User manual

UM EN FL NAT SMN 8TX

User manual for the NAT router with integrated switch

PHOENIX CONTACT
INSPIRING INNOVATIONS

User manual

User manual for the NAT router with integrated switch

2016-02-05

Designation: UM EN FL NAT SMN 8TX

Revision: 04

Order No.: —

This user manual is valid for:

Designation	Version	Order No.
FL NAT SMN 8TX		2989365
FL NAT SMN 8TX-M		2702443

Please observe the following notes

User group of this manual

The use of products described in this manual is oriented exclusively to:

- Qualified electricians or persons instructed by them, who are familiar with applicable standards and other regulations regarding electrical engineering and, in particular, the relevant safety concepts.
- Qualified application programmers and software engineers, who are familiar with the safety concepts of automation technology and applicable standards.

Explanation of symbols used and signal words

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

There are three different categories of personal injury that are indicated with a signal word.

DANGER This indicates a hazardous situation which, if not avoided, will result in death or serious injury.

WARNING This indicates a hazardous situation which, if not avoided, could result in death or serious injury.

CAUTION This indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

This symbol together with the signal word **NOTE** and the accompanying text alert the reader to a situation which may cause damage or malfunction to the device, hardware/software, or surrounding property.

This symbol and the accompanying text provide the reader with additional information or refer to detailed sources of information.

How to contact us

Internet

Up-to-date information on Phoenix Contact products and our Terms and Conditions can be found on the Internet at:
www.phoenixcontact.com

Make sure you always use the latest documentation.
It can be downloaded at:
www.phoenixcontact.net/catalog

Subsidiaries

If there are any problems that cannot be solved using the documentation, please contact your Phoenix Contact subsidiary.
Subsidiary contact information is available at www.phoenixcontact.com.

Published by

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
GERMANY

Should you have any suggestions or recommendations for improvement of the contents and layout of our manuals, please send your comments to:
tecdoc@phoenixcontact.com

General terms and conditions of use for technical documentation

Phoenix Contact reserves the right to alter, correct, and/or improve the technical documentation and the products described in the technical documentation at its own discretion and without giving prior notice, insofar as this is reasonable for the user. The same applies to any technical changes that serve the purpose of technical progress.

The receipt of technical documentation (in particular user documentation) does not constitute any further duty on the part of Phoenix Contact to furnish information on modifications to products and/or technical documentation. You are responsible to verify the suitability and intended use of the products in your specific application, in particular with regard to observing the applicable standards and regulations. All information made available in the technical data is supplied without any accompanying guarantee, whether expressly mentioned, implied or tacitly assumed.

In general, the provisions of the current standard Terms and Conditions of Phoenix Contact apply exclusively, in particular as concerns any warranty liability.

Phoenix Contact reserves the right to register its own intellectual property rights for the product identifications of Phoenix Contact products that are used here. Registration of such intellectual property rights by third parties is prohibited.

Other product identifications may be afforded legal protection, even where they may not be indicated as such.

Table of contents

1 FL NAT SMN 8TX(-M)

1.1 Properties

The NAT router combines routing and switching functions in a single device. The FL NAT SMN 8TX(-M) can be used to provide individual machines with the same IP addresses and to then translate these IP addresses to the IP address areas of the higher-level company network that are required for the application. This function is usually referred to as 1-to-1 NAT (1:1 NAT - Network Address Translation). Port 1 is the port via which the 1:1 NAT implementation takes place in the higher-level network. Ports 2 to 8 are standard switch ports for the lower-level network.

In addition to IP address translation, the FL NAT SMN 8TX(-M) provides several switch ports (port 2 to port 8) in the lower-level machine network. In addition to the switch and routing function, further (IT) functions are available, such as redundancy, port mirroring or LLDP.

The FL NAT SMN 8TX(-M) can be configured via a web server and via SNMP (Simple Network Management Protocol). A serial terminal interface is also available for initial startup.

Figure 1-1 The FL NAT SMN 8TX(-M)

Future-proof networks for the highest demands

Maximum performance 10/100 Mbps on each RJ45 port

Maximum availability Maximum network availability
A device design that does not use a fan, the redundant power supply, and conformance with all relevant industrial standards in terms of EMC, climate, mechanical load, etc. ensure the highest possible level of availability.

Quick media redundancy Redundancy can be created with standards: the Rapid Spanning Tree Protocol ensures the safe operation of the entire network regardless of topology, even in the event of a cable interrupt.

All information

Clear information
Two LEDs per port with switchable information ensure that you always have sufficient local information. A web server and an SNMP agent are provided for diagnostics, maintenance, and configuration via the network. A terminal access point can be used for local operation.

Port mirroring

Port mirroring can be used to monitor data traffic on the network connections or as an important service function.

Features and fields of application of the FL NAT SMN 8TX(-M)

- Use of different routing modes
  - Virtual NAT,
  - 1:1 NAT
  - Static routing
- Increased network performance by filtering data traffic:
  - Local data traffic remains local.
  - The data volume in network segments is reduced.
- Easy network expansion and network configuration.
- Coupling copper segments with different transmission speeds.
  Automatic detection of 10 Mbps or 100 Mbps data transmission speed with autocrossing.
- Support of various topologies and meshed structures as well as ring topologies with special ring detection.
- Configuration of the switch using web-based management, SNMP or locally via an RS-232 interface.
- Port mirroring
- Topology detection using LLDP (Link Layer Discovery Protocol).
- Address assignment via BootP, DHCP or statically.
- Diagnostic/status indicators
  Important information is displayed directly on the device. Each port has two LEDs. The "LNK" LED always indicates the "LINK", while the other LED display is set with the "MODE" function switch.
- MODE switch for LEDs
  The MODE switch can be used to specify which information is displayed by the second port-specific LED. The three LEDs below the switch indicate the selected mode. This information is then displayed by all port-specific LEDs (see also example on page 1-4).
- Mini-DIN RS-232
  RS-232 interface in Mini-DIN format for local configuration via the serial interface.
- Supply voltage connection
  The supply voltage can be connected via four positions of the 6-pos. COMBICON connector (redundancy is optional); the floating alarm contact can be connected via the remaining two positions.

