number of minutes of inactivity after which the device automatically terminates the SSH connection.
☐ In the “Automatic” line in the “Command Line Interface” frame, click “On”.
☐ In the “After [min]” line, enter the number of minutes of inactivity after which the device automatically terminates the HTTPS connection.
☐ Click “Set” to temporarily save the entry in the configuration.

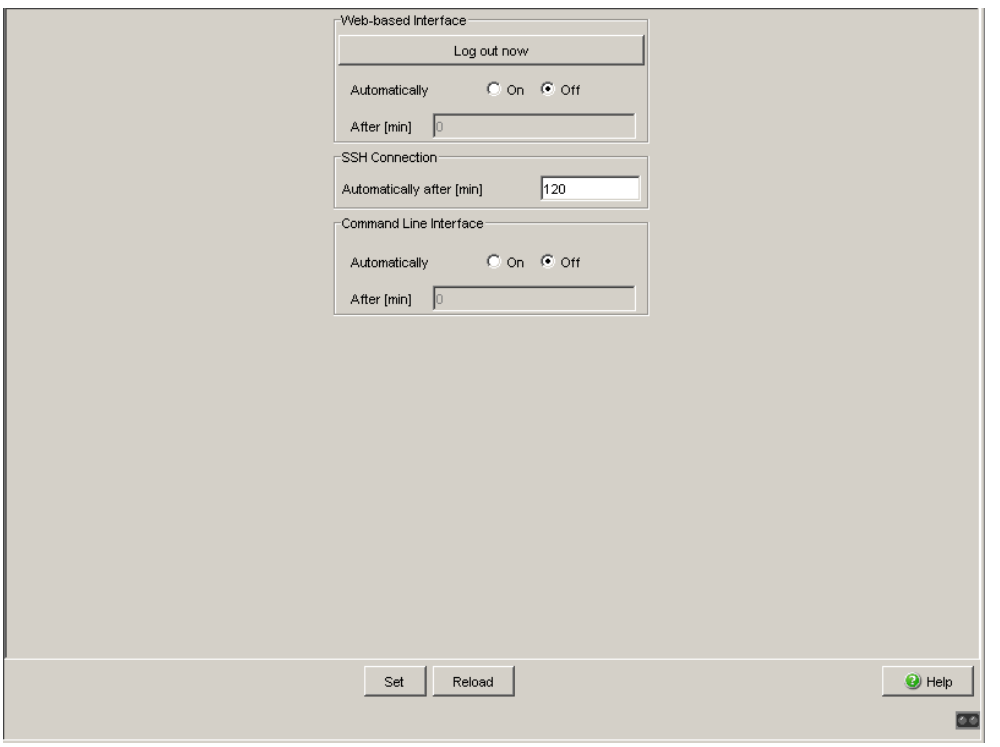



*Figure 26: Logout dialog*

☐ Save the settings in the non-volatile memory.

- ☐ Select the dialog `Basic Settings:Load/Save`.
- ☐ Click on “Save to NVM + EAM” to save the configuration in the active configuration.

# 5.3 Network Management 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 MIB of the device.

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

To help you 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 MIB of the device with the IP address of your computer.

☐ Check which SNMP version your Network Management software communicates with.
If necessary, activate SNMPv1 or SNMPv2.

☐ Enter the SNMP access rules.

# 5.4 Ethernet Switch Configurator Access

## 5.4.1 Description of the Ethernet Switch Configurator Protocol

The Ethernet Switch Configurator-Protocol allows you to allocate an IP address to the device in transparent mode on the basic of its MAC address (see on page 52 “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 decive.

## 5.4.2 Enabling/disabling the Ethernet Switch Configurator Function

☐ Select the `Basic Settings:Network:Transparent Mode` dialog.

☐ Disable the Ethernet Switch Configurator-Function in the „Ethernet Switch Configurator Protocol“ frame or limit the access to „read-only“.

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `network protocol ethernet-switch-conf off` | Disable Ethernet Switch Configurator function. |
| `network protocol ethernet-switch-conf read-only` | Enable Ethernet Switch Configurator function with “read-only” access |
| `network protocol ethernet-switch-conf read-write` | Enable Ethernet Switch Configurator function with “read-write” access |

# 5.5 External Authentication

## 5.5.1 Description of the external Authentication

“External Authentication” of the device allows you to create user firewall accounts with corresponding passwords in order to authenticate a user. For each account you can select an authentication list to define three authentication methods that the device uses in sequence for access via this account name. The device allows authentication by means of its user database (local) or via a RADIUS server.

Create accounts (users) in order to use the user firewall function (see on page 149 “User Firewall”).

## 5.5.2 Application example for external Authentication

In a typical case, a service technician wants to login to the Firewall in the login window of the Web-based interface, under the “user firewall” login type. After he successfully logs in, the user firewall function (see page 149) provides him with access to the internal and external networks, for a limited time and defined by additional rules, so that he can, for example, download a software update from a server to maintain a robot.
Parameter for the application example for the user firewall function (see page 149):

| Parameter | Value |
|---|---|
| Account Name | Service |
| Authentication List | userFirewallLoginDefaultList |

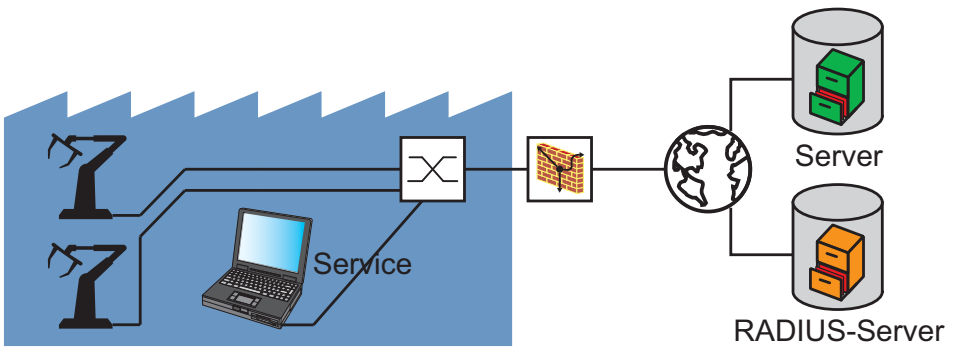



*Figure 27: Application example for external authentication*

Authentication procedure:

- The user logs in to the device in the login window of the Web-based interface, under the “user firewall” login type, with a user name and password.
- The device checks whether there is an entry under `External Authentication:User Firewall Accounts` for this user with this password.

- If there is an entry, and if this entry is active, the device uses the authentication method in accordance with the authentication list for this entry.
  If there is no entry, and if an authentication list is entered in “Authentication list for unknown users”, the device uses the authentication method in accordance with the authentication list for this entry.
  If there is no entry, and if there is no authentication list entered in “Authentication list for unknown users”, the device denies the authentication.
- If one of the authentication methods on the authentication lists leads to authentication, the user is logged in and can thus use the user firewall function.

☐ Configure the user firewall account.

☐ Select the dialog `Security:External Authentication:User Firewall Accounts`.
☐ Click on “Create Entry”.
You thus open a dialog for entering the name for this user firewall account.
☐ Enter the name for this account, e.g. `Service`.
☐ Click on „OK“.
You thus add a new entry to the table.
☐ Double-click on the cell “Password for local authentication” for this entry and enter the password.
☐ Click on the “Active” field of this entry to activate the entry.
☐ Click “Set” to temporarily save the entry in the configuration.

☐ Save the settings in the non-volatile memory.

- ☐ Select the dialog `Basic Settings:Load/Save`.
- ☐ Click on “Save to NVM + EAM” to save the configuration in the active configuration.

On delivery, the authentication lists contain the list “userFirewallDefaultList”. The example has been selected so that you can keep the parameters of this list.

# 6 Controlling the Data Traffic

This chapter describes the main task of a firewall. A firewall checks the data to be forwarded in accordance with defined rules. Data to which the rules apply is either forwarded by a firewall or blocked. Data to which no rules apply, is blocked.

The TCSEFEC provides the following functions for controlling the data traffic:

- Packet content-related data traffic control (packet filter)
- NAT - Network Address Translation
- User-related data traffic control (user firewall)
- Service request control (Denial of Service, DoS)
- VPN - Virtual Private Network

The firewall observes and monitors the data traffic. The firewall takes the results of the observation and the monitoring and combines them with the rules for the network security to create what are known as status tables. Based on these status tables, the firewall decides whether to accept, drop or reject data.

# 6.1 Packet Filter

## 6.1.1 Description of the Packet Filter Function

With the packet content-related data traffic control, the firewall checks the content of the data packets to be transmitted. Here, the firewall provides various packet groups which define the checking criteria:

- Incoming IP packets
  This group gives you the option to filter incoming IP packets at the external port based on their IP addressing information and protocol information.
- Outgoing IP packets
  This group gives you the option to filter incoming IP packets at the internal port based on their IP addressing information and protocol information.
- Incoming MAC packets
  This group gives you the option to filter incoming MAC packets at the external port based on their MAC addressing information.
  In router mode, the Firewall only transmits IP packets.
- Outgoing MAC packets
  This group gives you the option to filter incoming MAC packets at the internal port based on their MAC addressing information.
  In router mode, the Firewall only transmits IP packets.
- Incoming PPP packets
  This group gives you the option to filter incoming PPP packets at the external port based on their IP addressing information.

You can define filter rules which, when they apply, cause the firewall to either
– drop,
– reject or
– accept the packets.

| Action | Meaning |
|---|---|
| Drop | Delete data packet |
| Reject | Delete data packet and inform the sender |
| Accept | Forward data packet in accordance with the address information. |

*Table 8: Handling filtered data packets*

The Firewall checks each data packet, starting with the first rule. The first rule that applies determines how the firewall handles the data packet. The last rule “Drop everything” helps protect you from undesired data packets.

**Note:** If you insert packet filter entries that deny traffic or edit existing ones to deny traffic, note that the status tables may contain entries that nevertheless allow the traffic until they expire. If you delete a packet filter entry, the device clears the entire status table.

### Address Templates

You can use address templates to create and modify IP packet filter entries quickly and more easily.

If you use the same IP address ranges for the source or destination addresses in multiple rules, you have the option to define these addresses as an address template. An address template consists of 1 or more address entries with the same name. Optionally, you can enter an individual address with the address mask /32. You can activate or deactivate the individual addresses of the address template separately.

In your packet filter entries, use an address template in the form of a variable. You indicate a variable by putting a dollar sign (“$”) before its name. You can use variables for source and destination addresses.

The device automatically creates the suitable packet filter entries from a packet filter entry with variables. If you change the address template for a variable, the device automatically modifies the packet filter entries created.

For example, you can create an address template for the addresses in your internal network and use it as a variable in your packet filter entries. When you add an additional device to your internal network which is to have the same packet filters as the existing devices, you can update the corresponding packet filter entries by changing a single address template.

**Note:** The number of packet filter entries created through variables together with the number of other packet filter entries is limited to 1024.

In the state on delivery, no address templates are defined.

### Firewall Learning Mode (FLM)

The Firewall learn mode is an innovative set-up assistant. It helps you analyze the traffic and create suitable rules for permitting the traffic you desire.

The assistant for the Firewall learn mode allows you to

- automatically determine in an easy way the traffic which your existing rules do not permit yet (actual learn mode)
- analyze this traffic based on various criteria
- automatically create new rule defaults from the desired traffic
- modify these rules if required and automatically visualize their traffic coverage, and
- test the new rules for the desired coverage.

**Note:** However, the assistant for the Firewall learn mode still requires specialized knowledge of data networks, as the user is responsible for the rules created.

The FLM only applies to packets that want to pass through the device (the Firewall). It does not apply to packets that are sent to the device itself, and those that the device itself creates.

Perform the following steps to create the rules supported by FLM:

- ☐ Implement the Firewall at the desired position in your network.
- ☐ Activate the FLM assistant on the desired interfaces of the Firewall (typically on both interfaces).
- ☐ Start the actual learn mode.
- ☐ Operate the devices in your network for a while, so that the Firewall learns the desired traffic.

- ☐ Start the learn mode.
- ☐ Display the learned traffic on the selected interface:
  - ▶ If the Firewall has learned too little traffic, continue with the learn mode in order to learn more traffic.
  - ▶ When the Firewall has learned enough traffic, inspect the captured data.
- ☐ Select desired entries from the captured data and add them to the temporary rule set.
- ☐ If necessary, modify the added rules.
- ☐ Ignore undesired entries in the captured data, i.e. do not create any rules for them. Thus, the Firewall blocks this traffic after the learn and test mode has ended.
- ☐ Release the desired rules for testing.
- ☐ Start the test mode:
  - ▶ If the devices in your network are working as desired, write the temporary rules to your rule base.
  - ▶ If the devices in your network are not working as desired, modify the rules released for testing. Alternatively, restart the learn mode in order to learn more traffic.
- ☐ End the assistant for the Firewall learn mode.
- ☐ Save the rules in the configuration.

## 6.1.2 Application Example for Packet Filter

The figure shows a typical application case:
A production controller want to request data from a production robot. The production robot is located in a production cell which a Firewall keeps separate from the company network. The Firewall is to help prevent the data traffic between the production cell and the rest of the company network. Only the data traffic between the robot and the production controller's PC is allowed to flow freely.

The following is known:

| Parameter | Robot | Firewall | PC |
|---|---|---|---|
| IP address of internal port | | 10.0.1.201 | |
| IP address of external port | | 10.0.2.1 | |
| IP address | 10.0.1.5 | | 10.0.2.17 |
| Gateway | 10.0.1.201 | | 10.0.2.1 |

Prerequisites for further configuration:
- The Firewall is in router mode.
- The IP parameters of the Firewall router interface are configured.
- The devices in the internal network have the IP address of the internal interface (port 1) of the Firewall as their gateway.
- The gateway and the IP address of the PC and the robot are configured.

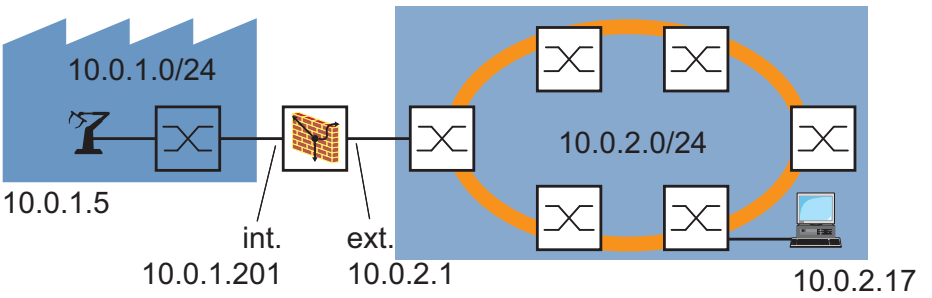



*Figure 28: Application example for packet filter*

☐ Enter the filter data for incoming IP packets.

☐ Select the dialog
`Network Security:Packet Filter:Incoming IP Packets`.
In the state on delivery, the TCSEFEC already has an invisible entry that helps prevent the data traffic from the external network to the internal network.

☐ Click on “Create Entry”.
You thus add a new entry to the table.

☐ Enter the filter data for “free access for PC”:
“Description”: `free access for PC`
“Source address (CIDR)”: `10.0.2.17/32`
“Source Port”: `any`
“Destination address (CIDR)”: `10.0.1.5/32`
“Destination port”: `any`
“Protocol”: `any`
“Action”: `accept`
“Log”: `disable`

☐ Click on the “Active” field of this entry to activate the entry.

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

The device allows you to selectively check incoming IP packets for specific ICMP traffic criteria. To activate this function for an existing or new packet filter, you proceed as follows:

☐ Select the dialog
`Network Security:Packet Filter:Incoming IP Packets`.
☐ As required, add a new entry to the table and enter the filter data as described in the previous table (see chapter “Application Example for Packet Filter”).
☐ In the “Protocol” selection field, choose the entry `icmp`.
☐ In the “Source port” input field, enter the ICMP type and code: `type 3 code 1` means:
– Destination Unreachable (ICMP type 3)
– Host Unreachable (ICMP code 1)
The values behind `type` and `code` are 1- to 3-digit decimal values. Entering an ICMP code is optional. You will find the possible values for the ICMP types and codes in the “ICMP types and codes” table in the “Web-based Interface” reference manual.
☐ Click on “Write” to temporarily save the entry in the configuration.

☐ Enter the filter data for outgoing IP packets.

☐ Select the dialog
`Network Security:Packet Filter:Outgoing IP Packets`.
In the state on delivery, the TCSEFEC already has an entry that allows the data traffic from the internal network to the external network.
☐ Select the entry.
☐ Enter the filter data for “drop everything”:
“Description”: `drop everything`
“Source address (CIDR)”: `any`
“Source port”: `any`
“Destination address (CIDR)”: `any`
“Destination port”: `any`
“Protocol”: `any`
“Action”: `drop`
“Log”: `disable`
☐ Click on the “Active” field of this entry to activate the entry.

☐ Select the entry.
Click on “↑”.
Repeat the operation until the entry represents the first row of the table.
☐ Click on “Create Entry”.
You thus add a new entry to the table.
☐ Select the entry.
☐ Enter the filter data for “free access for robot”:
“Description”: `free access for robot`
“Source address (CIDR)”: `10.0.1.5/32`
“Source Port”: `any`
“Destination address (CIDR)”: `10.0.2.17/32`
“Destination port”: `any`
“Protocol”: `any`
“Action”: `accept`
“Log”: `disable`
☐ Click on the “Active” field of this entry to activate the entry.
☐ Select the entry.
Click on “↑”.
Repeat the operation until the entry represents the first row of the table.
☐ Click “Set” to temporarily save the entry in the configuration.

☐ Save the settings in the non-volatile memory.

☐ Select the dialog
`Basic Settings:Load/Save`.
☐ Click on “Save to NVM + EAM” to save the configuration in the active configuration.

## Application Example for Address Templates

A production controller want to request data from a second production robot. As additional robots will be added, he decides to create the addresses of the robots in an address template and use the template as a variable in the existing packet filter entries.