1.1.1 Dimensions of the FL NAT SMN 8TX(-M)

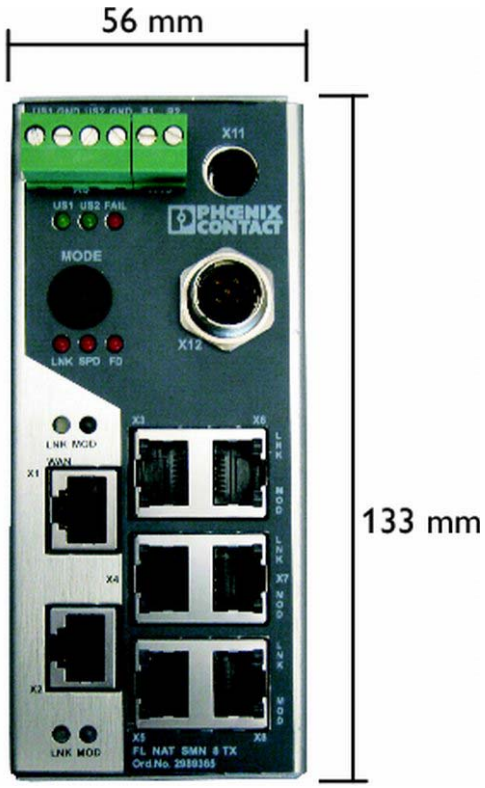


Figure 1-2 Housing dimensions of the FL NAT SMN 8TX(-M) in millimeters

Depth from top edge of DIN rail including MEM PLUG: 175 mm

1.2 Status and diagnostic indicators

Des.	Color	Status	Meaning
US1	Green	ON	Supply voltage 1 in the tolerance range
		OFF	Supply voltage 1 too low
US2	Green	ON	Supply voltage 2 in the tolerance range
		OFF	Supply voltage 2 too low
FAIL	Red	ON	Alarm contact open, i.e., an error has occurred
		OFF	Alarm contact closed , i.e., an error has not occurred

Des.	Color of MODE LED at the port	Status	Meaning
An additional LED is located on the front of the FL NAT SMN 8TX(-M) for each port. The function of the second LED (MOD) for each port can be set using the MODE switch (see also example below). There are three options (during the boot process the Link LEDs of the ports are permanently on):			
LNK (Link)	Green	ON	Transmitting/receiving telegrams
		OFF	Not transmitting/receiving telegrams
SPD (Speed)	Green	ON	100 Mbps
		OFF	10 Mbps if Link LED is active at the port
FD (Duplex)	Green	ON	Full duplex
		OFF	Half duplex
ACT/SPD/FD	Green	Flashing	Switch is in Smart mode

Example:

In Figure 1-3, the LED indicators have the following meaning:

A: The MODE switch has been set to display the duplex mode (FD); the mode LED now indicates that the port is in full duplex mode.

B: The switch has been set to display the data transmission rate (SPD); the mode LED now indicates that the port is operating at 100 Mbps.

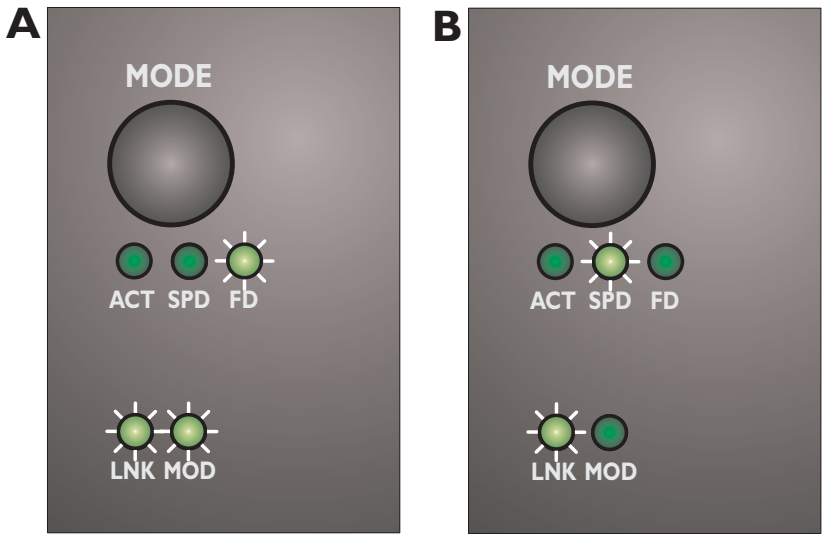


Figure 1-3 Example for status indicators

2 Mounting and installation

2.1 Mounting and removing the FL NAT SMN 8TX(-M)

Mount the FL NAT SMN 8TX(-M) on a clean DIN rail according to DIN EN 50022 (e.g., NS 35... from Phoenix Contact). To avoid contact resistance, only use clean, corrosion-free DIN rails. End clamps (E/NS 35N, Order No. 0800886) can be mounted to the right and left of the device to stop the modules from slipping on the DIN rail.

Mounting:

1 Place the module onto the DIN rail from above (A). The upper holding keyway of the module must be hooked onto the top edge of the DIN rail. Push the module from the front towards the mounting surface (B).

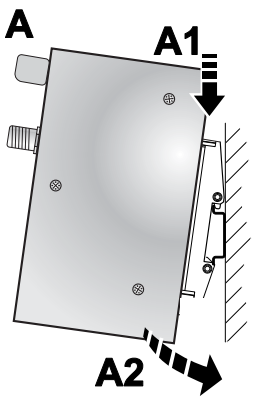


Figure 2-1 Snapping the FL NAT SMN 8TX(-M) onto the DIN rail

2 Once the module has been snapped on properly, check that it is fixed securely on the DIN rail. Check whether the positive latch is facing upwards, i.e., snapped on correctly.

Removal:

1 Pull down the positive latch using a suitable tool (e.g., screwdriver). The positive latch remains snapped out. Then swivel the bottom of the module away from the DIN rail slightly (A). Next, lift the module upwards away from the DIN rail (B).

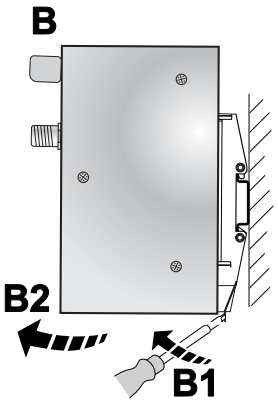


Figure 2-2 Removing the FL NAT SMN 8TX(-M)

2.2 Installing the FL NAT SMN 8TX(-M)

2.2.1 Connecting the 24 V DC supply voltage

The FL NAT SMN 8TX(-M) is operated using a 24 V DC voltage, which is applied via COMBICON. If required, the voltage can also be supplied redundantly (see Figure 2-4).

If redundant power supply monitoring is active (default setting), an error is indicated if only one voltage is applied. A bridge between US1 and US2 prevents this error message. It is also possible to deactivate monitoring in web-based management or via SNMP.

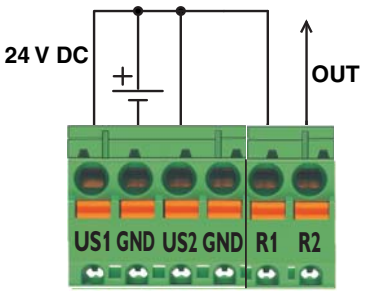


Figure 2-3 Supplying the FL NAT SMN 8TX(-M) using one voltage source

Redundant 24 V DC supply

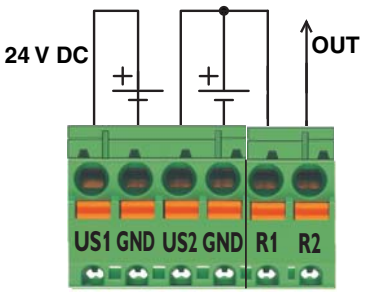


Figure 2-4 Supplying the FL NAT SMN 8TX(-M) using two voltage sources

In order to reset the FL NAT SMN 8TX(-M) on power up, the power supply must be interrupted for at least 3 seconds.