The following is known:

| Parameter | Robot 1 | Robot 2 | Firewall | PC |
|---|---|---|---|---|
| IP address of internal port | | | 10.0.1.201 | |
| IP address of external port | | | 10.0.2.1 | |
| IP address | 10.0.1.5 | 10.0.1.6 | | 10.0.2.17 |
| Gateway | 10.0.1.201 | 10.0.1.201 | | 10.0.2.1 |

Prerequisites for further configuration:

- The previous “Application Example for Packet Filter” is already configured.

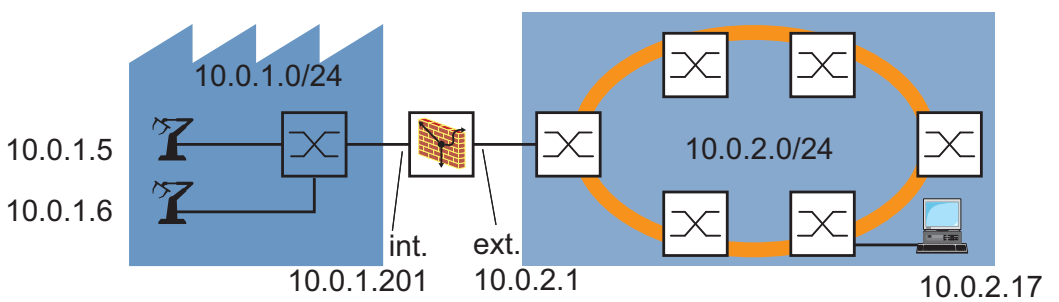



*Figure 29: Packet filter with address template; application example*

☐ Create the address template for the robots in the production cell.

☐ Select the dialog `Network Security:Packet Filters:Address Templates`.
☐ Click on “Create Entry”.
☐ Enter the first address of the address template in the dialog. Optionally, you can enter an individual address with the address mask /32:
“List Name”: `robo_cell_1`
“IP address (CIDR)”: `10.0.1.5/32`
☐ Click on “OK” to create the entry in the address template table.
☐ Click on the “Active” field of this entry to activate the entry.
☐ Click on “Create Entry” again.

☐ Enter the second address of the address template in the dialog. Use the same name again:
“List Name”: `robo_cell_1`
“IP address (CIDR)”: `10.0.1.6/32`
☐ Click on “OK” to create the entry in the address template table.
☐ Click on the “Active” field of this entry to activate the entry.
☐ Click on “Write” to temporarily save the entries in the configuration.

☐ Transfer the variables to the filter data for incoming IP packets.

☐ Select the dialog
`Network Security:Packet Filter:Incoming IP Packets`.
☐ Select the entry “free access for PC”.
☐ Replace the destination address in the entry “free access for PC” with the variable. Put a dollar sign (“$”) in front of the variable name to indicate that it is a variable:
“Description”: `free access for PC`
“Source address (CIDR)”: `10.0.2.17/32`
“Source port”: `any`
“Destination address (CIDR)”: `$robo_cell_1` (instead of `10.0.1.5/32`)
“Destination port”: `any`
“Protocol”: `any`
“Action”: `accept`
“Log”: `disable`
☐ Click “Set” to temporarily save the entry in the configuration.

☐ Transfer the variables to the filter data for outgoing IP packets.

☐ Select the dialog `Network Security:Packet Filter:Outgoing IP Packets`.
☐ Select the entry “free access for robot”.
☐ Replace the source address in the entry “free access for PC” with the variable:
“Description”: `free access for robot`
“Source address (CIDR)”: `$robo_cell_1` (instead of `10.0.1.5/32`)
“Source port”: `any`
“Destination address (CIDR)”: `10.0.2.17/32`
“Destination port”: `any`
“Protocol”: `any`
“Action”: `accept`
“Log”: `disable`
☐ Click “Set” to temporarily save the entry in the configuration.

☐ Save the settings in the non-volatile memory.

☐ Select the dialog `Basic Settings:Load/Save`.
☐ Click on “Save to NVM + EAM” to save the configuration in the active configuration.

### 6.1.3 Application Example for the Firewall Learn Mode (FLM)

The figure shows a typical application case:
A production controller sets up a new production cell. A Firewall is to separate the production cell from the company network. It is to permit only the desired traffic from the configuration computer in the company network to the devices in the production cell, and to drop the other traffic, especially the traffic from the transfer network. In the opposite direction, from the production cell to the company network, the data traffic is to flow freely.
To begin with, the user wants to access the switch in the production cell from his configuration computer in the company network and configure this switch.

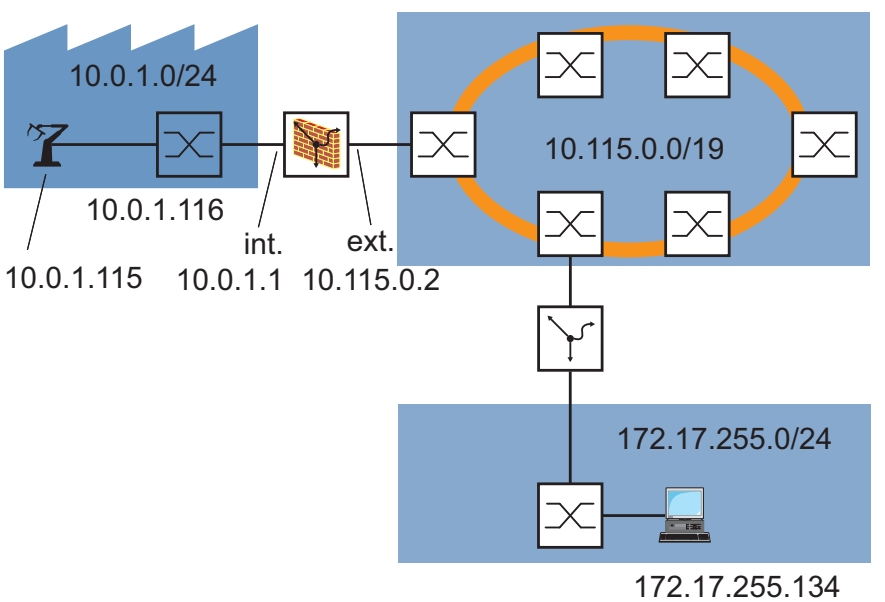



*Figure 30: Firewall Learn Mode (FLM), application example*

The following IP addresses are known:

| Parameter | Robot | Switch | Firewall | Configuration computer |
|---|---|---|---|---|
| IP address of internal port | | | 10.0.1.1 | |
| IP address of external port | | | 10.115.0.2 | |
| IP address | 10.0.1.115 | 10.0.1.116 | | 172.17.255.134 |
| Default gateway | 10.0.1.1 | 10.0.1.1 | | |

In the state on delivery,
- the Firewall permits the traffic from the internal to the external interface. The user wants to keep this configuration.
- the Firewall drops the traffic from the external to the internal interface. The user wants to change this configuration.

Prerequisites for further configuration:
- The Firewall is in router mode.
- The IP parameters of the Firewall router interface are configured.
- The packet filter rules at the external interface of the Firewall are in the state on delivery.
- The devices in the internal network have the IP address of the internal interface (port 1) of the Firewall as their gateway.
- The IP parameters of the configuration computer and the router in the company network are configured.

Special features of the learn mode:
- In the learn mode, the device only learns the traffic that is not covered by the current rules. This is the traffic for which you have configured neither specific discard rules (`drop`, `reject`) nor accept rules (`accept`).
- Thus, during the learning phase the device ignores the traffic for which you have already configured explicit drop or accept rules.
- The assistant for the firewall learn mode only creates `accept` rules. During operation, the stateful Firewall permits the traffic that it has captured with an accept rule for this communication relationship afterwards.

**Opening the assistant for the firewall learn mode:**

☐ Select the dialog `Network Security:Packet Filters:Firewall Learn Mode`.
☐ In the “Operation” frame, click “On”.
☐ To activate the assistant for the firewall learn mode, click on “Write”.
The Web-based interface informs you that the firewall learn mode has started, and it asks you whether you want to save the current configuration of the device.
☐ Click on “Yes”.
The Web-based interface asks you to enter a file name. The default file name has the format `nnnnnnnnnnnnn_beforeFLM`.
☐ Enter `Example01_before_FLM` and click on “OK”.
The device saves the current configuration in the NVM under the specified name and sets it to the status “active”.
The Web-based interface then activates the control elements for the firewall learn mode.

**The learning starts:**

☐ Select the external interface for the learning.
☐ To start the actual learning process on the Firewall, click on “Start learn mode”.
☐ On your configuration computer, load the Web-based interface of the switch in the production cell in another browser window. The Web-based interface accesses the switch via http and snmp. This data traffic is desired by you to configure the switch.
☐ Go back to the assistant for the firewall learn mode and click on “Load”.
The device refreshes its display in the “Information” frame and displays the number of learned IP connections.
☐ To stop the learn mode, click on “Stop learn mode”.
The Web-based interface activates the “External interface” tab page.

**Inspect traffic data and use the assistant to derive rules for desired traffic:**

- ☐ Select the “External interface” tab page.
- ☐ In the “Captured Data” frame, sort the table in ascending order based on the “Source IP” column.
- ☐ Search for the first row with the IP address of the configuration computer.
- ☐ From this row onwards, search for the http traffic data between the configuration computer and the switch (tcp port 80). This is the first row with:
  - the destination address of the switch,
  - destination port 80 and
  - the `tcp` protocol.
- ☐ Select this row.
- ☐ Click on “Add to Rule Set”.

The device transfers the learned data of the selected row into a new rule.

In the “Captured Data” frame, the Web-based interface displays the row that the new rule covers in dark green.

- ☐ To permit the random source ports of the http requests, change the source port of the rule to `any`.

In the “Captured Data” frame, the Web-based interface now displays the rows that the new rule covers in dark green.

- ☐ In the “Captured Data” frame, search again for the first row with the IP address of the configuration computer.
- ☐ From this row onwards, search for the snmp traffic data between the configuration computer and the switch (udp port 161). This is the first row with:
  - the destination address of the switch,
  - destination port 161 and
  - the `udp` protocol.
- ☐ Select this row.
- ☐ Click on “Add to Rule Set”.

The device transfers the learned data of the selected row into a new rule.

The Web-based interface displays the row that the new rule covers in dark green.
The Web-based interface displays the rows covered by the rule previously created in light green.

☐ To permit the random source ports of the snmp requests, change the source port of the rule to `any`.

In the “Captured Data” frame, the Web-based interface now displays the rows that the new rule covers in dark green.

From the desired traffic you have now created new rules, which the Firewall will use to permit this traffic after you have closed the assistant for the firewall learn mode.

The Firewall shall drop the other learned traffic during operation. Therefore you ignore this traffic when creating the rules.
In the “Captured Data” frame, the Web-based interface displays these rows unmarked (with a white background).

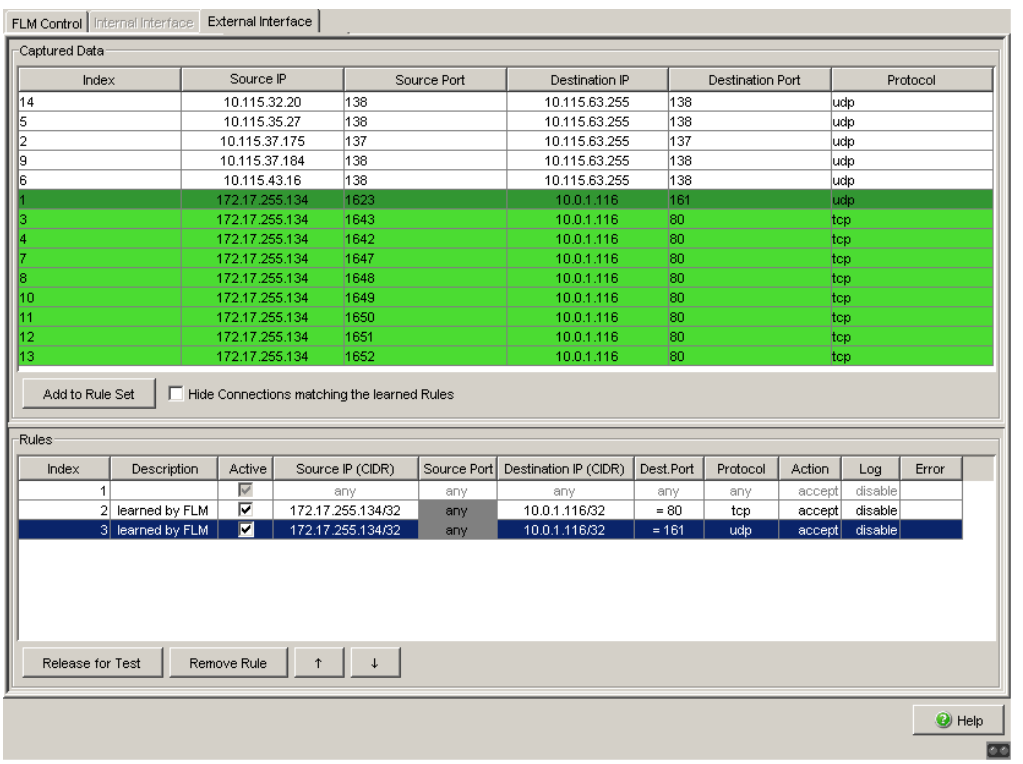



*Figure 31: Firewall Learn Mode dialog, “External interface” tab page*

**Testing the newly created packet filter rules:**

☐ Click on “Release for Test”.
☐ Select the “FLM Control” tab page.
☐ Click on “Start test mode”.

The Web-based interface sets the number of “IP entries” learned in the test mode up to now to 0.

☐ On your configuration computer, once again load the Web-based interface of the switch in the production cell in another browser window. To test the new packet filter rules, access dialog pages and HTML pages again. You thus create the desired snmp and http traffic.
☐ Go back again to the assistant for the firewall learn mode.
☐ Click on “Stop test mode”.

The Web-based interface refreshes its display and displays the number of new IP entries that the device has learned in the test mode.

☐ Select the “External interface” tab page.

During the learning, the device has now ignored the http and snmp traffic that you previously permitted.
If you discover in the learned data additional traffic that you want you permit, you have the option to derive additional rules from this traffic. Afterwards, repeat the test.

**Closing the assistant for the firewall learn mode and saving the new packet filter rules:**

☐ Select the “FLM Control” tab page.
☐ In the “Operation” frame, click “Off”.
☐ To close the assistant for the firewall learn mode, click on “Write”.
The Web-based interface informs you that you are leaving the firewall learn mode, and it asks you whether you want to save the current configuration of the device or restore the previous configuration.
☐ Click on “Write”.
The Web-based interface asks you to enter a file name. The default file name has the format `nnnnnnnnnnnn_afterFLM`.
☐ Enter `Example01_after_FLM` and click on “OK”.
The device saves the current configuration with the new packet filter rules in the NVM under the specified name and sets it to the status “active”.
The Web-based interface then deactivates the control elements for the firewall learn mode and the “External interface” tab page.

**Additional options:**

If you are adding new devices to the production cell, or also want to manage the devices in the production cell from other configuration computers, you have the option:

- to execute the assistant for the firewall learn mode again and create additional rules for new desired traffic, e.g. for controlling a robot.
- to change existing rules manually in the Incoming IP Packets dialog, e.g.
  – To permit the entire production cell as a destination for desired http and snmp data traffic, change the entries for “Destination address (CIDR)” to `10.0.1.0/24`.
  – To permit the production cell as a destination for desired http and snmp data traffic, change the entries for “Destination address (CIDR)” to `172.17.255.0/24`.

- To quickly hide the Web servers of the devices in the production cell, change the action to `drop` for the entry with destination port 80 and protocol `tcp`. The Firewall still allows the management of the devices via snmp.
- To access a robot for test purposes using a currently unknown, proprietary, TCP-based protocol, temporarily change the entry for “Destination port” from 80 to `any` and set the action to `accept`.

You also have the option to manually add new rules in the `Incoming IP packets` dialog:

- for desired traffic, e.g. for controlling a robot that uses a proprietary protocol with the Layer 4 protocol No. 141:
  - Description: `Robot, IP/141`
  - active: `on`
  - Source address: `172.17.255.0/24`
  - Source port: `any`
  - Destination address (CIDR): `10.0.1.5/32`
  - Destination port: `any`
  - Protocol: `141`
  - Action: `accept`
- if applicable, also for undesired traffic, e.g. to explicitly ignore NetBIOS traffic to the network Broadcast address of the company network during the learning:
  - Description: `Drop NetBIOS Broadcasts`
  - active: `on`
  - Source address: `10.115.0.0/19`
  - Source port: `any`
  - Destination address (CIDR): `any`
  - Destination port: `136><140`
  - Protocol: `any`
  - Action: `drop`

  **Note:** When you are learning traffic at an interface for which you have configured an active `drop` rule, the firewall ignores the traffic to which the rule applies during the learning.
  To learn and inspect this traffic, deactivate the `drop` rule before the learning.

# 6.2 NAT – Network Address Translation

The Network Address Translation (NAT) protocol describes a procedure for automatically and transparently changing IP address information in data packets while still transmitting the data packets to their precise destination. NAT is used when you do not want IP addresses of an internal network to be visible from outside. The reasons for this can include, for example:

- Keeping the structure of the internal network hidden from the outside world.
- Keeping private IP addresses hidden (see on page 38 “Private IP addresses”).
- Using IP addresses multiple times - for example, by forming identical production cells.

Depending on your reason for using NAT, it offers you various procedures for using the IP address information.

| Properties | IP Masquerading | 1:1 NAT | Port Forwarding |
|---|---|---|---|
| Initialization of a connection from within | Yes | Yes | No |
| Initialization of a connection from outside | No | Yes | Yes |

*Table 9: Comparison of the individual NAT procedures*

## 6.2.1 IP Masquerading

You use IP Masquerading to hide the internal network structure from outside, concealing it behind a mask, so to speak.