2.2.2 Alarm contact

The FL NAT SMN 8TX(-M) has a floating alarm contact. When opening the contact, an error is reported.

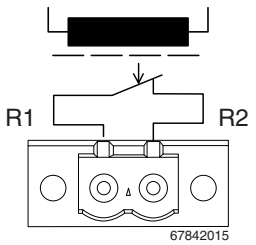


Figure 2-5 Basic circuit diagram for the alarm contact

The indicated error states are configured in web-based management or via SNMP. For a list of error states that can be configured, please refer to Section ""Diagnostics/Alarm Contact" Menu" on page 4-26.

In the event of non-redundant power supply, the device indicates a supply voltage failure by opening the alarm contact. This error message can be prevented by connecting the supply voltage to both terminal blocks in parallel, as shown in Figure 2-3, or by deactivating redundant power supply monitoring in web-based management or via SNMP.

2.2.3 Assignment of the RJ45 Ethernet connectors

Table 2-1 Pin assignment of RJ45 connectors

Pin number	10Base-T/10 Mbps	100Base-T/100 Mbps
1	TD+ (Transmit)	TD+ (Transmit)
2	TD- (Transmit)	TD- (Transmit)
3	RD+ (Receive)	RD+ (Receive)
4	-	-
5	-	-
6	RD- (Receive)	RD- (Receive)
7	-	-
8	-	-

2.2.4 RS-232 interface for external management

The 6-pos. Mini-DIN female connector provides a serial interface to connect a local management station. It can be used to connect a VT100 terminal or a PC with corresponding terminal emulation to the management interface (for an appropriate cable, please refer to page 8-3). Set the following transmission parameters:

Bits per second	38400
Data bits	8
Parity	None
Stop bits	1
Flow control	None

RS-232 (V.24) interface

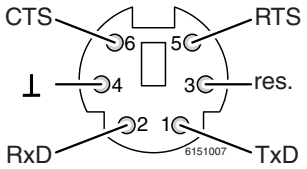


Figure 2-6 Transmission parameters and assignment of the RS-232 interface

2.3 Grounding

Grounding protects people and machines against hazardous voltages. To avoid these dangers, correct installation, taking the local conditions into account, is vital.

All Factoryline devices must be grounded so that any possible interference is shielded from the data telegram and discharged to ground potential.

A conductor of at least 2.5 mm^2 must be used for grounding. When mounting on a DIN rail, the DIN rail must be connected to protective earth ground via grounding terminal blocks. The module is connected to protective earth ground via the metal base element.

3 Startup and functions

3.1 Configuration

3.1.1 Assigning IP parameters at the WAN interface (port 1)

After the connection has been established between the WAN interface and the network, the NAT router is started. By default upon delivery, the NAT router starts without an IP configuration at the WAN port. It cyclically sends a DHCP discover as broadcast requests to a DHCP server in the local network (company network). The server responds to the requests with a DHCP offer, which contains the requested parameters. The device can then be accessed via the IP parameters that have been assigned via DHCP.
The “IPAssign.exe” addressing tool, which is available free of charge, can be used to assign the IP parameters (see “IP address assignment using IPAssign.exe” on page 3-2).
The IP parameters of the WAN port can be configured statically via the RS-232 interface using the password.

Modifications can only be made by entering the valid password. By default upon delivery, the password is “private”.

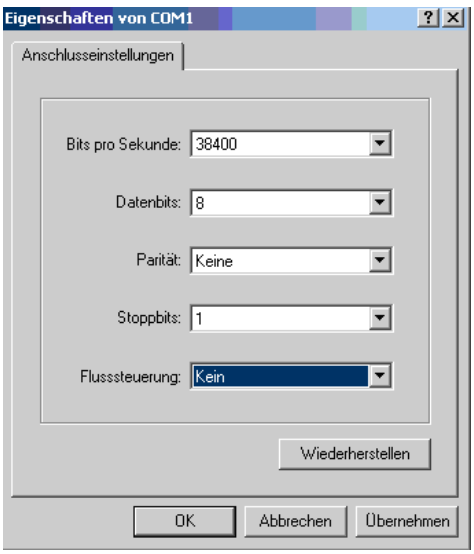


Figure 3-1 Serial interface settings

A local communication connection can be established to an external management station via the RS-232 interface in Mini-DIN format. The “PRG CAB MINI DIN” programming cable, Order No. 2730611, should be used for this. Communication is established using a corresponding emulation between the NAT router and a PC (e.g., HyperTerminal under Windows) and thus enables access to the user interface.

The IP parameters of the WAN port can now be modified via the RS-232 interface using the password.

3.1.2 Assigning IP parameters at the LAN interface (port 2 to port 8)

By default upon delivery, the NAT router starts without an IP configuration at the LAN port. It sends BootP requests cyclically, which are answered by a BootP server with a corresponding BootP reply.

The “IPAssign.exe” addressing tool, which is available free of charge, can be used to assign the IP parameters (see “IP address assignment using IPAssign.exe” on page 3-2).

3.1.3 IP address assignment using IPAssign.exe

Step 1: downloading and executing the program

- On the Internet, select the link www.phoenixcontact.net/catalog.
- Enter the order number 2832700 in the search field, for example.

The IP addressing tool can be found under “Configuration file”.

- Double-click on the “IPAssign.exe” file.
- In the window that opens, click on “Run”.

Step 2: “IP Assignment Wizard”

The program opens and the start screen of the addressing tool appears.

The program is mostly in English for international purposes. However, the program buttons change according to the country-specific settings.

The start screen displays the IP address of the PC. This helps when addressing the device in the following steps.

- Click on “Next”.

Step 3: “IP Address Request Listener”

All devices sending a BootP request are listed in the window which opens. These devices are waiting for a new IP address.

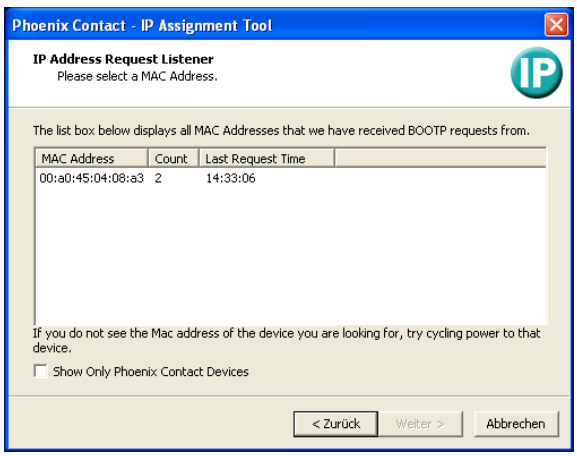


Figure 3-2 “IP Address Request Listener” window

In this example, the device has MAC address 00.A0.45.04.08.A3.