With IP Masquerading, the Firewall replaces the source IP address of a data packet from the internal network with the external IP address of the Firewall. To identify the different internal IP addresses, NAT adds the logical port number of the connection to the address information. Adding the port information also gave the IP Masquerading the name “Network Address Port Translation” (NAPT).

By converting the IP addresses using port information, devices can set up communication connections to the outside from the internal network. However, as devices in the external network only know the external IP address of the Firewall, they are unable to set up a communication connection to a device in the internal network.

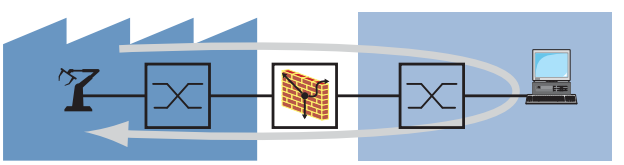


*Figure 32: Setting up a communication connection with IP Masquerading*

### 6.2.2 1:1 NAT

You use 1:1 NAT when you are setting up identical production cells with the same IP addresses and want to connect them with the external network. The Firewall then allocates to the devices in the internal network a different IP address in the external network.

With 1:1 NAT, the Firewall replaces the source IP address of a data packet from the internal network with an IP address of the external network.

Through the 1:1 conversion of the IP addresses, devices can set up communication connections to the outside from the internal network, and devices in the external network can set up communication connections to a device in the internal network.
This is why 1:1 NAT is also called bi-directional NAT.

You have the option to combine 1:1 NAT with the router redundancy. In the process, 2 physical devices form a virtual, high-availability 1:1 NAT router (see on page 191 “Router Redundancy”).

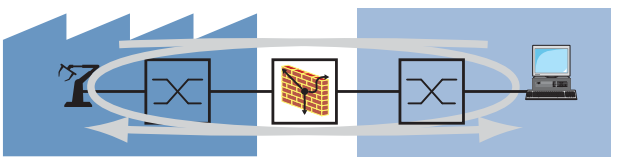


*Figure 33: Setting up a communication connection with 1:1 NAT*

**Note:** 1:1 NAT only changes IP addresses in the IP header of the packets. For FTP, the device provides an Application Layer Gateway.

**Note:** With 1:1 NAT the Firewall responds to ARP requests from the external network to addresses which it maps from the internal network. This is also the case when no device with the IP address exists in the internal network. Therefore, in the external network, only allocate to devices IP addresses located outside the area which 1:1 NAT maps from the internal network to the external network.

### Inverse 1:1 NAT

You use inverse 1:1 NAT if you want the devices in the internal network to communicate with the devices in the external network as if the devices in the external network were in the internal network. The Firewall then allocates to the devices in the external network a different IP address in the internal network.

With inverse 1:1 NAT, the Firewall replaces the destination IP address of a data packet from the internal network with an IP address of the external network.

To do this, you create an inverse 1:1 NAT entry for the devices in the external network.

**Note:** With inverse 1:1 NAT the Firewall responds to ARP requests from the internal network to addresses which it maps from the external network. This is also the case when no device with the IP address exists in the external network. Therefore, in the internal network, only allocate to devices IP addresses located outside the area which the inverse 1:1 NAT entry maps from the external network to the internal network.

### Double NAT

You use Double NAT, also known as Twice NAT, if you want the devices in the internal network to communicate with the devices in the external network as if the devices in the external network were in the internal network, and vice versa.

In the process, the Firewall allocates

- to the devices in the internal network a different IP address in the external network (1:1 NAT function) and
- to the devices in the external network a different IP address in the internal network (inverse 1:1 NAT function).

With double NAT, for a data packet from the internal network, the Firewall replaces

- the source IP address with an IP address from the external network and
- the destination IP address with an IP address from the external network.

To do this, you create a 1:1 NAT entry for the devices in the internal network, and also an inverse 1:1 NAT entry for the devices in the external network.

### 6.2.3 Port Forwarding

You use port forwarding when you want to hide the internal network structure from the outside, but want to allow a communication connection to be set up from the outside in.

With port forwarding, one or more external devices sets up a communication connection to the internal network. In doing so, an external device addresses data packets to a specific port with the external IP address of the Firewall. Data packets with a permitted source IP address that the Firewall receives at this port are forwarded by the firewall to the port of the internal device entered in the NAT table. Hence the name Port Forwarding. As a dedicated destination is addressed in this case, this procedure is also known as Destination NAT.

By converting the IP addresses and the port information using the incoming port addressing, devices can set up network communication connections to the inside from the external network.

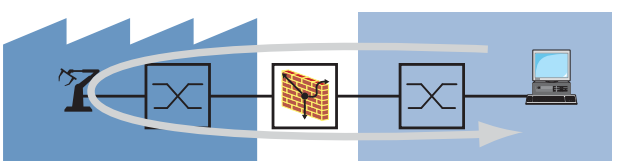


*Figure 34: Setting up a communication connection with Port Forwarding*

A typical application in the industrial sector is port 5631 for the remote maintenance of a PC in a production cell.

## 6.2.4 NAT Application Examples

### Connecting a production cell with the company network via 1:1 NAT

You have multiple identical production cells and want to connect them with your company network. As even the IP addresses used in the production cells are identical, you convert the IP addresses using the 1:1 NAT function.
The following is known:

| Parameter | Firewall Number 1 | Firewall Number 2 |
|---|---|---|
| Internal Network | 10.0.1.192/28 | 10.0.1.192/28 |
| External Network | 10.0.2.192/28 | 10.0.2.208/28 |

Prerequisites for further configuration:

- The Firewall is in router mode.
- The IP parameters of the router interface are configured.
- The gateway and the IP address of the devices in production cells are configured.
- The devices in the production cells have the IP address of the internal interface (port 1) of the Firewall as their gateway.

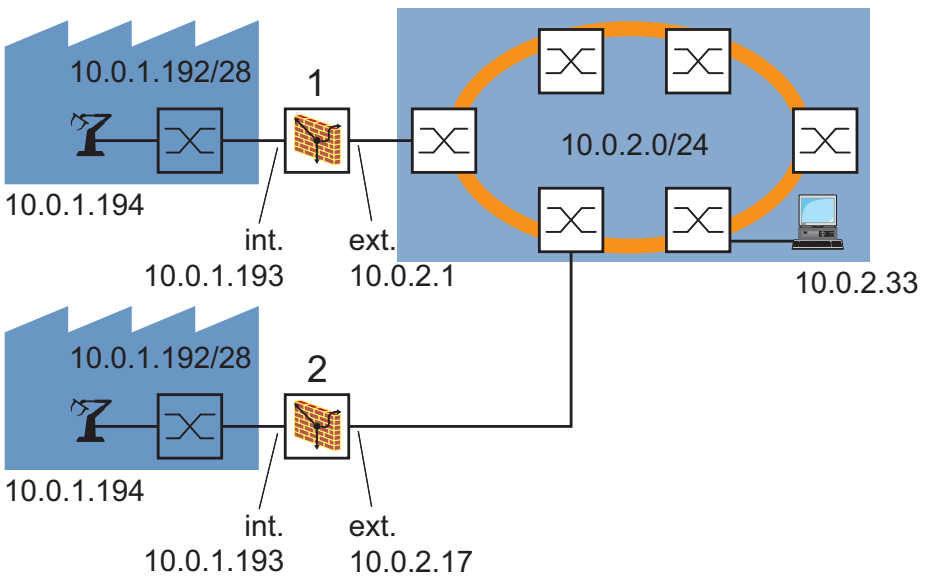



*Figure 35: Connecting one of multiple identical production cells with the company network via 1:1 NAT*

☐ First you configure firewall number 1.
Enter the parameters for converting the IP addresses.

☐ Select the dialog
`Network Security:NAT:1:1 NAT`.
☐ Click on “Create Entry”.
You thus add a new entry to the table.
☐ Enter the parameters for converting the IP addresses:
“Description”: `Production hall 1`
“Internal network”: `10.0.1.193`
“External network”: `10.0.2.1`
“Netmask”: `28`
☐ Click on the “Active” field of this entry to activate the entry.
☐ Click “Set” to temporarily save the entry in the configuration.

☐ Save the settings in the non-volatile memory.

☐ Select the dialog
`Basic Settings:Load/Save`.
☐ Click on “Save to NVM + EAM” to save the configuration in the active configuration.

☐ Configure firewall number 2 in the same way.
Use the values for firewall number 2 from the table on the previous page.

## Connecting 2 Devices via Double NAT

For test purposes, you want to connect a work station in your company network with a robot in a production cell. As the test set-up requires the two devices to be logically located in the same network, you convert the IP addresses using the double NAT function.

The following is known:

| Parameter | Robot | Work station |
|---|---|---|
| IP address in the production network (internal) | 10.0.1.194 | 10.0.1.195[a] |
| IP address in the company network (external) | 10.0.2.194[a] | 10.0.2.195 |

*Table 10: the IP addresses of the test devices*
*a: This IP address is created using NAT*

Prerequisites for further configuration:

- The Firewall is in router mode.
- The IP parameters of the router interface are configured.
- The IP addresses of the devices are configured.

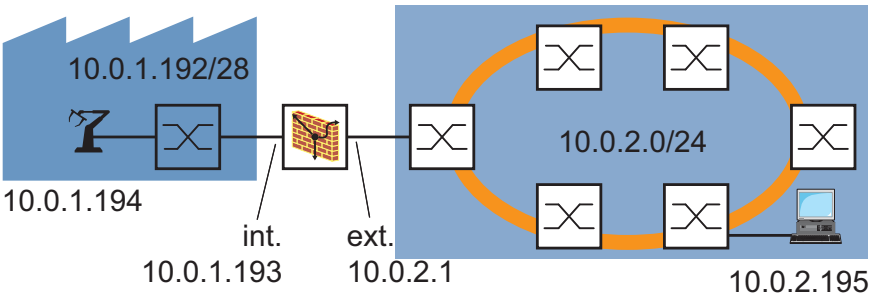



*Figure 36: Connecting 2 Devices via Double NAT*

☐ Enter the parameters for converting the IP addresses.

☐ Select the dialog `Network Security:NAT:1:1 NAT`.
☐ Click on “Create Entry”.
You thus add a new entry to the table.
☐ Enter the parameters for converting the IP address of the robot:
“Description”: `Robot production hall (test)`
“Internal network”: `10.0.1.194`
“External network”: `10.0.2.194`
“Netmask”: `32`
☐ Click on the “Output” (double NAT) field of this entry to activate double NAT for the entry.
☐ Click on the “Active” field of this entry to activate the entry.
☐ Click on “Create Entry”.
You thus add a new entry to the table.
☐ Enter the parameters for converting the IP address of the work station:
“Description”: `Work station company network (test)`
“Internal network”: `10.0.1.195`
“External network”: `10.0.2.195`
“Netmask”: `32`
☐ Click on the “Output” (double NAT) field of this entry to activate double NAT for the entry.
☐ Click on the “Inverted” field of this entry to select the entry as an inverted 1:1 NAT entry.
☐ Click on the “Active” field of this entry to activate the entry.
☐ Click on “Write” to temporarily save the entries in the configuration.

☐ Save the settings in the non-volatile memory.

☐ Select the dialog `Basic Settings:Load/Save`.
☐ Click on “Save to NVM + EAM” to save the configuration in the active configuration.

## Managing a switch in a production cell from a PC outside the production cell (Port Forwarding)

You have used a Firewall to connect with your company network a production cell with its own IP addresses which should not be visible in the company network. You configure the port forwarding function so that an administrator in the company network can manage a switch within the production cell.
The following is known:

| Parameter | Switch | Firewall | PC |
|---|---|---|---|
| IP address of internal port | | 10.0.1.201 | |
| IP address of external port | | 10.0.2.1 | |
| IP address | 10.0.1.193 | | 10.0.2.17 |
| Gateway | 10.0.1.201 | | 10.0.2.1 |

Prerequisites for further configuration:

- The Firewall is in router mode.
- The IP parameters of the router interface are configured.
- The gateway and the IP address of the devices in production cells are configured.
- The devices in the production cells have the IP address of the internal interface (port 1) of the Firewall as their gateway.

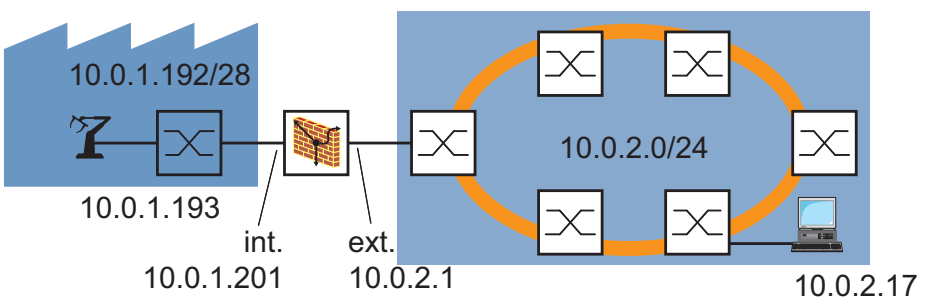



*Figure 37: Managing a switch within the production cell from outside*

☐ Configure the firewall.
Enter the parameters for converting the IP addresses.

☐ Select the dialog
`Network Security:NAT:Port Forwarding`.
☐ Click on “Create Entry”.
You thus add a new entry to the table.
☐ Enter the parameters for the http transmission:
“Source Address (CIDR)”: `10.0.1.17/24`
“Source Port”: `any`
“Incoming Address”: `10.0.2.1`
“Incoming Port”: `8080`
You can freely allocate port numbers higher than 1024.
“Forwarding address”: `10.0.1.193`
“Forwarding port”: `http`, Web server of the switch.
“Protocol”: `tcp`.
☐ Click on the “Active” field of this entry to activate the entry.
☐ Click on “Create Entry”.
You thus add a new entry to the table.
☐ Enter the parameters for the SNMP transmission:
“Source Address (CIDR)”: `10.0.1.17/24`
“Source Port”: `any`
“Incoming Address”: `10.0.2.1`
“Incoming Port”: `8081`
You can freely allocate port numbers higher than 1024.
“Forwarding address”: `10.0.1.193`
“Forwarding port”: `snmp`, for the communication of the applet with the website of the switch.
“Protocol”: `udp`.
☐ Click on the “Active” field of this entry to activate the entry.
☐ Click on “Write” to temporarily save the entries in the configuration.

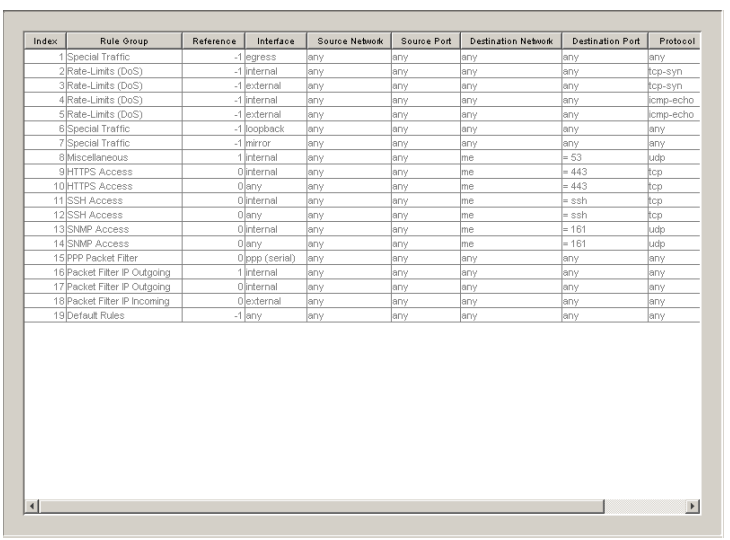
☐ Save the settings in the non-volatile memory.

☐ Select the dialog
`Basic Settings:Load/Save`.
☐ Click on “Save to NVM + EAM” to save the configuration in the active configuration.

# 6.3 User Firewall

## 6.3.1 Description of the User Firewall Function

With the user-related data traffic control, the firewall checks the data of a user previously defined by you (see on page 112 “Description of the external Authentication”). The firewall allows you to define multiple users. For every user defined, you can create different rules, on the basis of which the firewall handles data packets for the user defined.
After a user has registered for the user firewall on the firewall's website (see fig. 7), the firewall checks the data packets for this user on the basis of these rules defined for him.
If none of these rules apply, the firewall checks these data packets on the basis of the general packet filters (see on page 118 “Packet Filter”).



| Index | Rule Group | Reference | Interface | Source Network | Source Port | Destination Network | Destination Port | Protocol |
|---|---|---|---|---|---|---|---|---|
| 1 | Special Traffic | -1 | egress | any | any | any | any | any |
| 2 | Rate-Limits (DoS) | -1 | internal | any | any | any | any | tcp-syn |
| 3 | Rate-Limits (DoS) | -1 | external | any | any | any | any | tcp-syn |
| 4 | Rate-Limits (DoS) | -1 | internal | any | any | any | any | icmp-echo |
| 5 | Rate-Limits (DoS) | -1 | external | any | any | any | any | icmp-echo |
| 6 | Special Traffic | -1 | loopback | any | any | any | any | any |
| 7 | Special Traffic | -1 | mirror | any | any | any | any | any |
| 8 | Miscellaneous | 1 | internal | any | any | me | = 53 | udp |
| 9 | HTTPS Access | 0 | internal | any | any | me | = 443 | tcp |
| 10 | HTTPS Access | 0 | any | any | any | me | = 443 | tcp |
| 11 | SSH Access | 0 | internal | any | any | me | = ssh | tcp |
| 12 | SSH Access | 0 | any | any | any | me | = ssh | tcp |
| 13 | SNMP Access | 0 | internal | any | any | me | = 161 | udp |
| 14 | SNMP Access | 0 | any | any | any | me | = 161 | udp |
| 15 | PPP Packet Filter | 0 | ppp (serial) | any | any | any | any | any |
| 16 | Packet Filter IP Outgoing | 1 | internal | any | any | any | any | any |
| 17 | Packet Filter IP Outgoing | 0 | internal | any | any | any | any | any |
| 18 | Packet Filter IP Incoming | 0 | external | any | any | any | any | any |
| 19 | Default Rules | -1 | any | any | any | any | any | any |

*Figure 38: IP firewall list*

You use the user firewall function if you want to provide certain users with access to the internal or external network for a limited period of time, whereby this access is extended on the basis of rules.