- Select the device to which you would like to assign an IP address.
- Click on “Next”.

Step 4: “SeT IP Address”

The following information is displayed in the window which opens:

– IP address of the PC
– MAC address of the selected device
– IP parameters of the selected device
(IP address, subnet mask, and gateway address)
– Any incorrect settings

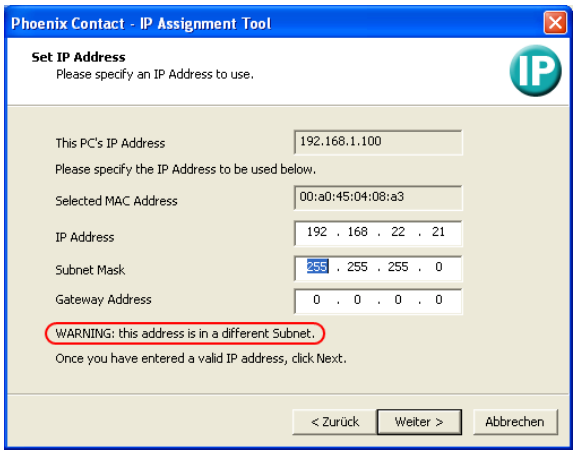


Figure 3-3 "Set IP Address" window with incorrect settings

- Adjust the IP parameters according to your requirements.

If inconsistencies are no longer detected, a message appears indicating that a valid IP address has been set.

- Click on “Next”.

Step 5: “Assign IP Address”

The program transmits the parameters set to the device.

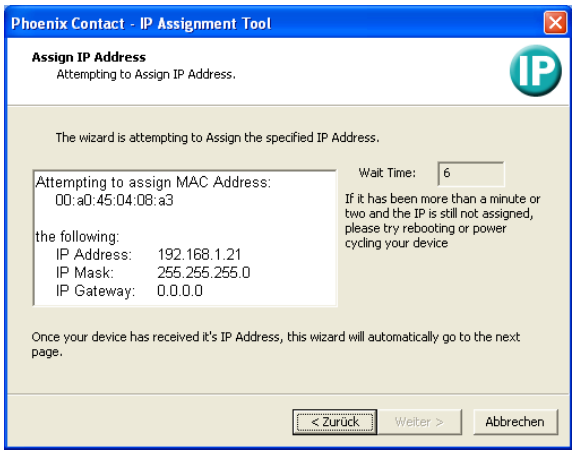


Figure 3-4 “Assign IP Address” window

Following successful transmission, the next window opens.

Step 6: finishing IP address assignment

The window that opens informs you that IP address assignment has been successfully completed. It gives an overview of the IP parameters that have been transmitted to the device with the MAC address shown.

To assign IP parameters for additional devices:

- Click on “Back”.

To exit IP address assignment:

- Click on “Finish”.

3.2 Frame switching at ports 2 - 8

Devices in the company network (WAN) can access IP addresses of machines (at ports 2 - 8) in the production cell (LAN) without additional configuration. The FL NAT SMN 8TX(-M) operates in store-and-forward mode. When receiving a data packet, the switch analyzes the source and destination addresses. The switch stores up to 4000 MAC addresses with an adjustable aging time of 10 to 825 seconds in its address table.

3.2.1 Store-and-forward

All data telegrams received by the switch are stored and checked for validity. Invalid or faulty data packets (> 1522 bytes or CRC errors) and fragments (< 64 bytes) are rejected. Valid data telegrams are forwarded by the switch.

3.2.2 Multi-address function

The switch learns all the source addresses for each port. Only packets with:

– Unknown source addresses
– A source address for this port
– A multicast/broadcast address

in the destination address field are forwarded via the relevant port. The switch can learn up to 4000 addresses. This is important when more than one termination device is connected to one or more ports. In this way, several independent subnetworks can be connected to one switch.

3.2.3 Learning addresses

The FL NAT SMN 8TX(-M) independently learns the addresses for termination devices, which are connected via a port, by evaluating the source addresses in the data telegram. When the switch receives a data telegram, it only forwards this data telegram to the port that connects to the specified device (if the address could be learned beforehand).
The FL NAT SMN 8TX(-M) can learn up to 4000 addresses and store them in its table. The switch monitors the age of the learned addresses. The switch automatically deletes from its address table address entries that have exceeded a specific age (default: 40 seconds, adjustable from 10 to 825 seconds, aging time).

All learned entries are deleted on a restart.
A link down deletes all the entries of the affected port.

A list of detected MAC addresses can be found in the MAC address table (see Section ““Diagnostics/Mac Address Table” menu” on page 4-29). The MAC address table can be deleted via "Clear".

The aging time is set using the "dot1dTpAgingTime"
MIB object (OID 1.3.6.1.2.1.17.4.2). The available setting range is 10 - 825 seconds. For static configuration, an aging time of 300 seconds is recommended.

3.2.4 Prioritization

The switch supports four priority queues (traffic classes according to IEEE 802.1D) for adjusting the internal packet processing sequence. Data telegrams that are received are assigned to these classes according to their priority, which is specified in the prioritization tag:

– Data packets with the value “0” or “1” in the priority field have the lowest priority (default).
– Data packets with the value “2” or “3” in the priority field have the second lowest priority.
– Data packets with values between “4” and “5” in the priority field have the second highest priority and are transmitted via the switch.
– Data packets with values between “6” and “7” in the priority field have the highest priority and are transmitted via the switch.

Processing rules

The switch controller in the FL NAT SMN 8TX(-M) forwards received packets to one of the receive queues according to the following decisions:

– BPDU packets are always assigned to the high-priority queue.
– Packets with prioritization tag are forwarded according to the queues listed above.
– All residual data is assigned to the low-priority queue.

3.3 Network connection

The company network must be connected to the WAN port (port 1).

3.4 Configuration and diagnostics

The FL NAT SMN 8TX(-M) offers several user interfaces for accessing management features. The preferred interfaces are the web interface and SNMP interface.

Das WEB-Interface erreicht man durch Eingabe der WAN- oder LAN-IP-Adresse in einem Browser, z.B. Internet Explorer, Mozilla Firefox, o. ä.

The SNMP interface can be accessed via corresponding SNMP tools, e.g., MG Soft MIB Browser.

Using the password, all configuration settings can be made and information read via the web interface.

Modifications can only be made by entering the valid password. By default upon delivery, the password is “private”.

Access via SNMP is only possible using the password.

In addition to the recommended interfaces, access is also possible via the RS-232 interface using the password. However, this interface only provides access to basic configuration settings.