### 6.3.2 Application example for the User Firewall Function

The figure shows a typical application case:
A service technician wants to download a software update from a server for the maintenance of a robot.
The following is known:

| Parameter | Firewall | Service PC | Server |
|---|---|---|---|
| IP address of internal port | 10.0.1.201 | | |
| External port | PPPoE | | |
| IP address | | 10.0.1.51 | 10.149.1.51 |
| Gateway | | 10.0.1.201 | |

Prerequisites for further configuration:
- The Firewall is in router mode.
- The IP parameters of the Firewall router interface are configured.
- The devices in the internal network have the IP address of the internal interface (port 1) of the Firewall as their gateway.
- The gateway and the IP address of the PC are configured.
- The packet filters are configured according to the example (see on page 122 “Application Example for Packet Filter”).
- The external authentication for the “service” is configured (see on page 112 “Description of the external Authentication”).

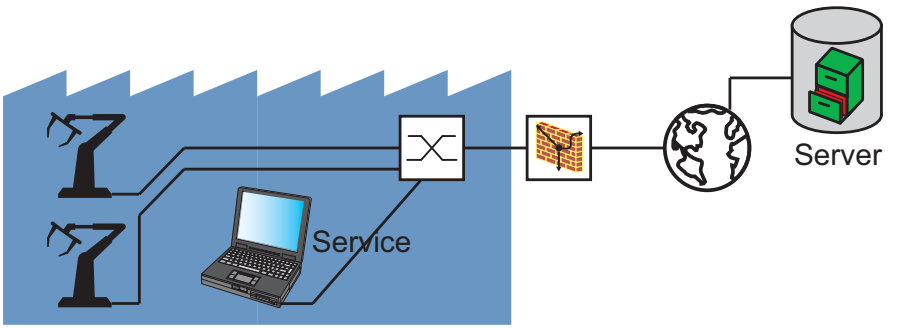



*Figure 39: User firewall application example*

☐ Create a user firewall entry.

☐ Select the dialog `Network Security:User Firewall Entries`.
☐ Click on “Create Entry”.
You thus add a new entry to the table.
☐ Select the entry.
Click on “Edit”.
☐ Select the tab page `Basic Settings`.
☐ Enter the data:
- “Name”, `Service User`
  This is the name for this user firewall entry.
- “Timeout”, `7200`
  Maximal duration of access in seconds.
- “Timeout Type”, `static`
  The countdown of the timeout begins when the user logs on.
- “Source Address”, `10.0.1.51`
  This is the IP address of the service PC.
- “Description”, `Open the access to the production cell for the service operation.`

☐ Select the `Accounts` tab page.
☐ Click on “Create Entry”.
A dialog gives you the option to select an existing account, e.g. `Service`(see on page 112 “Description of the external Authentication”).
Select an account.
Click on „OK“.

☐ Select the `Rules` tab page.
☐ Click on “Create Entry”.
You thus add a new entry to the table.
☐ Select the entry.
Click on “Edit”.
☐ Enter the data:
- “Source port”, `any`
Since the port through which the browser of the notebook is normally not a fixed port, the setting `any` is required.
- “Destination network”, `10.149.1.51/32`
IP address of the server on which the software for the robot is located.
- “Destination port”, `http`
With the `http` setting, the service technician downloads the software via his browser.
- “Description”, `Software Download`
Meaningful description of the rule.
- “Protocol”, `tcp`.
- “Log”, if you want to log the accesses, you select this function.

☐ Click “Set” to temporarily save the entry in the configuration.
☐ Click on “Back”.
This returns you to the `Rules` tab page.
☐ Click on the “Active” field of this entry to activate the entry.
☐ Click on “Back”.
This returns you to the table view.
☐ Click on the “Active” field of this entry to activate the entry.
☐ Click “Set” to temporarily save the entry in the configuration.

☐ Save the settings in the non-volatile memory.

☐ Select the dialog
`Basic Settings:Load/Save`.
☐ Click on “Save to NVM + EAM” to save the configuration in the active configuration.

# 6.4 Helping protect against Denial of Service (DoS)

This function assists you with the protection of your network and your server from unauthorized access via excessive flooding with TCP connections, ping packets or ARP packets. The default values support these protective measures during typical data traffic, without hindering the data traffic.

Furthermore, the device offers the possibility to create a log entry when a limit is exceeded. You can set this for each limit separately.

# 6.5 VPN – Virtual Private Network

A virtual private network (VPN) refers to the part of a public network that someone uses for their private purposes.
The special feature of a VPN, as the name “private” suggests, is that it is closed off from the public network. Different measures help protect the data of the virtual private network from spying, data falsification and other attacks from external subscribers.
In the industrial environment, for example, a VPN serves to connect two plant sections with each other via the public Internet.

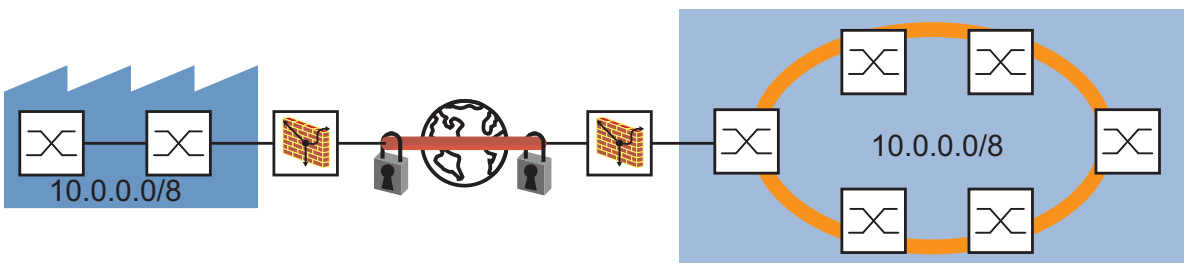



*Figure 40: VPN for connecting two plant sections*

### 6.5.1 IPsec – Internet Protocol Security

IPsec (Internet Protocol Security) is the most commonly used VPN protocol. IPsec regulates the setting up of a VPN connection and the measures for secure data transmission in the virtual private network.
Secure data transmission in a VPN involves:

- Integrity protection
  Integrity protection helps ensure that the data transmitted is genuine, i.e. that it comes from a trustworthy sender (is authentic) and that the recipient receives the data in an unfalsified form.
- Encryption
  Encryption helps ensure that nobody without authorization can view the data.
  Encryption procedures code the data to be transmitted using a code (key) that is exclusively available to the authorized communication subscribers.
- Traffic flow confidentiality
  The traffic flow confidentiality helps ensure that no unauthorized person can gain knowledge of the actual recipient and sender of a data packet. IPsec performs this in the tunnel mode by encrypting the complete IP packet.

For the mediation of the security parameters to be used between the two endpoints of a VPN connection, IPsec provides two modes (transport mode and tunnel mode):

- Transport mode:
  In the transport mode, two terminal devices authenticate themselves to each other, then they set up the parameters required for the signing and the encryption. As the communication taking place between two defined terminal devices, the recipient and sender addresses remain visible.
- Tunnel mode:
  In the tunnel mode, two routers/gateways authenticate themselves to each other, then they set up the parameters required for the signing and the encryption.
  With the two routers/gateways, the VPN connection has two addressable endpoints, but the communication takes place between the subscribers of the network connected to the routers/gateways. This enables the encryption of the communication data to be transmitted, including the recipient and sender addresses. The addresses of the routers/gateways are used to address the endpoints of the VPN connection.
  The tunnel mode can also be used for the VPN connection between a terminal device and a router/gateway. Thus the address data within the network connected to the router/gateway remains hidden.

## 6.5.2 IKE – Internet Key Exchange

IPsec uses the Internet Key Exchange protocol for authentication, for exchanging keys and for agreeing on further parameters for the security arrangement of a VPN connection.

### Authentication

Use authentication as part of the security arrangement. During authentication, the connection partners show each other their ID cards, so to speak.

This ID card can consist of

- what is known as a pre-shared key, which is a character string previously exchanged via a different communication channel.
- a digital certificate, which was issued by a certification authority (CA). Certificates based on the X.509 standard contain, for example
  - information on the certification authority itself,
  - validity period of the certificate,
  - information on the permitted usage,
  - the identity of the person to whom the certificate is assigned (X.500 DN),
  - the public key belonging to this identity,
  - the digital signature for verifying the connection between this identity and this related public key.

  Larger companies and authorities usually have their own certification authority. You can also obtain certificates from the Schneider Electric SA company.

  A commonly used file name extension for a certificate based on the PKCS#12 standard is “.p12”.

  You can also find the information contained in a PKCS#12 file separately in individual files with the file name extension “.pem”.

### Encryption

To help protect the data, IKE uses various cryptographic algorithms to encrypt the data. The endpoints of the VPN connection require the key to code and decode the data.

In a first step to set up the IKE security arrangement between the endpoints of the VPN connection

- they agree on a cryptographic algorithm which will subsequently use the key for coding and decoding the IKE protocol messages
- they specify the time periods during which the key exchange takes place and
- they communicate the endpoints at which the coding and decoding takes place. The administrator defines the endpoints beforehand in the settings of the endpoints of the VPN connection.

In the second step, the endpoints of the VPN connection agree on the key to code and decode the data.

## 6.5.3 Application Examples

The following examples consider the special features of frequently occurring application cases.

### Connecting two subnetworks

In a large company network, the subnetworks are connected to each other via a transfer network. Two of these subnetworks, e.g. the production control and the production hall, are to be connected via a VPN. As the internal IP addresses are to remain hidden, the VPN is to be operated in tunnel mode.
The following is known:

| Parameter | Firewall Number 1 | Firewall Number 2 |
|---|---|---|
| IP address of internal port | 10.0.1.201 | 10.0.3.201 |
| IP address of external port | 10.0.2.1 | 10.0.2.2 |
| Pre-shared key | 123456abcdef | 123456abcdef |
| Start IKE mode as | Initiator | Responder |
| IP parameters of the networks to be connected | 10.0.1.0/24 | 10.0.3.0/24 |

Prerequisites for further configuration:

- Both Firewalls are in router mode.
- The IP parameters of the Firewall router interface are configured.
- The devices in the internal network have the IP address of the internal interface (port 1) of the Firewall as their gateway.

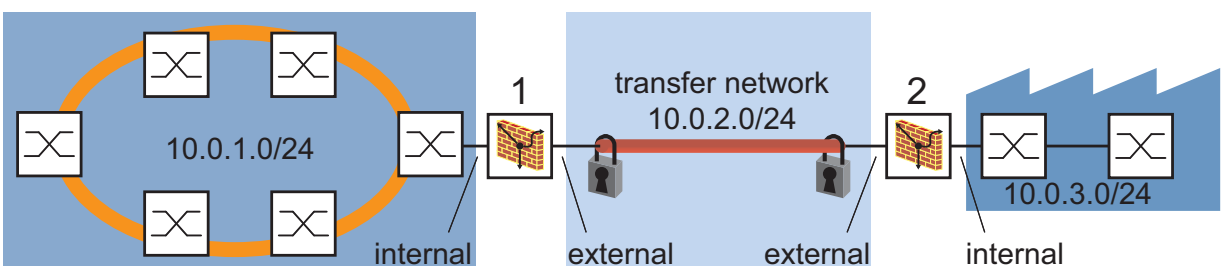



*Figure 41: Connecting two subnetworks via a transfer network*

☐ Create a new VPN connection.

☐ Select the dialog `Virtual Private Network:Connections`.
☐ Click on “Create Entry”.
In the `Basic Settings` tab page, the dialog for editing the entries gives you the option to give this connection any name you want.
☐ Give the connection a name, e.g.
“Production Control - Production Hall 1”.

The Firewall allows you to activate/deactivate a connection remotely. In the command for activating/deactivating remotely, you enter the name of the connection as a parameter. The command is:

```
https://vpn-user:passwort@host/nph-
vpn.cgi?name=verbindung&cmd=(up|down)
```

Example:

```
https://vpn:helen25miller@10.0.2.1/nph-
vpn.cgi?name=Fertigungssteuerung-Produktionshalle&cmd=up
```

Depending on your browser, you can alternatively select the syntax without `vpn-user:passwort@` and enter the VPN user with the password in the dialog.
☐ Enter the authentication parameters.

☐ Select the `Authentication` tab page.
☐ In the `Key Information` frame, you enter:
- “Method” `psk`
- “Pre-shared key”, e.g. `123456abcdef`

☐ In the `Identities` frame, you enter:
- “Local type” `ipaddr`
  With this, you specify that the entry in “Local ID” is an IP address.
- “Local ID”, e.g. `10.0.2.1`
  Value for identification (within the authentication) on the opposite side
- “Remote type” `ipaddr`
  With this, you specify that the remote IP address is part of the identification.
- “Remote ID”, e.g. `10.0.2.2`

☐ Enter the IKE key exchange parameters.

☐ Select the `IKE - Key Exchange` tab page.
☐ In the `Mode` frame, you enter:
- "Protocol" `auto`
  With this, the Firewall selects the protocol version automatically, depending on the VPN remote terminal.
- "Startup as", `initiator`
  With this, this Firewall initiates the VPN connection to the remote terminal.
- "DPD Timeout", `120`
  With this, the Firewall terminates the VPN connection if it does not receive a sign of life from the remote terminal within 120 seconds.
- "Lifetime" `28800`
  After this lifetime has elapsed, the two participating Firewalls agree on new keys for the IKE security arrangement (IKE SA). The lifetime is there to effect a periodic key change for the IKE SA.
- "Compatibility Mode", `Off`

☐ In the `Algorithms` frame, enter the encryption procedures you wish to use for the various applications:
- "Key Agreement" `modp1024`
- "Hash", e.g. `md5`
- "Integrity" `hmacsha1`
- "Encryption" `aes128`

☐ In the `Peers (Endpoints)` frame, you enter:
- "Local IP Address" `10.0.2.1`
- "Remote IP Address" `10.0.2.2`

In the current example, the external ports of the two Firewalls are the endpoints of the VPN connection.

☐ Enter the IPsec data exchange parameters.

☐ Select the `IPsec - Data Exchange` tab page.
☐ In the `Mode` frame, you enter:
- "Encapsulation" `tunnel`
  With this, the Firewall encrypts the entire data packet, including the IP addresses of the communication partners.
- "Force NAT-T" `No`.
- "Lifetime" `3600`.

☐ In the `Algorithms` frame, you enter:
- "Key Agreement" `modp1024`
- "Integrity" `hmacsha1`
- "Encryption" `aes128`

☐ Enter the parameters for the IP networks whose data is to be transmitted via the VPN connection.

- ☐ Select the `IP Networks` tab page.
- ☐ Click on `Create entry`.
- ☐ After you double-click on a cell of the entry, you can edit the cell:
  - "Source address" `10.0.1.0/24`
  - "Source port" `any`
  - "Destination address" `10.0.3.0/24`
  - "Destination port" `any`
  - "Protocol" `any`
  - "Description" `Free data traffic between the two networks Production Control and Production Hall`
  - "Active" `On`
- ☐ Click "Set" to temporarily save the entry in the configuration.

☐ Activate the connection.

- ☐ Click on "Back" to return to the connection overview.
- ☐ Select `Active` in the entry for the connection to activate the connection.
- ☐ Click "Set" to temporarily save the entry in the configuration.

☐ Save the settings in the non-volatile memory.

- ☐ Select the dialog `Basic Settings:Load/Save`.
- ☐ Click on "Save to NVM + EAM" to save the configuration in the active configuration.

☐ Make exactly the same settings on both Firewalls. For the second Firewall, in the settings for the authentication, the IKE key exchange and the IP networks, you merely swap the IP addresses for the endpoints or networks.

## Connecting multiple subnetworks via a public network (hub and spoke architecture)

A newly formed department in the 2nd production hall carries out maintenance work not only locally, but also for the 1st production hall. The devices also access the 1st production network via the existing VPN connection. To implement this, the administrator selects the “Hub and Spoke” architecture, since this is easy to set up and does not require any additional hardware.

The Firewall 1 in the production control thereby assumes the function of the central node (“Hub”). The VPN connections perform the function of the spokes.

If the Firewall is working as a hub, it sends out the routed packets at the same interface at which it received them. This is also called “hub and spoke routing”.

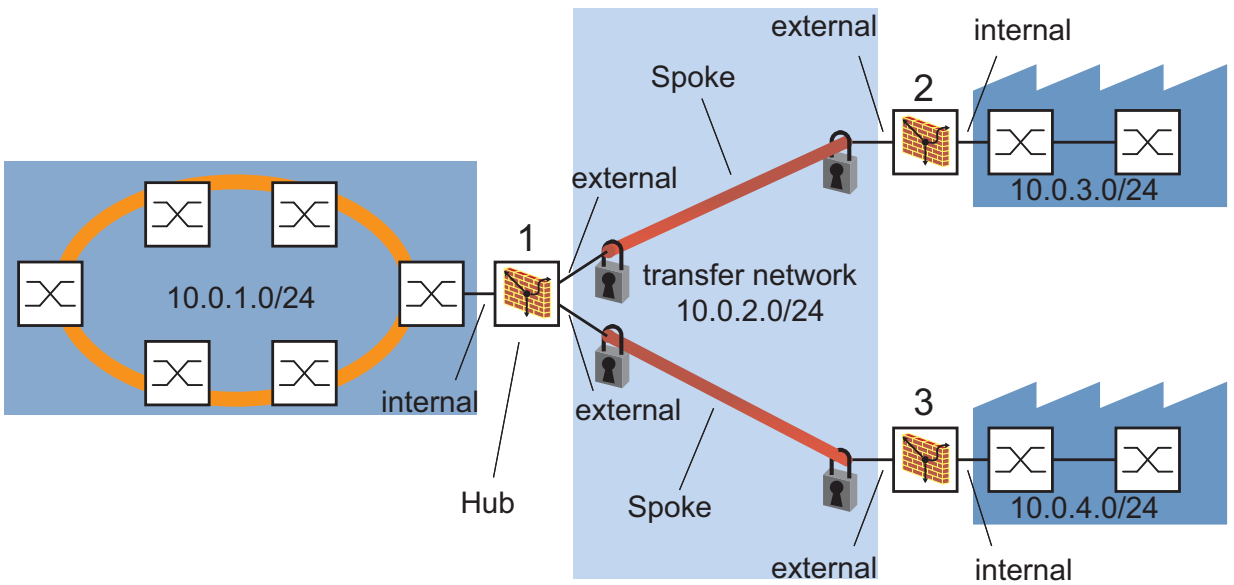



*Figure 42: Connecting several subnetworks via a public network (hub-and-spoke routing)*

The following is known:

| Parameter | Firewall 1 | Firewall 2 | Firewall 3 |
|---|---|---|---|
| IP address of internal port | 10.0.1.201 | 10.0.3.201 | 10.0.4.201 |
| IP address of external port | 10.0.2.1 | 10.0.2.2 | 10.0.2.3 |
| Pre-shared key | 456789defghi | 456789defghi | 456789defghi |
| Start IKE mode as | Initiator | Responder | Responder |
| IP parameters of the networks to be connected | 10.0.1.0/24 | 10.0.3.0/24 | 10.0.4.0/24 |

*Table 11: Interface settings for “hub and spoke” on the participating firewalls*

For the routing of the firewall 1 set the IP networks for every VPN connection in the dialog `VPN:Connections` and in the tab page `IP Networks` according to the following table:

| VPN name | Index | Source Address (CIDR) | Destination Address (CIDR) | Description |
|---|---|---|---|---|
| Production control production hall 1 | 1 | 10.0.1.0/24 | 10.0.3.0/24 | FW 1 to FW 2 |
| | 2 | 10.0.4.0/24 | 10.0.3.0/24 | FW 3 to FW 2 |
| Production control production hall 2 | 1 | 10.0.1.0/24 | 10.0.4.0/24 | FW 1 to FW 3 |
| | 2 | 10.0.3.0/24 | 10.0.4.0/24 | FW 2 to FW 3 |

*Table 12: VPN routing settings for “hub and spoke” on the firewall*

**Note:** The lines with the index 1 allow the communication of the subnetwork of the production control (10.0.1.0/24) directly with subnetworks of the production halls 1 and 2 (10.0.3.0/24 or 10.0.4.0/24).

For the routing of firewalls 2 and 3, set the IP networks for the VPN connection in the dialog `VPN:Connections` and in the tab page `IP Networks` according to the following table:

| Firewall No.: | Index | Source Address (CIDR) | Destination Address (CIDR) | Description |
|---|---|---|---|---|
| 2 | 1 | 10.0.3.0/24 | 10.0.1.0/24 | FW 2 to FW 1 |
| 2 | 2 | 10.0.3.0/24 | 10.0.4.0/24 | FW 2 to FW 3 |
| 3 | 1 | 10.0.4.0/24 | 10.0.1.0/24 | FW 3 to FW 1 |
| 3 | 2 | 10.0.4.0/24 | 10.0.3.0/24 | FW 3 to FW 2 |

*Table 13: VPN routing settings for “hub and spoke” on the spoke firewall*

Prerequisites for further configuration:
- The VPN parameters are configured on the 3 devices.
- The IP parameters of the Firewall router interface are configured.
- The devices in the internal network have the IP address of the internal interface (port 1) of the respective Firewall as their gateway.

☐ Create the routing for Firewall 2 on Firewall 1.

☐ Select the dialog `Virtual Private Network:Connections`.
☐ Select the connection with the name “Production control production hall 1” and click on “Edit”.
☐ Select the IP “Networks” tab page. The device shows an empty table.
☐ Click on “Create entry” to create a new line.
☐ In the 1st line, enter:
- “Source address (CIDR)”, `10.0.1.0/24`
- “Destination address (CIDR)”, `10.0.3.0/24`
- “Description”, `FW 1 to FW 2`

☐ Click on “Create entry” to create a new line.
☐ In the 2nd line, enter:
- “Source address (CIDR)”, `10.0.4.0/24`
- “Destination address (CIDR)”, `10.0.3.0/24`
- “Description”, `FW 3 to FW 2`

☐ Click on “Write” to temporarily save the data.
☐ Click on “Back” to return to the `Virtual Private Network Connections` dialog.

☐ Create the routing for Firewall 3 on Firewall 1.

☐ Select the connection with the name “Production control production hall 2” and click on “Edit”.
☐ Select the IP “Networks” tab page. The device shows an empty table.
☐ Click on “Create entry” to create a new line.
☐ In the 1st line, enter:
- “Source address (CIDR)”, `10.0.1.0/24`
- “Destination address (CIDR)”, `10.0.4.0/24`
- “Description”, `FW 1 to FW 3`

☐ Click on “Create entry” to create a new line.
☐ In the 2nd line, enter:
- “Source address (CIDR)”, `10.0.3.0/24`
- “Destination address (CIDR)”, `10.0.4.0/24`
- “Description”, `FW 2 to FW 3`

- ☐ Click on “Write” to temporarily save the data.
- ☐ Click on “Back” to return to the `Virtual Private Network Connections` dialog.

☐ Save your settings.

- ☐ Click on “Write” to temporarily save the data.
- ☐ Select the dialog `Basic Settings:Load/Save` to save the example configuration.
- ☐ Click on “Save to NVM + EAM” to temporarily save the data in the non-volatile memory.

☐ Create the routing on Firewall 2.

- ☐ Select the dialog `Virtual Private Network:Connections`.
- ☐ Select the connection with the name “Production control production hall 1” and click on “Edit”.
- ☐ Select the IP “Networks” tab page. The device shows an empty table.
- ☐ Click on “Create entry” to create a new line.
- ☐ In the 1st line, enter:
  - “Source address (CIDR)”, `10.0.3.0/24`
  - “Destination address (CIDR)”, `10.0.1.0/24`
  - “Description”, `FW 2 to FW 1`
- ☐ Click on “Create entry” to create a new line.
- ☐ In the 2nd line, enter:
  - “Source address (CIDR)”, `10.0.3.0/24`
  - “Destination address (CIDR)”, `10.0.4.0/24`
  - “Description”, `FW 2 to FW 3`
- ☐ Click on “Write” to temporarily save the routing and mapping data.
- ☐ Click on “Back” to return to the `Virtual Private Network Connections` dialog.
- ☐ Click on “Write” to temporarily save the data.
- ☐ Select the dialog `Basic Settings:Load/Save` to save the example configuration.
- ☐ Click on “Save to NVM + EAM” to temporarily save the data in the non-volatile memory.

☐ Create the routing on Firewall 3.

- ☐ Select the dialog `Virtual Private Network:Connections`.
- ☐ Select the connection with the name “Production control production hall 2” and click on “Edit”.
- ☐ Select the IP “Networks” tab page. The device shows an empty table.
- ☐ Click on “Create entry” to create a new line.
- ☐ In the 1st line, enter:
  - “Source address (CIDR)”, `10.0.4.0/24`
  - “Destination address (CIDR)”, `10.0.1.0/24`
  - “Description”, `FW 3 to FW 1`
- ☐ Click on “Create entry” to create a new line.
- ☐ In the 2nd line, enter:
  - “Source address (CIDR)”, `10.0.4.0/24`
  - “Destination address (CIDR)”, `10.0.3.0/24`
  - “Description”, `FW 3 to FW 2`
- ☐ Click on “Write” to temporarily save the routing and mapping data.
- ☐ Click on “Back” to return to the `Virtual Private Network Connections` dialog.
- ☐ Click on “Write” to temporarily save the data.
- ☐ Select the dialog `Basic Settings:Load/Save` to save the example configuration.
- ☐ Click on “Save to NVM + EAM” to temporarily save the data in the non-volatile memory.

## Schneider Electric Address Mapping

Schneider Electric Address Mapping allows you to establish an unlimited number of networks with identical IP address ranges which are connected via VPN with a public network and clearly distinguishable from the public network.

- The individual networks’ identical address ranges simplify the porting of their configuration.
- Their distinguishability from the common network facilitates the unambiguous administration.

You can use the Schneider Electric Address Mapping, for example, to centrally administer multiple production cells.

The Firewall with Schneider Electric Address Mapping allows you to replace the internal IP addresses with external valid and distinct IP addresses for the VPN connection. Schneider Electric Address Mapping works like a 1:1 NAT router integrated in the VPN connection. The Firewall provides outgoing data packets from a definable address range with a new return address - the Firewall thus maps the internal return address to an valid external address. The Firewall automatically supplies incoming data packets with the valid internal destination address. This assignment is reversibly unique.

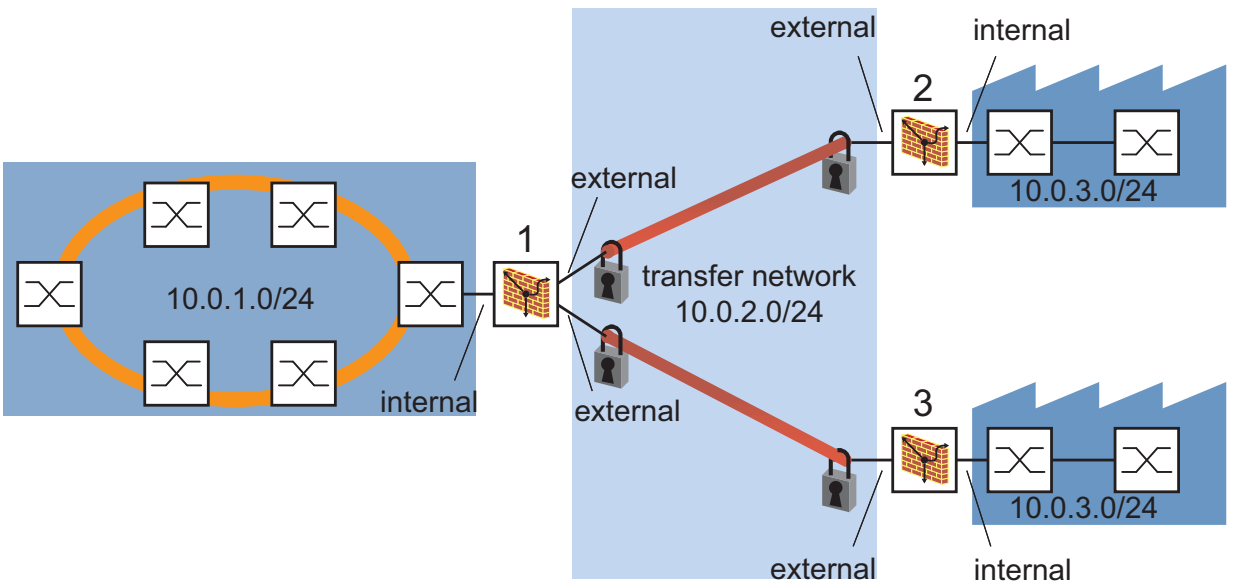



*Figure 43: Addressing several identical subnetworks from a public network (Schneider Electric Address Mapping)*

The following is known:

| Parameter | Firewall 1 | Firewall 2 | Firewall 3 |
|---|---|---|---|
| IP address of internal port | 10.0.1.201 | 10.0.3.201 | 10.0.3.201 |
| IP address of external port | 10.0.2.1 | 10.0.2.2 | 10.0.2.3 |
| Pre-shared key | 456789defghi | 456789defghi | 456789defghi |
| Start IKE mode as | Initiator | Responder | Responder |
| IP parameters of the networks to be connected | 10.0.1.0/24 | 10.0.3.0/24 | 10.0.3.0/24 |
| Mapped IP parameter from the network | - | 10.0.4.0/24 | 10.0.5.0/24 |

*Table 14: Interface settings for Schneider Electric Address Mapping on the participating firewalls*

For the routing of the firewall 1 set the IP networks for every VPN connection in the dialog `VPN:Connections` and in the tab page `IP Networks` according to the following table:

| VPN-name | Index | Source Address (CIDR) | Destination Adress (CIDR) | Description |
|---|---|---|---|---|
| Production control-production hall 1 | 1 | 10.0.1.0/24 | 10.0.4.0/24 | FW 1 to FW 2 |
| Production control-production hall 2 | 1 | 10.0.1.0/24 | 10.0.5.0/24 | FW 1 to FW 3 |

*Table 15: VPN routing settings for Schneider Electric Adress Mapping on the firewall of the production control*

For the address mapping of firewalls 2 and 3, set the IP networks in the dialog `VPN:Connections` and in the tab page `IP Networks` according to the following table:

| Firewall | Index | Source address (CIDR) | Destination address (CIDR) | Mapped source address (CIDR) | Description |
|---|---|---|---|---|---|
| 2 | 1 | 10.0.3.0/24 | 10.0.1.0/24 | 10.0.4.0/24 | FW 2 to FW 1 |
| 3 | 1 | 10.0.3.0/24 | 10.0.1.0/24 | 10.0.5.0/24 | FW 3 to FW 1 |

*Table 16: VPN routing settings for Schneider Electric Address Mapping on the firewall of the production networks*

**Note:** In the “Mapping destination address (CIDR)” column, no entry is required.

Prerequisites for further configuration:
- The VPN parameters are configured on the 3 devices.
- The IP parameters of the Firewall router interface are configured.
- The devices in the internal network have the IP address of the internal interface (port 1) of the respective Firewall as their gateway.

☐ Create the routing for Firewall 2 on Firewall 1.

- ☐ Select the dialog `Virtual Private Network:Connections`.
- ☐ Select the connection with the name “Production control production hall 1” and click on “Edit”.
- ☐ Select the IP “Networks” tab page. The device shows an empty table.
- ☐ Click on “Create entry” to create a new line.
- ☐ In the 1st line, enter:
  - “Source address (CIDR)”, `10.0.1.0/24`
  - “Destination address (CIDR)”, `10.0.4.0/24` (mapped network)
  - “Description”, `FW 1 to FW 2`
- ☐ Click on “Write” to temporarily save the data.
- ☐ Click on “Back” to return to the `Virtual Private Network Connections` dialog.

☐ Create the routing for Firewall 3 on Firewall 1.

- ☐ Select the connection with the name “Production control production hall 2” and click on “Edit”.
- ☐ Select the IP “Networks” tab page. The device shows an empty table.
- ☐ Click on “Create entry” to create a new line.
- ☐ In the 1st line, enter:
  - “Source address (CIDR)”, `10.0.1.0/24`
  - “Destination address (CIDR)”, `10.0.5.0/24` (mapped network)
  - “Description”, `FW 1 to FW 3`
- ☐ Click on “Write” to temporarily save the data.
- ☐ Click on “Back” to return to the `Virtual Private Network Connections` dialog.

☐ Save your settings.

- ☐ Click on “Write” to temporarily save the data.
- ☐ Select the dialog `Basic Settings:Load/Save` to save the example configuration.
- ☐ Click on “Save to NVM + EAM” to temporarily save the data in the non-volatile memory.

☐ Create the address mapping for the Firewall 2.

- ☐ Select the dialog `Virtual Private Network:Connections`.
- ☐ Select the connection with the name “Production control production hall 1” and click on “Edit”.
- ☐ Select the IP “Networks” tab page. The device shows an empty table.
- ☐ Click on “Create entry” to create a new line.
- ☐ In the 2nd line, enter:
  - “Source address (CIDR)”, `10.0.3.0/24`
  - “Destination address (CIDR)”, `10.0.1.0/24`
  - “Mapping source address (CIDR)”, `10.0.4.0/24`
  - “Description”, `FW 2 to FW 1`
- ☐ Click on “Write” to temporarily save the data.
- ☐ Click on “Back” to return to the `Virtual Private Network Connections` dialog.
- ☐ Click on “Write” to temporarily save the data.
- ☐ Select the dialog `Basic Settings:Load/Save` to save the example configuration.
- ☐ Click on “Save to NVM + EAM” to temporarily save the data in the non-volatile memory.

☐ Create the routing for Firewall 3.

- ☐ Select the dialog `Virtual Private Network:Connections`.
- ☐ Select the connection with the name “Production control production hall 2” and click on “Edit”.
- ☐ Select the IP “Networks” tab page. The device shows an empty table.
- ☐ Click on “Create entry” to create a new line.
- ☐ In the 2nd line, enter:
  - “Source address (CIDR)”, `10.0.3.0/24`
  - “Destination address (CIDR)”, `10.0.1.0/24`
  - “Mapping source address (CIDR)”, `10.0.5.0/24`
  - “Description”, `FW 3 to FW 1`
- ☐ Click on “Write” to temporarily save the data.
- ☐ Click on “Back” to return to the `Virtual Private Network Connections` dialog.
- ☐ Click on “Write” to temporarily save the data.
- ☐ Select the dialog `Basic Settings:Load/Save` to save the example configuration.
- ☐ Click on “Save to NVM + EAM” to temporarily save the data in the non-volatile memory.

## Connecting a PC with a subnetwork

The production manager wants to be able to view the current production data from home. For this purpose, he sets up a VPN connection via a DSL port. As his DSL connection does not have a fixed IP address, he uses DynDNS to determine his IP address.
Increased security requirements make it a good idea to use X.509 key information.

| Parameter | Firewall Number 5 | Firewall Number 6 |
|---|---|---|
| IP address of internal port | 10.0.1.202 | 10.0.3.202 |
| IP address of external port | 10.149.112.92 | DynDNS |
| Key information | PKCS#12 file | PKCS#12 file |
| Start IKE mode as | Initiator | Responder |
| IP parameters of the networks to be connected | 10.0.1.0/24 | 10.0.5.25/32 |

Prerequisites for further configuration:

- Both Firewalls are in PPPoE mode.
- The logon data for the DSL provider is configured.
- The IP parameters of the internal interface are configured.
- The devices in the internal network have the IP address of the internal interface (port 1) of the Firewall as their gateway.
- You have an account at www.DynDNS.org.
- The PKS#12 files/machine certificates with the key information are provided by the same certification authority.