Protected data cannot be accessed using the password.

3.5 Using Smart mode

Smart mode enables the user to reset the switch to its default settings without having to access the management interfaces.

The switch offers the following setting options via Smart mode:

– Reset to the default settings
– Exit Smart mode without changes

3.5.1 Activating Smart mode

The mode button is used to call/exit Smart mode and to select the desired setting. The three mode LEDs indicate the mode that is currently set and the mode that is entered when exiting Smart mode.

3.5.1.1 Calling Smart mode

- Once the switch has booted, as soon as the three mode LEDs go out press and hold down the mode button for at least five seconds. When Smart mode is active, the three LEDs flash.
- When Smart Mode is started, the switch is initially in the "Exit without changes" state.

3.5.1.2 Selecting the desired setting

- To select the various settings, press the mode button briefly and select the desired operating mode according to Table 3-1.

Table 3-1 Operating modes in Smart mode

Mode	ACT LED 1	SPD LED 2	FD LED 3
Exit Smart mode without changes	OFF	OFF	**ON**
Reset to the default settings	OFF	**ON**	OFF

3.5.1.3 Exiting Smart mode

- To exit, press and hold down the mode button for at least five seconds.

3.5.2 Default settings

The mode button can be used to reset the NAT router to the settings default upon delivery. Use Smart mode as described in Section 3.5 on page 3-7. The NAT router takes a few seconds to restart automatically.

4 Configuration and diagnostics

The FL NAT SMN 8TX(-M) offers several user interfaces for accessing configuration and diagnostic data. The preferred interfaces are the web interface and SNMP interface. These two interfaces can be used to make all necessary settings and request all information. Access via the RS-232 interface only enables access to basic information and supports basic configuration. However, the RS-232 interface also enables firmware update via TFTP in the event of faulty firmware.

Settings are not automatically saved permanently. The active configuration can be saved permanently by selecting “Save current configuration” on the “Configuration Management” web page. Additional saving options are also available via SNMP or RS-232.

4.1 Web-based management (WBM)

4.1.1 General function

Online diagnostics

The user-friendly web-based management interface can be used to manage the switch from anywhere in the network using a standard browser. Comprehensive configuration and diagnostic functions are clearly displayed on a graphical user interface. Every user with a network connection to the device has read access to that device via a browser. A wide range of information about the device itself, set parameters, and the operating state can be viewed.

Modifications can only be made by entering the valid password. By default upon delivery, the password is “private”.

For security reasons, we recommend changing the existing password to a new one known only to you.

4.1.2 Requirements for the use of WBM

As the web server operates using the Hyper Text Transfer Protocol, a standard browser can be used. Access is via the URL “http://IP address of the device”.
Example: http://172.16.29.112.For full operation of the web pages, the browser must support JavaScript 1.2 and Cascading Style Sheets Level 1. We recommend the use of Microsoft Internet Explorer > 6.0.

WBM can only be called using a valid IP address. By default, the switch has **no** valid IP address.

Settings are not automatically saved permanently. If the active configuration has not been saved, a flashing floppy disk icon appears in the top-right corner in WBM. The icon is linked to the “Configuration Management” web page. The active configuration can be saved permanently by selecting “Save current configuration” on this web page.

If the connection is interrupted during transmission of web pages, a waiting time of several minutes must be observed before the web interface can be accessed again.

4.1.2.1 Password concept

After having entered the valid password, no further entry of the password is necessary for a period of 300 s (default). After this period of time has elapsed or after clicking on “Logout”, the password must be re-entered.

The concept is valid for the first ten users logged in simultaneously. All other users must confirm each configuration modification by entering the password, until less than ten users are logged in.

4.1.3 Functions/information in WBM

The navigation tree provides direct access to the following four areas:

– **General Instructions**
  Basic information about WBM.
– **Device Information**
  General device information.
– **General Configuration**
  Device configuration/device as a network device.
– **Switch Station**
  Device-specific configuration and diagnostics.

4.1.3.1 Start page for web-based management (WBM)

After entering the current IP address, access is provided to the device web server and the start page is displayed.

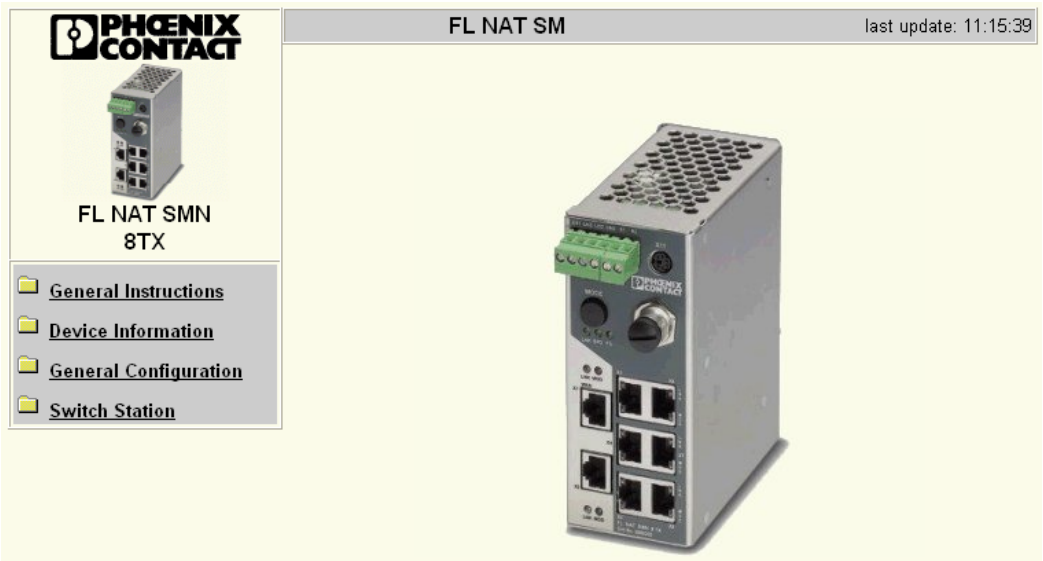


Figure 4-1 Start page for web-based management

4.1.3.2 General Instructions

Contains a brief description of WBM (information) and a navigation tree (site map), which is linked to every page of WBM. The site map can be used to jump directly to the desired page.