*Figure 44: Connecting a PC with a subnetwork via a public network*

☐ Configure the DynDNS client on TCSEFEC No. 6.
To configure the DynDNS, you require:
– the name of the DynDNS server.
At DynDNS.org, the host name of the HTTP server for the DynDNS service is “members.dyndns.org”.
– the “user name”, from the logon at DynDNS.org,
e.g. “hugo”

– the “password”, from the logon at DynDNS.org, e.g. “oguh”
– the “host name” registered at DynDNS.org, from the logon at DynDNS.org, e.g. “gerhardsFW.dyndns.org”

☐ Select the `Enhanced:DNS:DynDNS` dialog.
☐ Activate “Register” so that TCSEFEC No. 6 passes its current IP address to the DynDNS server as soon as it changes.
☐ Enter the name of the DynDNS server: `member.dyndns.org`.
☐ In “Login”, you enter your DynDNS user name: `hugo`.
☐ In “Password”, you enter your DynDNS password: `oguh`.
☐ In “Host name”, you enter your DynDNS host name: `gerhardsFW.dyndns.org`.

☐ Configure the DNS server on TCSEFEC No. 5.
To configure the DynDNS, you require:
– the name of the DynDNS server.
At DynDNS.org, the host name of the HTTP server for the DynDNS service is “members.dyndns.org”.
– the “user name”, from the logon at DynDNS.org, e.g. “hugo”
– the “password”, from the logon at DynDNS.org, e.g. “oguh”
– the “host name” registered at DynDNS.org, from the logon at DynDNS.org, e.g. “gerhardsFW.dyndns.org”

☐ Select the `Enhanced:DNS:DynDNS` dialog.
☐ Activate “Register” so that TCSEFEC No. 5 passes its current IP address to the DynDNS server as soon as it changes.
☐ Enter the name of the DynDNS server: `member.dyndns.org`.
☐ In “Login”, you enter your DynDNS user name: `hugo`.
☐ In “Password”, you enter your DynDNS password: `oguh`.
☐ In “Host name”, you enter your DynDNS host name: `gerhardsFW.dyndns.org`.

☐ On TCSEFEC No. 5, you create a new VPN connection to TCSEFEC No.6.

☐ Select the dialog `Virtual Private Network:Connections`.
☐ Click on “Create Entry”.
In the `Basic Settings` tab page, the dialog for editing the entries gives you the option to give this connection any name you want.
☐ Give the connection a name, e.g.
“Home - Production Hall number 3”.

☐ Enter the authentication parameters.

☐ Select the `Authentication` tab page.
☐ In the `Key Information` frame, you enter:
- “Method” `x509rsa`

☐ In the `Identities` frame, you enter:
- “Local type” `asn1dn`
  With this, you specify that the local Firewall identifies itself with the “Distinguished Name” from the certificate.
- “Remote type” `asn1dn`
  With this, you specify that the remote Firewall identifies itself with the “Distinguished Name” from the certificate.

☐ Enter the certificate parameters.

☐ Select the `Certificates` tab page.
☐ Click on “Load PKCS#12 file from PC”.
The “Copy from PC” dialog enables you to
– select the PKCS#12 file,
– enter the password belonging to the certificate and
– load the PKCS#12 file onto the Firewall by clicking on “Copy from PC”.
After loading the PKCS#12 file, you can see the individual certificate shares in the dialog.

☐ Enter the IKE key exchange parameters.

☐ Select the `IKE - Key Exchange` tab page.
☐ In the `Mode` frame, you enter:
- "Protocol" `auto`
  With this, the Firewall selects the protocol version automatically, depending on the VPN remote terminal.
- "Startup as", `initiator`
  With this, this Firewall initiates the VPN connection to the remote terminal.
- "DPD Timeout", `120`
  With this, the Firewall terminates the VPN connection if it does not receive a sign of life from the remote terminal within 120 seconds.
- "Lifetime" `28800`
  After this lifetime has elapsed, the two participating Firewalls agree on new keys for the IKE security arrangement (IKE SA). The lifetime is there to effect a periodic key change for the IKE SA.
- "Compatibility Mode", `Off`

☐ In the `Algorithms` frame, enter the encryption procedures you wish to use for the various applications:
- "Key Agreement" `modp1024`
- "Hash", e.g. `md5`
- "Integrity" `hmacsha1`
- "Encryption" `aes128`

☐ In the `Peers (Endpoints)` frame, you enter:
- "Local IP address" `10.149.112.92`
- "Remote IP Address" `gerhardsFW.dyndns.org`

In the current example, the external ports of the two Firewalls are the endpoints of the VPN connection. While the local IP address is known, the remote IP address is subject to being changed by the DSL provider. In this case, the Firewall determines the remote IP address using DynDNS.

☐ Enter the parameters for the IP networks whose data is to be transmitted via the VPN connection.

☐ Select the `IP Networks` tab page.
☐ Click on `Create entry`.
☐ After you double-click on a cell of the entry, you can edit the cell:
- "Source address" `10.0.1.0/24`
- "Source port" `any`
- "Destination address" `gerhardsFW.dyndns.org`
- "Destination port" `any`
- "Protocol" `any`
- "Description" `Free data traffic between Home and Production Hall`
- "Active" `On`

☐ Click "Set" to temporarily save the entry in the configuration.

☐ Save the settings in the non-volatile memory.

☐ Select the dialog
`Basic Settings:Load/Save`.
☐ Click on “Save to NVM + EAM” to save the configuration in the active configuration.

☐ Make exactly the same settings on both Firewalls. For the second Firewall, in the settings for the authentication, the IKE key exchange and the IP networks, you merely swap the IP addresses for the endpoints or networks.

## Connecting a LANCOM Advanced VPN Client with a private network

In this case, a production manager wants to access his production data from any location within the company via a VPN connection. To do so, he uses a notebook with installed LANCOM Client software. He can thus set up the VPN connection directly between his notebook and the TCSEFEC.

| Parameter | Firewall | LANCOM Client |
|---|---|---|
| IP address of internal port | 10.0.1.201 | |
| IP address of external port | 10.0.2.1 | |
| Pre-shared key | 123456abcdef | 123456abcdef |
| Start IKE mode as | Responder | Initiator |
| IP parameters of the networks to be connected | 10.0.1.0/24 | 10.0.2.92/32 |

Prerequisites for further configuration:

- The Firewall is in router mode.
- The IP parameters of the Firewall router interface are configured.
- The devices in the internal network have the IP address of the internal interface (port 1) of the Firewall as their gateway.

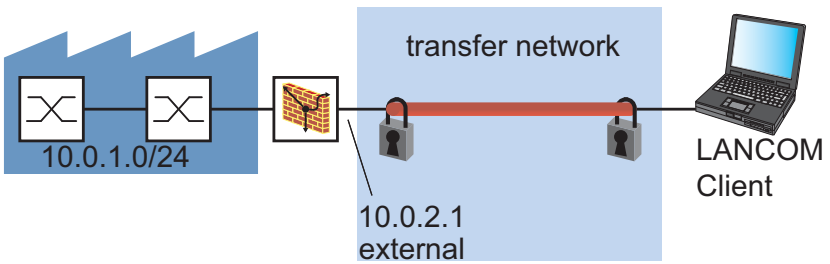



*Figure 45: Connecting a LANCOM Client with a private network via a public network*

Settings on the TCSEFEC:

☐ Create a new VPN connection.

☐ Select the dialog `Virtual Private Network:Connections`.

☐ Click on “Create Entry”.
In the `Basic Settings` tab page, the dialog for editing the entries gives you the option to give this connection any name you want.

☐ Give the connection a name, e.g.
“Production Manager - Production Hall”.

☐ Enter the authentication parameters.

☐ Select the `Authentication` tab page.

☐ In the `Key Information` frame, you enter:

- “Method” `psk`
- “Pre-shared key”, e.g. `123456abcdef`

☐ In the `Identities` frame, you enter:

- “Local Type” `default`
- “Remote type” `fqdn`
  With this, you specify that the remote key identification is part of the identification.
- “Remote ID”, e.g. `www.schneider-electric.com`

☐ Enter the IKE key exchange parameters.

☐ Select the `IKE - Key Exchange` tab page.

☐ In the `Mode` frame, you enter:

- "Protocol" `auto`
  With this, the Firewall selects the protocol version automatically, depending on the VPN remote terminal.
- "Startup as", `responder`
  With this, this Firewall responds to the request to set up a VPN connection to the remote terminal.
- "DPD Timeout", `120`
  With this, the Firewall terminates the VPN connection if it does not receive a sign of life from the remote terminal within 120 seconds.
- "Lifetime" `28800`
  After this lifetime has elapsed, the two participating Firewalls agree on new keys for the IKE security arrangement (IKE SA). The lifetime is there to effect a periodic key change for the IKE SA.
- "Compatibility Mode", `Off`

☐ In the `Algorithms` frame, you enter which encryption procedures you want to use for the different applications:

- "Key Agreement" `modp1024`
- "Hash", e.g. `md5`
- "Integrity" `hmacmd5`
- "Encryption" aes128

☐ In the `Peers (Endpoints)` frame, you enter:

- "Local IP Address" `10.0.2.1`
- "Remote IP Address" `10.0.2.92`

In the current example, the external port of the Firewall and the Ethernet interface of the LANCOM Client are the endpoints of the VPN connection.

☐ Enter the IPsec data exchange parameters.

☐ Select the `IPsec - Data Exchange` tab page.
☐ In the `Mode` frame, you enter:
- "Encapsulation" `tunnel`
  With this, the Firewall encrypts the entire data packet, including the IP addresses of the communication partners.
- "Force NAT-T" `No`.
- "Lifetime" `3600`.

☐ In the `Algorithms` frame, you enter:
- "Key Agreement" `modp1024`
- "Integrity" `hmacmd5`
- "Encryption" `aes128`

☐ Enter the parameters for the IP networks whose data is to be transmitted via the VPN connection.

☐ Select the `IP Networks` tab page.
☐ Click on `Create entry`.
☐ After you double-click on a cell of the entry, you can edit the cell:
- "Source address" `10.0.1.0/24`
- "Source port" `any`
- "Destination address" `10.0.2.92/32`
- "Destination port" `any`
- "Protocol" `any`
- "Description" `Free data traffic between Production Manager and Production Hall`
- "Active" `On`

☐ Click "Set" to temporarily save the entry in the configuration.

☐ Save the settings in the non-volatile memory.

☐ Select the dialog `Basic Settings:Load/Save`.
☐ Click on "Save to NVM + EAM" to save the configuration in the active configuration.

Settings on the notebook with the LANCOM Advanced VPN Client:

Requirement: The LANCOM Advanced VPN Client Software is installed on the notebook.

☐ Start the LANCOM Client software on your PC.
☐ Create a new profile with `Configuration:Profile Settings`.
☐ Click on “New Entry”.

An assistant takes you through the configuration of the new profile.

☐ Select the connection type
“Connection to company network via IPsec”.
Click on “Continue”.
☐ Enter a name for the profile.
Click on “Continue”.
☐ Select the connection medium “LAN (over IP)”.
Click on “Continue”.
☐ For the gateway address, you enter the IP address of the external interface of the Firewall, e.g. `10.0.2.1`.
Click on “Continue”.
☐ Select the exchange mode “Main Mode”.
Select the PFS group “DH group 2 (1024 Bit)”.
Click on “Continue”.
☐ Under “Shared Secret”, you enter the pre-shared key `123456abcdef`.
Repeat the entry for the pre-shared key.
Select the local identity type “Fully Qualified Domain Name”.
Enter the local identity ID `www.schneider-electric.com`.
Click on “Continue”.
☐ For the IP address assignment, select the manual assignment “Use local IP address”.
Click on “Continue”.
☐ To select the IP network for the communication, click on “New”.
Enter the IP address and the network mask of the network in the production hall, e.g. `10.0.1.0` and `255.255.255.0`.
Click on „OK“.
Click on “Finish”.
You thus quit the assistant for the configuration of the profile.
☐ Select the new profile and click on “Configure”.
☐ Click on “IPsec settings” in the left field.
☐ Under “Guideline” you enter:
– “IKE guideline”: `Pre-shared Key`.
– “IPsec guideline”: `ESP-AES128-MD5`.
☐ Click on “Validity”.

- ☐ In the “IPsec guideline” frame, under “Duration”, you enter `000:01:00:00`.
  This value is the same as the “Lifetime” in the TCSEFEC settings under “IPsec - Data Exchange”.
- ☐ Click on “OK” to close the input window.
- ☐ Click on “OK” to finish the profile setting.
- ☐ On the LANCOM client main screen, select the profile created and click on “Connect” to set up the VPN connection to the TCSEFEC.
  If the LANCOM Client cannot set up the connection, then restart the PC with the LANCOM Client.
  After the restart, click on “Connect” to set up the VPN connection to the TCSEFEC.

## Activating VPN connection automatically and displaying activation via STATUS LED

The TCSEFEC device provides you with a service mode function. In service mode, the device automatically activates one or more VPN connections that you have pre-configured

- if the redundant power supply (PS2) of the TCSEFEC device is inoperable
- if you switch off the redundant power supply (PS2) of the TCSEFEC device for this purpose, in order to automatically activate one or more VPN connections.

☐ Create a new VPN connection and configure the connection.

☐ Select the dialog `Virtual Private Network:Connections`.
☐ Click on “Create Entry”.
☐ Enter a name for the connection in the “Name” field, for example maintenance_production .
☐ Select the “Service Mode” field to activate the service mode for this connection.
☐ Select the “Active” field.
☐ In the “Exchange Mode” field, choose the entry `mainaggressive`.
☐ Click on “Write” to temporarily save the entry in the configuration.

☐ Repeat these steps for additional VPN connections.

The “Status” field shows you the status for each VPN connection. If the service mode is activated, the entry is `servicemode-up`.

The TCSEFEC device allows you to use the „STATUS” LED to display active VPN connections. To activate this function, you proceed as follows:

☐ Select the dialog `Virtual Private Network:Connections`.
☐ Select the “Status LED Indication” field.
☐ Click on “Write” to temporarily save the entry in the configuration.

The “STATUS” LED of the TCSEFEC device blinks once a second, alternatively in yellow and green, if one or more VPN connections are active.

**Note:** Displaying flash and EAM access has a higher priority than displaying active VPN connections. If the TCSEFEC device performs a flash or EAM access and an active VPN connection at the same time, the LED indicates the flash/EAM access by blinking green.

# 7 Setting up the Redundancy

The Redundancy function of the Firewall allows you to operate the Firewall and its supply lines redundantly.
If a Firewall or a supply line to the Firewall is inoperable, the other Firewall and its supply lines take over the function of the first Firewall.
For this purpose, the two Firewalls continuously synchronize the state of the stateful firewall. Thus, when there is a switch from one Firewall to the other, the existing connections are maintained.

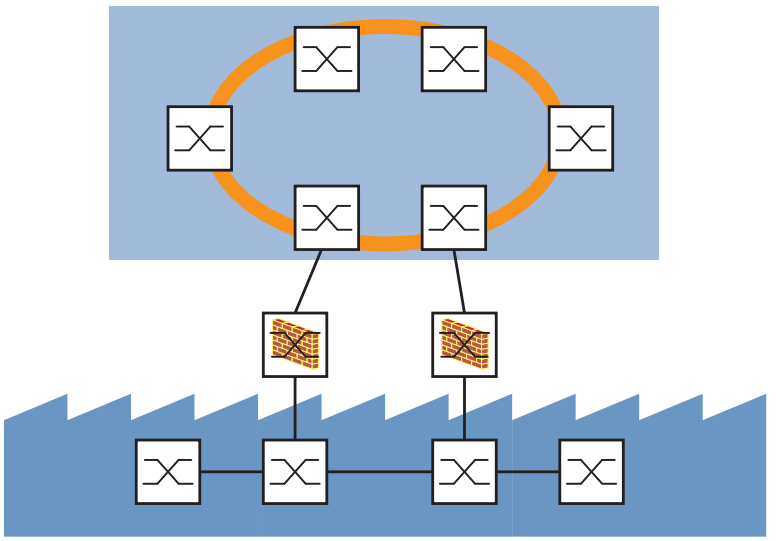


*Figure 46: Redundant Firewall connection*

# 7.1 Transparent Redundancy

## 7.1.1 Description of the Transparent Redundancy function

In the Network Transparent mode, the Firewall allows you to incorporate one Firewall each into the paths of two redundantly coupled networks (see the user manual for the redundancy configuration of your Schneider Electric device that supports redundant coupling).
If the main connection is inoperable, the substitute Firewall takes over the tasks of the main Firewall.

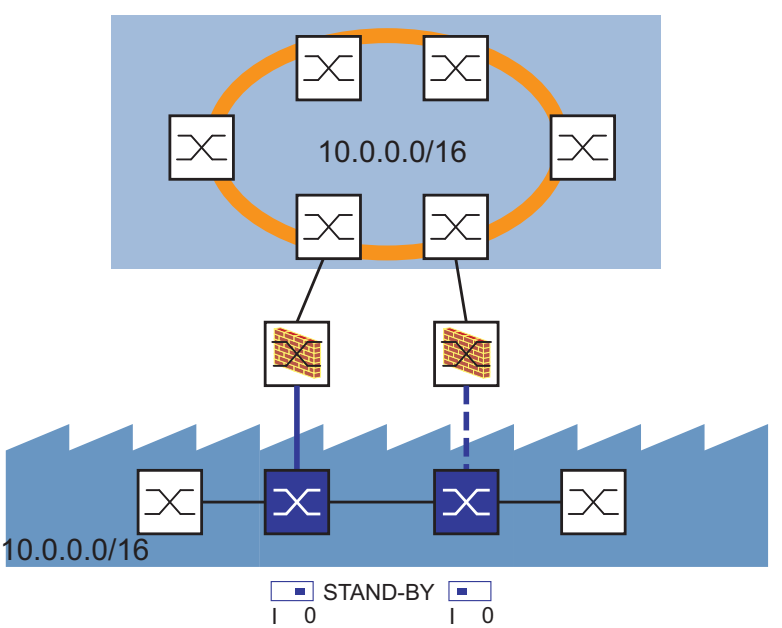



*Figure 47: Transparent Redundancy*

### 7.1.2 Application Example for the Transparent Redundancy

You are using Transparent Redundancy in a flat network.
For availability reasons, you have connected a production cell that continuously requires current production data to the company network via redundant coupling.
To help make the production cell secure, you install a Firewall in every path to the company network.
The following is known:

| Parameter | Firewall 1 | Firewall 2 |
|---|---|---|
| Own IP Address | 10.0.0.201/16 | 10.0.0.202/16 |
| Redundancy Partner IP Address | 10.0.0.202/16 | 10.0.0.201/16 |

Prerequisites for further configuration:
- The Firewall is in transparent mode.
- The IP parameters in transparent mode are configured.

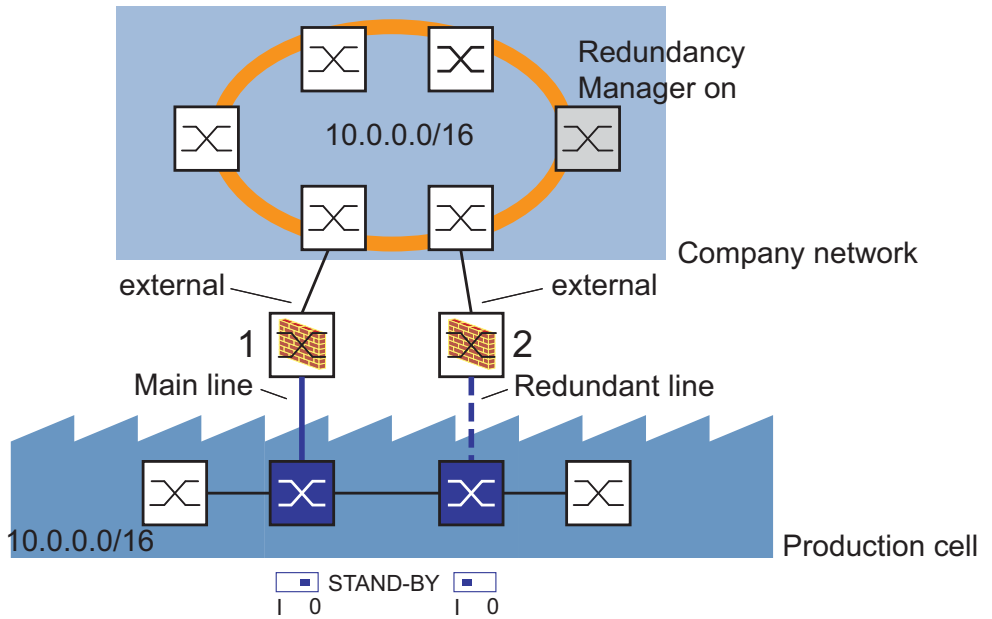



*Figure 48: Transparent Redundancy application example*

☐ First you configure firewall number 1.
Enter the parameters for the Transparent Redundancy and activate the function.

☐ Select the dialog `Redundancy:Transparent`.
☐ In the “Function” line in the “Configuration” frame, click `On` to activate the function.
☐ In the “Transparent Mode” frame, select the Master or Slave Port: `internal` (main line).
☐ In the “Firewall state table synchronization” frame, enter the IP address of the redundancy partner.
In this case, this is the IP address of firewall number 2: `10.0.0.202`.
☐ Click “Set” to temporarily save the entry in the configuration.

☐ Save the settings in the non-volatile memory.

- ☐ Select the dialog `Basic Settings:Load/Save`.
- ☐ Click on “Save to NVM + EAM” to save the configuration in the active configuration.

☐ Now you configure firewall number 2.
Enter the parameters for the Transparent Redundancy and activate the function.

- ☐ Select the dialog `Redundancy:Transparent`.
- ☐ In the “Function” line in the “Configuration” frame, click `On` to activate the function.
- ☐ In the “Transparent Mode” frame, select the Master or Slave Port: `internal` (redundant line).
- ☐ In the “Firewall state table synchronization” frame, enter the IP address of the redundancy partner.
  In this case, this is the IP address of firewall number 1: `10.0.0.201`.
- ☐ Click “Set” to temporarily save the entry in the configuration.

☐ Save the settings in the non-volatile memory.

- ☐ Select the dialog `Basic Settings:Load/Save`.
- ☐ Click on “Save to NVM + EAM” to save the configuration in the active configuration.

**Note:** In the display field behind `Communication` in the `Redundancy:Transparent` dialog window, the Web-based interface shows you the Layer 2 status of your redundancy connection:

- Behind the `Communication` parameter, the `Active` display field is checkmarked: The communication via the main line of your redundancy configuration is active.
- Behind the `Communication` parameter, the `Inactive` display field is checkmarked: There is currently no communication via the main line of your redundancy configuration.

  ☐ Check whether a data line or a network component in your redundancy configuration may be inoperable. Check the redundancy status using the switches in the path of the redundant ring/network coupling in which you have incorporated the firewall (see the user manual for the redundancy configuration of your Schneider Electric device that supports redundant coupling).

# 7.2 Router Redundancy

## 7.2.1 Description of the Router Redundancy Function

In the Router mode, the Firewall allows you to use a Firewall to install a redundant line and a redundant Firewall for an existing connection between two networks.

Terminal devices usually give you the option of entering a default gateway for transmitting data packets in external subnetworks. Here the term “Gateway” applies to a router by means of which the terminal device can communicate in other subnetworks.
If this router is inoperable, the terminal device cannot send any more data to external subnetworks.
In this case, the Router Redundancy function helps the Firewall with the virtual IP address. This function helps provide a type of “gateway redundancy”. It describes a process that groups two routers into one virtual router. Terminal devices address the virtual router, and the Router Redundancy function helps ensure that a physical router belonging to the virtual router takes over the data transmission.

The two Firewalls continuously exchange information via the internal interface and also via the external interface. Thus they also check the accessibility at the same time.
If the firewall, which temporarily assumes the virtual router function, discovers a line interruption on one of its ports, it informs its partner firewall, which then takes over the virtual router function.
The Firewall also offers you the ICMP host check function for monitoring lines in the connected network.
As soon as one Firewall loses the connection to the other Firewall at one port, both Firewalls send ping requests to the IP addresses entered in the ICMP Host Check table.
After the evaluation of the ping responses, the two Firewalls decide which

Firewall takes over the active transmission function.
By entering specific IP addresses, such as those of servers, routers, controllers/PLC, in the ICMP Host Check table, you help ensure the high availability of the connection to these devices in the internal and external networks.

If the main connection is inoperable, the redundant Firewall takes over the tasks of the main Firewall.

You can combine 1:1 NAT with the router redundancy. You thus obtain a high-availability 1:1-NAT router (see on page 139 “1:1 NAT”).

**Note:** With 1:1 NAT the Firewall responds to ARP requests from the external network to addresses which it maps from the internal network. This is also the case when no device with the IP address exists in the internal network. Therefore, in the external network, only allocate to devices IP addresses located outside the area which 1:1 NAT maps from the internal network to the external network.

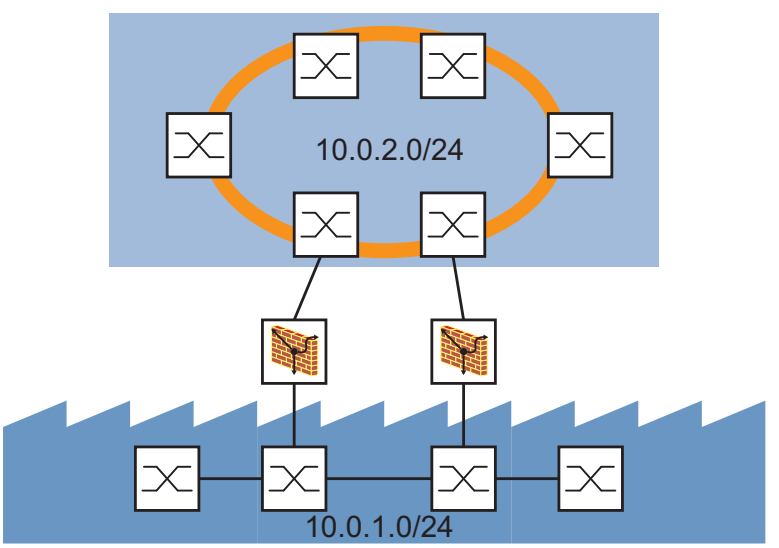



*Figure 49: Router Redundancy*

### 7.2.2 Application Example for the Router Redundancy

You use Router Redundancy when you are operating the Firewall in Router mode.
For availability reasons, you have connected a production cell that continuously requires current production data to the company network via a redundant line with a redundant Firewall.
The following is known:

| Parameter | Firewall 1 | Firewall 2 |
|---|---|---|
| Priority | 100 | 90 |
| Internal IP Address | 10.0.1.201/24 | 10.0.1.202/24 |
| Virtual IP Address (VR-IP) of the internal interface | 10.0.1.200/24 | 10.0.1.200/24 |
| Virtual Router ID (VRID) of the internal interface | 1 | 1 |
| Redundancy Partner IP Address (internal interface) | 10.0.1.202/24 | 10.0.1.201/24 |
| External IP Address | 10.0.2.201/24 | 10.0.2.202/24 |
| Virtual IP Address (VR-IP) of the external interface | 10.0.2.200/24 | 10.0.2.200/24 |
| Virtual Router ID (VRID) of the internal interface | 2 | 2 |
| Redundancy Partner IP Address (external interface) | 10.0.2.202/24 | 10.0.2.201/24 |

Prerequisites for further configuration:
- The Firewall is in router mode.
- The IP parameters in Router mode are configured.
- The devices in the internal network (production cell) have the VR IP address of the internal interface as their gateway.
- The devices in the external network (company network) have the VR IP address of the external interface as their gateway.

**Note:** When using multiple redundant routers in your network, use unique VRIDs. You thus help prevent these virtual router applications that use VRRP from having a negative influence on each other.

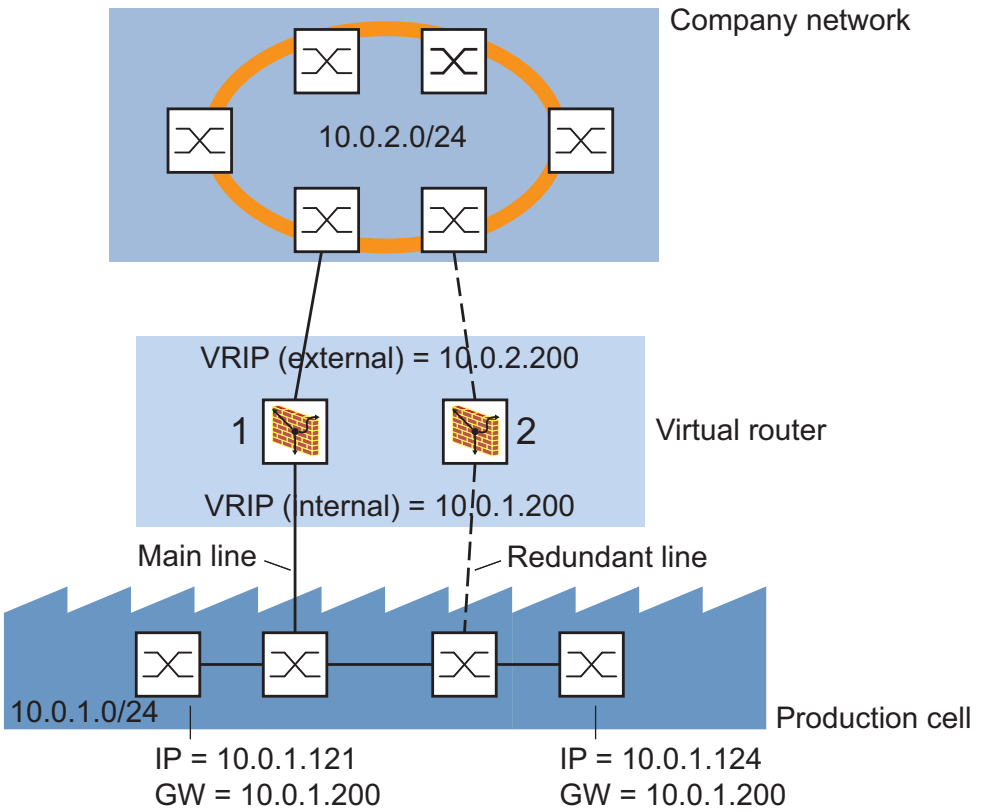



*Figure 50: Router Redundancy application example*

☐ First you configure firewall number 1.
Enter the parameters for the Router Redundancy and activate the function.

☐ Select the dialog `Redundancy:Router`.
☐ Select the tab page `Basic Settings`.
☐ In the “Function” line in the “Configuration” frame, click `On` to activate the function.
☐ Enter the parameters in accordance with the above table.
☐ Click “Set” to temporarily save the entry in the configuration.

☐ Save the settings in the non-volatile memory.

☐ Select the dialog
`Basic Settings:Load/Save`.
☐ Click on “Save to NVM + EAM” to save the configuration in the active configuration.

☐ Now you configure firewall number 2.
Enter the parameters for the Router Redundancy and activate the function.
☐ Save the settings in the non-volatile memory.

# 8 Operation Diagnosis

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

- Reachability Test (Ping)
- Sending traps
- Monitoring the device status
- Out-of-band signaling via signal contact
- Port status indication
- Topology Discovery
- Configuration Check
- Reports
- MAC Firewall List
- IP Firewall List

# 8.1 Reachability Test (Ping)

The Firewall allows you to test the reachability of any network node directly from the device, including through a VPN tunnel.

Thus, in the case of detected problems in the network you quickly receive information from the device about the accessibility of a particular network node (e.g. a server).

The Reachability Test sends out a series of ICMP echo requests and checks if the responses arrive within a set time limit. You can see the test result a few seconds later in the same dialog window.

**Note:** The Reachability Test requires that the network node that you want to test supports ICMP and that the existing firewalls in the path allow through ICMP echo requests and responses.

State on delivery: deactivated, source address: 0.0.0.0
When the source address is 0.0.0.0, the Firewall uses the IP address of the interface at which the pings are sent. The Firewall determines the interface from the destination address and the routing table.

# 8.2 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 unusual events.

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.

### 8.2.1 SNMP trap listing

You can find a list of the traps the device can send in the “Web-based Interface” reference manual.

### 8.2.2 SNMP Traps during Boot

The device sends the ColdStart trap every time it boots.

## 8.2.3 Configuring Traps

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

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

☐ Click “Create entry” to create a new table entry.

☐ In the “Name” column, enter a name for the recipient to whom the traps should be sent.

☐ In the “IP Address” column, enter the IP address of the recipient to whom the traps should be sent.

☐ Click on “OK”.

☐ In the “Active” column, you select the entries which should be taken into account when traps are being sent.

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

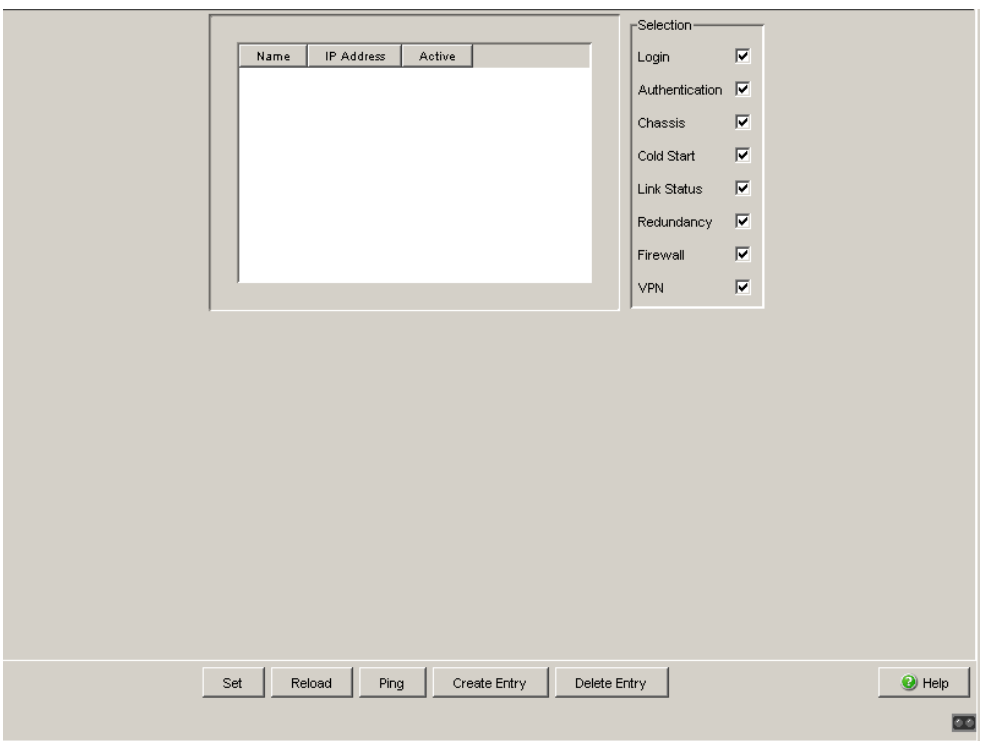



*Figure 51: Alarms dialog*

# 8.3 Monitoring the Device Status

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

The device displays its current status as “Error” or “OK” in the “Device Status” frame. The device determines this status from the individual monitoring results.
The device enables you to

- signal the device status out-of-band via a signal contact (see on page 208 “Monitoring the Device Status via the Signal Contact”)
- signal the device status by sending a trap when the device status changes
- detect the device status in the Web-based interface on the system side.
- query the device status in the Command Line Interface.

The device status of the device includes:

- Incorrect supply voltage,
  the detected failure of at least one of the two supply voltages,
  a detected failure in the device (internal supply voltage).
- The temperature threshold has been exceeded or has not been reached.
- The removal of the EAM.
- The interrupted connection to at least one port. With the device, the indication of link status can be masked via the management for each port (see on page 84 “Displaying detected connection errors”). On delivery, there is no link monitoring.