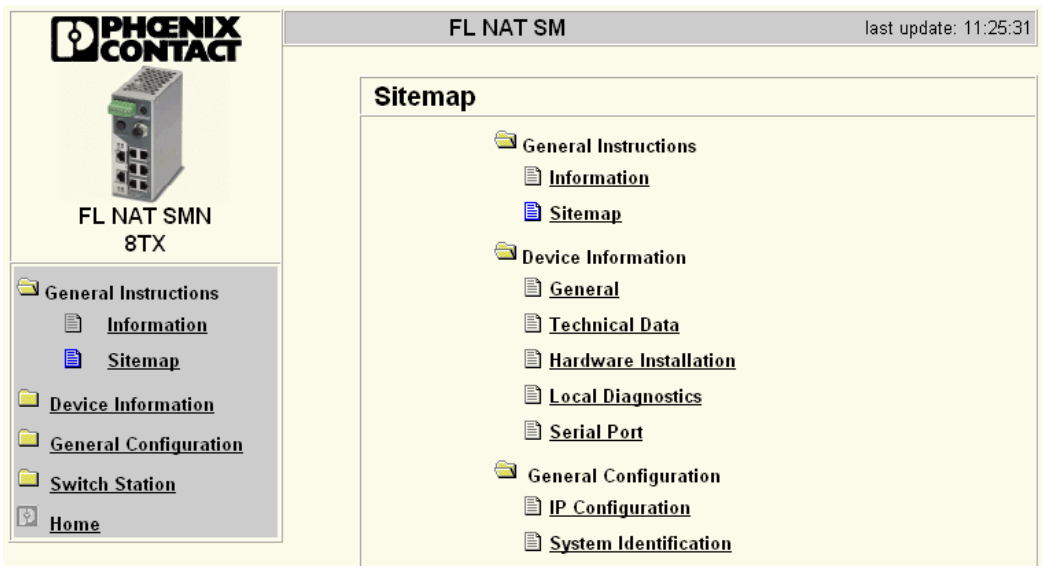


Figure 4-2 "Sitemap" web page for the FL NAT SMN 8TX(-M)

4.1.3.3 Device Information

“General” menu

This page contains a range of static information about the device and the manufacturer, as well as some user-specific settings.

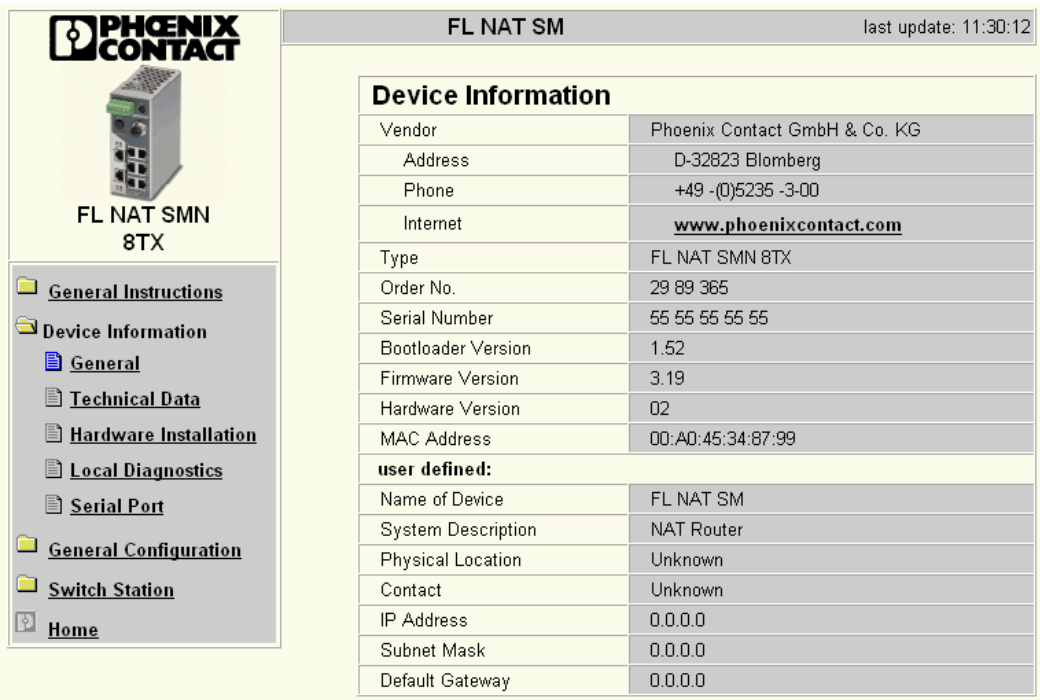


Figure 4-3 “Device Information/General” web page

“Technical Data” menu

This page lists the main technical data.

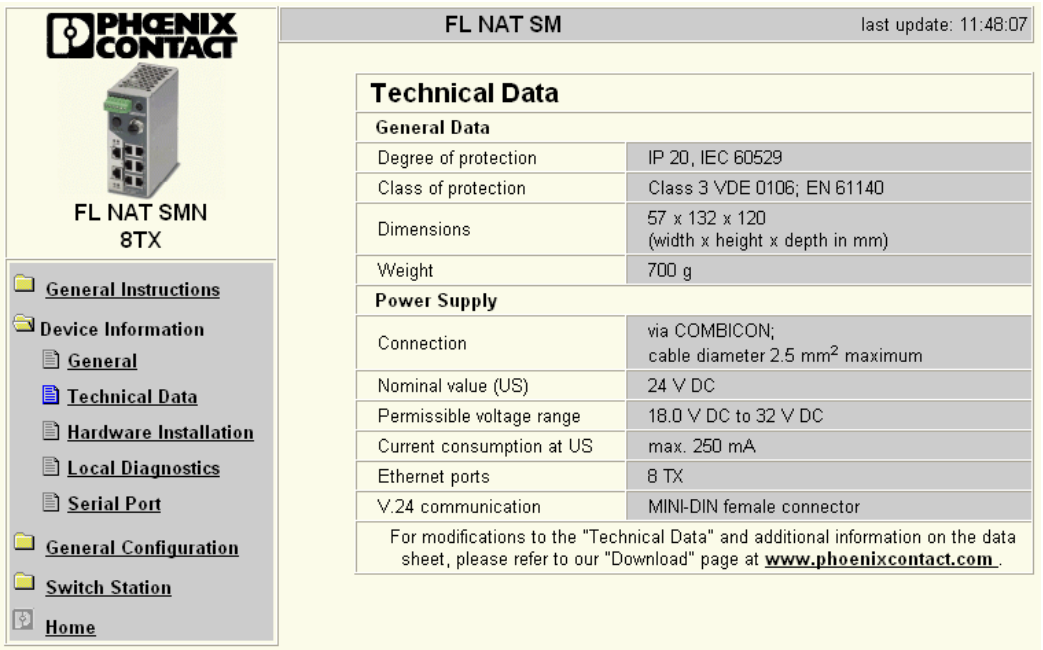
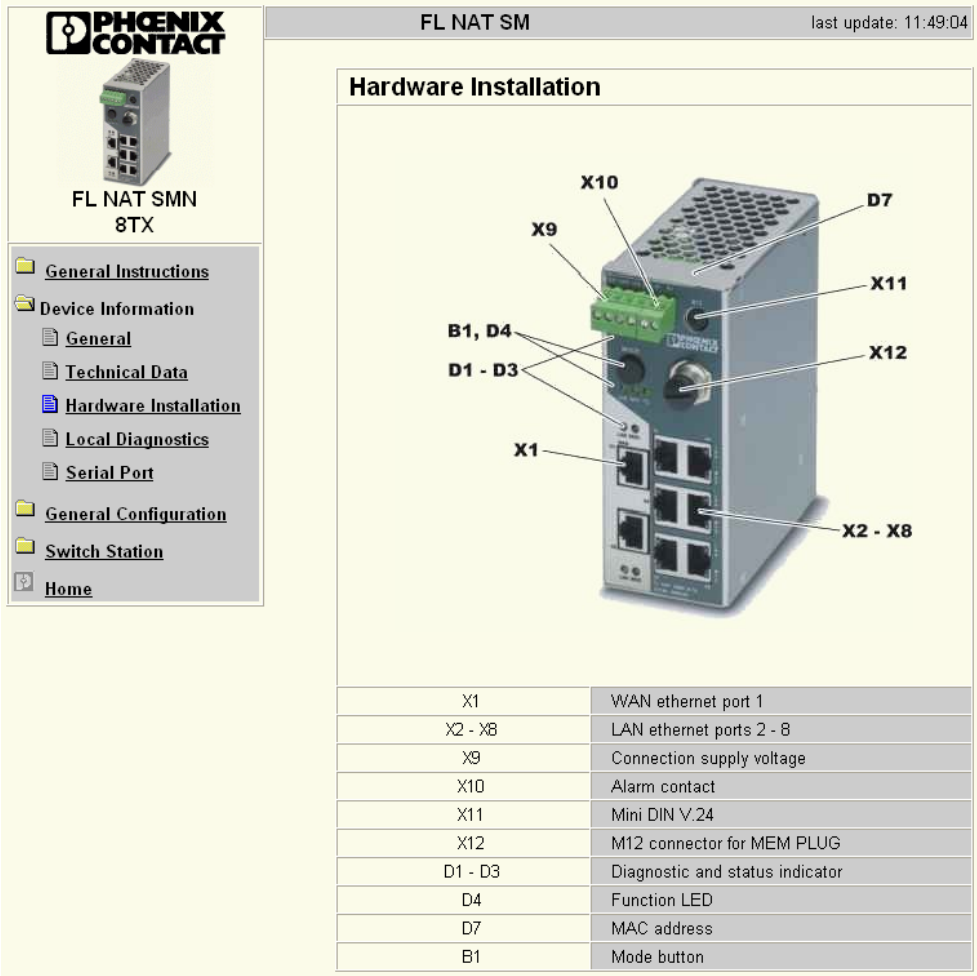


Figure 4-4 “Technical Data” web page

“Hardware Installation” menu

Here you will find a diagram that lists all the elements of the device.



X1	WAN ethernet port 1
X2 - X8	LAN ethernet ports 2 - 8
X9	Connection supply voltage
X10	Alarm contact
X11	Mini DIN V.24
X12	M12 connector for MEM PLUG
D1 - D3	Diagnostic and status indicator
D4	Function LED
D7	MAC address
B1	Mode button

Figure 4-5 “Hardware Installation” web page

“Local Diagnostics” menu

This page describes the meaning of the switchable diagnostic and status indicators.

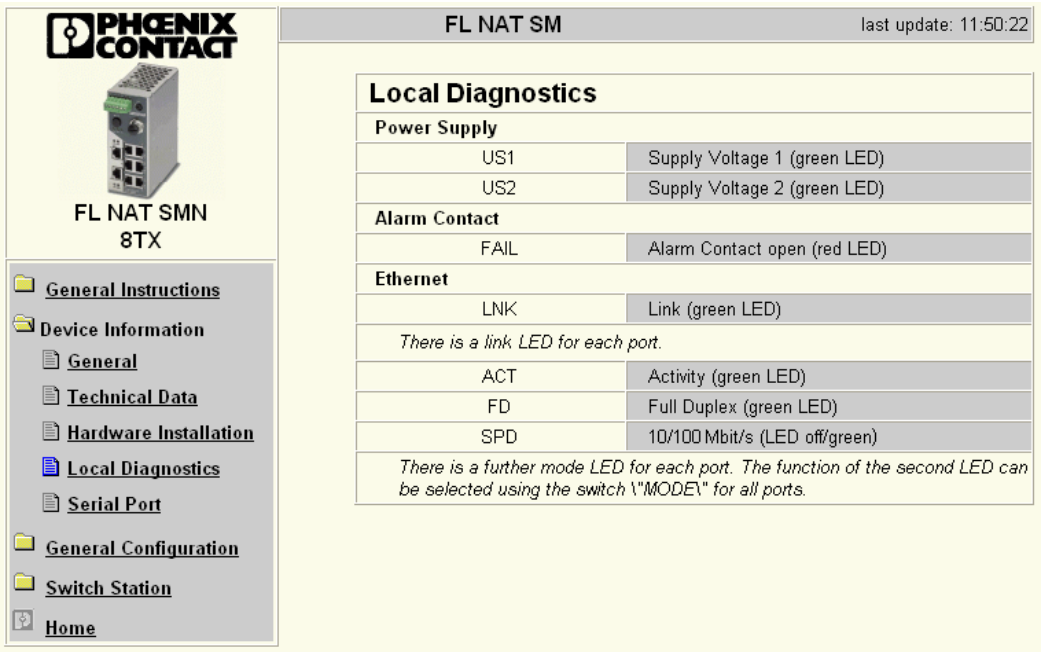


Figure 4-6 “Local Diagnostics” web page

“Serial Port” menu

This page lists the transmission parameters for serial communication.