The management setting specifies which events determine the device status.

**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 208 “Monitoring the Device Status via the Signal Contact”).

## 8.3.1 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 also set the temperature thresholds in the `Basic settings: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 enable` | Includes all the possible events in the device status determination. |
| `device-status trap enable` | Enable a trap to be sent if the device status changes. |

## 8.3.2 Displaying the Device Status

☐ Select the `Basics:System` dialog.

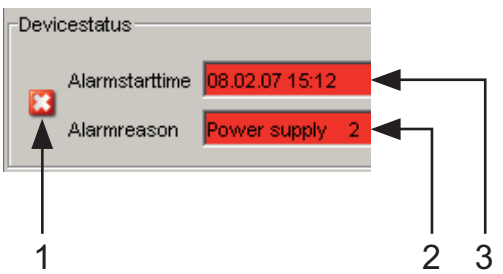



*Figure 52: Device status and display of detected alarms*
*1 - Symbol indicates the Device Status*
*2 - Cause of the oldest existing alarm detected*
*3 - Time of the oldest existing alarm detected*

| | |
|---|---|
| `show device-status` | Display the device status and the setting for the device status determination. |

# 8.4 Out-of-band Signaling

The signal contact is used to control external devices and monitor the operation of the device, thus enabling remote diagnostics.
A break in contact is reported by the device via the potential-free signal contact (relay contact, closed circuit):

- Incorrect supply voltage,
  the detected failure of at least one of the two supply voltages,
  a detected failure in the device (internal supply voltage).
- The temperature threshold has been exceeded or has not been reached.
- The removal of the EAM.
- The interrupted connection to at least one port. With the device, the indication of link status can be masked via the management for each port (see on page 84 “Displaying detected connection errors”). On delivery, there is no link monitoring.

The management setting specifies which events switch a contact.

**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 208 “Monitoring the Device Status via the Signal Contact”).

## 8.4.1 Controlling the Signal Contact

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

Application options:

- Simulation of a detected 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` 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 mode manual` | Select the manual setting mode for the signal contact. |
| `signal-contact state open` | Open the signal contact. |
| `signal-contact state closed` | Close the signal contact. |

## 8.4.2 Monitoring Correct Operation 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 also set the temperature thresholds in the `Basic settings:System` dialog at the end of the system data.

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `configure` | Switch to the Configuration mode. |
| `signal-contact monitor temperature enable` | Includes the temperature for the operation monitoring. |
| `signal-contact 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.

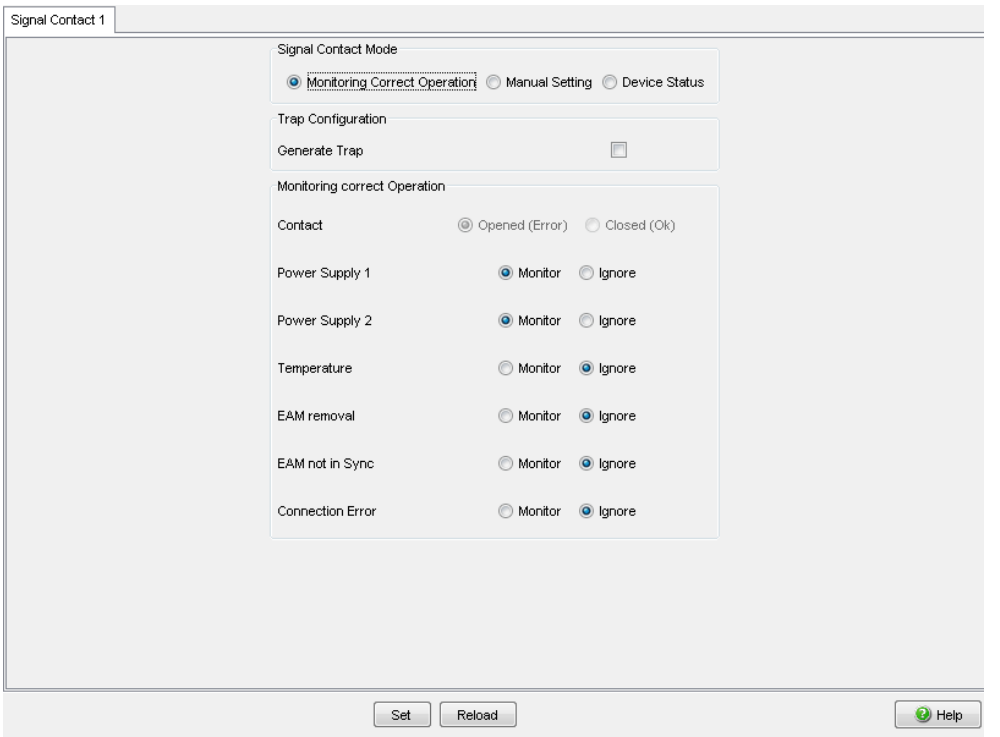



*Figure 53: Signal contact dialog*

`show signal-contact` Displays the status of the operation monitoring and the setting for the status determination.

## 8.4.3 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 202 “Monitoring the Device Status”) via the signal contact.

# 8.5 Port Status Indication

☐ Select the `Basics:System` dialog.
The device view shows the device. Symbols on the ports represent the status of the individual ports.

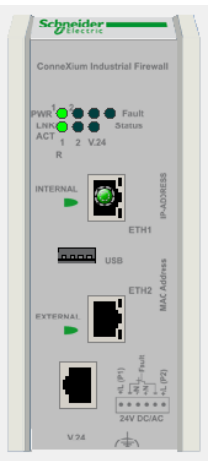



*Figure 54: Device View*

Meaning of the symbols:

The port (10, 100 Mbit/s) is enabled and the link has been established.

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

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

The port is in autonegotiation mode.

The port is in HDX mode.

# 8.6 Network Load and Event Counter at Port Level

## 8.6.1 Network Load

The network load indicates what percentage of the actual data transmission rate available in your network is currently being used. You can use the network load as a simple indicator for the dimensioning of your network. If the average network load is very high for a long period, you should re-dimension the network and, for example, verify that the network has a higher data transmission rate, or that the network load is split up.

To display the network load for each port, you proceed as follows:

☐ Select the `Diagnostics:Ports:Network Load` dialog.

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `show interfaces utilization` | Display the network load as a percentage for port 1 (internal) and port 2 (external). |

## 8.6.2 Port Statistics

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 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.

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

☐ To reset the counters, click on “Reset port counters” in the Basic Settings:Restart dialog.

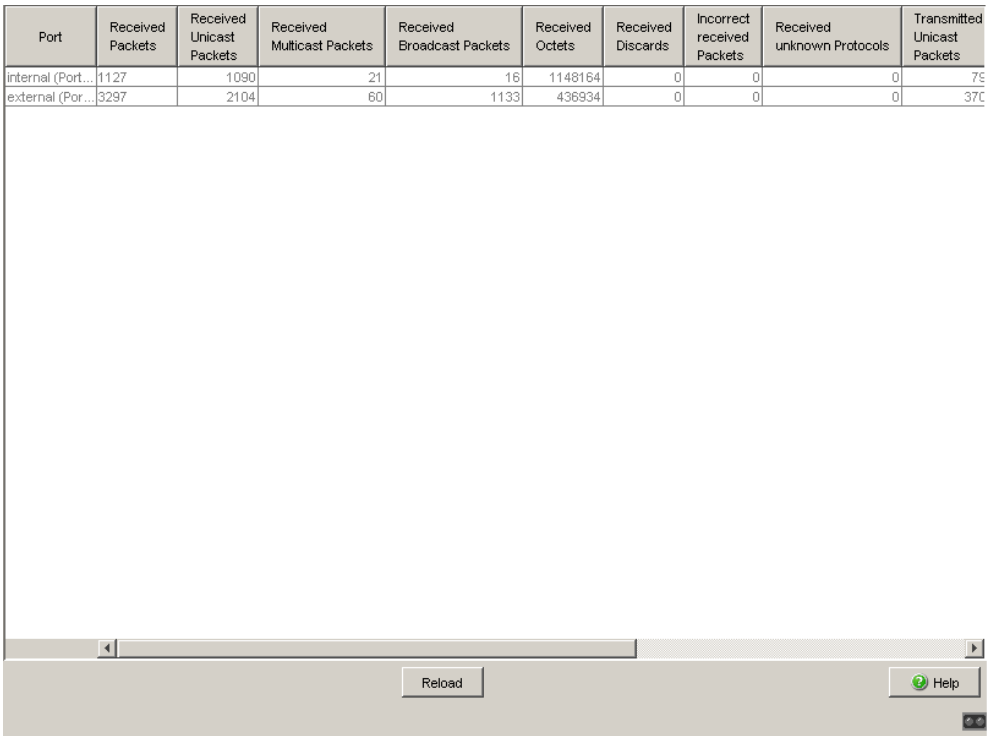



*Figure 55: Displaying port statistics*

```
enable
show interfaces counters
```

Switch to the privileged EXEC mode.
Display the statistic counters for port 1 (internal) and port 2 (external).

The device uses the Address Resolution Protocol (ARP) to determine the MAC address relating to the IP address of a device, and it saves this allocation in the ARP table.

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

☐ To reset the counters, click on “Reset ARP table” in the Basic Settings:Restart dialog.

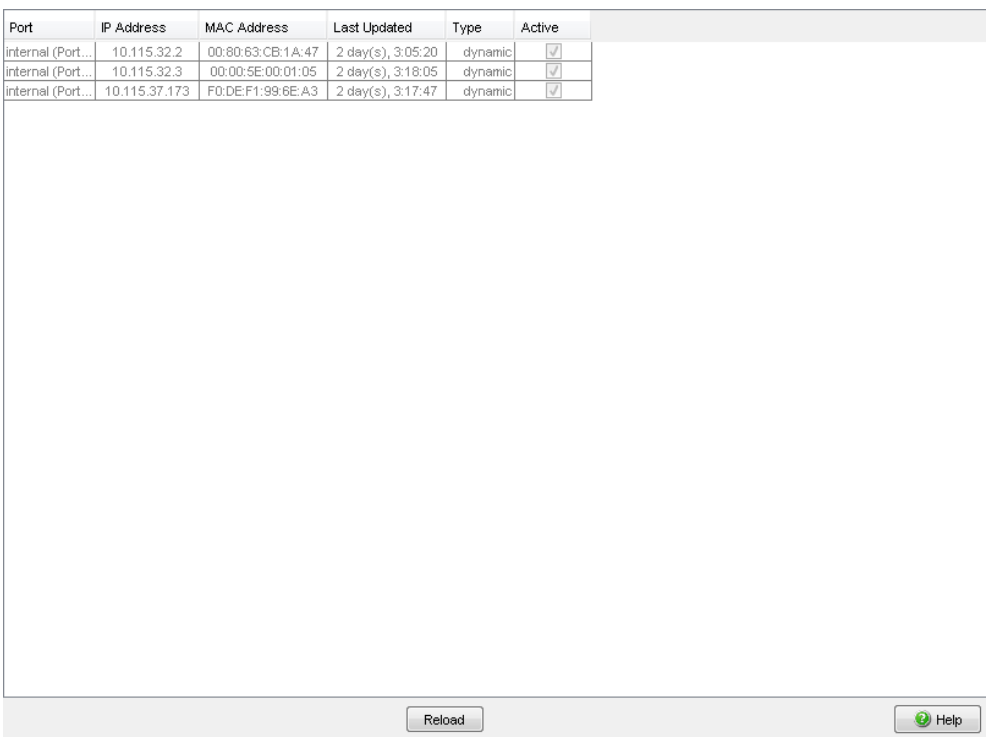



*Figure 56: Example of ARP entries.*

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `show network statistics` | Display the network statistics for port 1 (internal) and port 2 (external), including the ARP entries. |

# 8.7 Topology Discovery

## 8.7.1 Description of Topology Discovery

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

A device with active LLDP

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

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

- Chassis ID (its MAC address)
- Port ID (its port MAC address)
- Description of the port
- System Name
- System description
- Supported system capabilities
- Currently activated system capabilities
- Interface ID of the management address
- Status of the autonegotiation at the port
- Medium, half and full duplex settings and speed setting of the port
- Information about 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. Thus a non-LLDP-capable device between 2 LLDP-capable devices disables 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.

## 8.7.2 Displaying the Topology Discovery Results

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

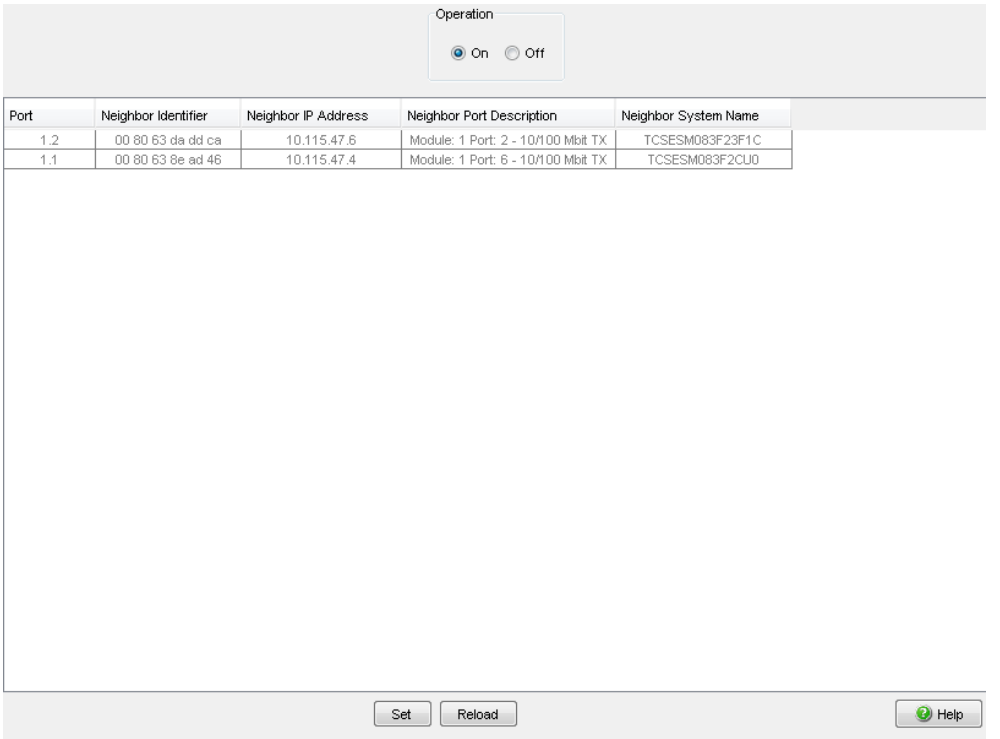



*Figure 57: Topology Discovery*

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

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

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

If
- only devices without active topology discovery are connected to a port, the table will contain one line for this port to represent all devices. This line contains the number of connected devices. IP addresses of devices that the topology table hides for the sake of clarity, are located in the configuration check table (see on page 217 “Configuration Check”) .

# 8.8 Configuration Check

This function allows you to check your configuration after the installation and the configuration. The configuration check also includes the configuration of the neighboring device for the check.
By clicking on a line, you will find details of the result of a check on a port, in the lower part of the dialog.

# 8.9 Reports

The following reports are available for the diagnostics:

- System information.
  The system information is an HTML file containing the system-relevant data.

☐ Select the `Diagnostics:Report` dialog.

☐ Click “System Information” to open the HTML file in the Web-based interface.

# A Setting up the Configuration Environment

# A.1 Access via SSH

The program PuTTY enables you to access your device via SSH.
This program is located on the product CD.

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

Shortly before the connection is set up, PuTTY displays a security alert message and gives you the option of checking the fingerprint of the key.


*Figure 58: Security alert prompt for the fingerprint*

☐ Check the fingerprint to help protect yourself from unwelcome guests.
☐ If the fingerprint matches that of the device key, click “Yes”.

**Note:** Schneider Electric delivers the device with a unique, permanently stored SSH-RSA/DSA device key. This unique key allows you to identify the device in the case of SSH access.

The OpenSSH Suite offers experienced network administrators a further option to access your device via SSH. To set up the connection, enter the following command:

```
ssh admin@10.149.112.53
```

`admin` represents the user name.
`10.149.112.53` is the IP address of your device.

# B General Information

# B.1 Abbreviations used

| | |
|---|---|
| EAM | Memory Backup Adapter |
| ACL | Access Control List |
| AES | Advanced Encryption Standard |
| BOOTP | Bootstrap Protocol |
| CIDR | Classless Inter-Domain Routing |
| CLI | Command Line Interface |
| DHCP | Dynamic Host Configuration Protocol) |
| DES | Data Encryption Standard |
| DN | Distinguished Name |
| GARP | General Attribute Registration Protocol |
| FDB | Forwarding Database |
| FQDN | Fully Qualified Domain Name |
| GMRP | GARP Multicast Registration Protocol |
| HMAC | Hashed Message Authentication Code |
| http | Hypertext Transfer Protocol |
| ICMP | Internet Control Message Protocol |
| IGMP | Internet Group Management Protocol |
| IKE | Internet Key Exchange |
| IP | Internet Protocol |
| IPsec | IP Security |
| LED | Light Emitting Diode |
| LLDP | Link Layer Discovery Protocoll |
| MAC | Media Access Control |
| MD5 | Message Digest 5 |
| MODP | Modular Exponentiation |
| NTP | Network Time Protocol |
| NVM | Non-volatile Memory |
| PC | Personal Computer |
| PTP | Precision Time Protocol |
| QoS | Quality of Service |
| RFC | Request For Comment |
| RM | Redundancy Manager |
| RS | Rail Switch |
| RSTP | Rapid Spanning Tree Protocol |
| SA | Security Association |
| SFP | Small Form-factor Pluggable |
| SHA | Secure Hash Algorithm |
| SNMP | Simple Network Management Protocol |

| | |
|---|---|
| SNTP | Simple Network Time Protocol |
| TCP | Transfer 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 |

# C Index

## U



## V



## W



## X



## d



## o