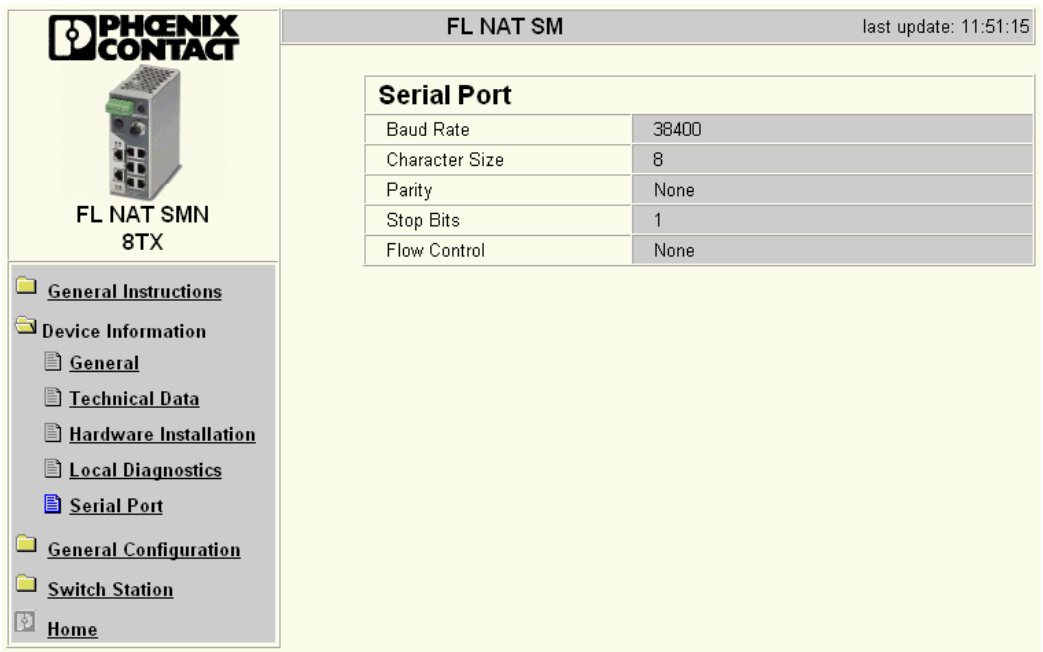


Figure 4-7 “Serial Port” web page

4.1.3.4 General Configuration

This page displays the set IP parameters and addressing mechanism. This page displays the parameters of both the WAN port and the LAN port.

To change the IP parameters via WBM, “Static” assignment must be selected.

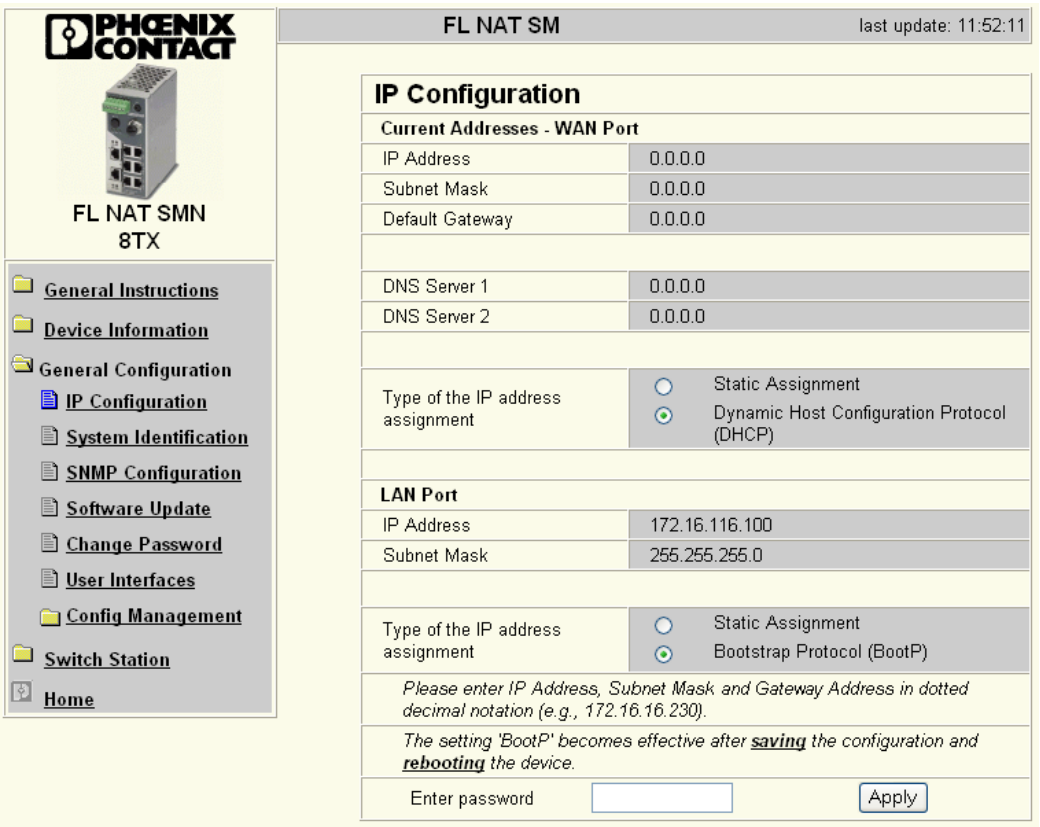


Figure 4-8 “IP Configuration” web page

“System Identification” menu

This menu is used to display or modify user-specific device data, e.g., location, device name or function. This device data is also available in SNMP.

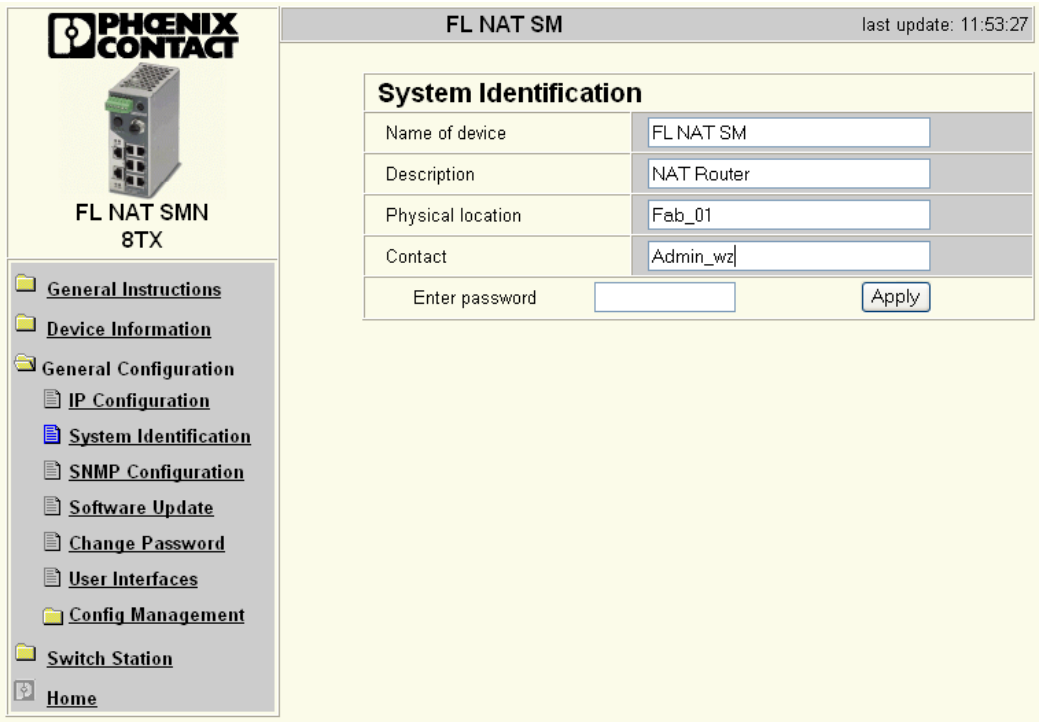


Figure 4-9 “System Identification” menu

“SNMP Trap Configuration” menu

SNMP Agent

The “Sending traps” function can be globally enabled/disabled here.

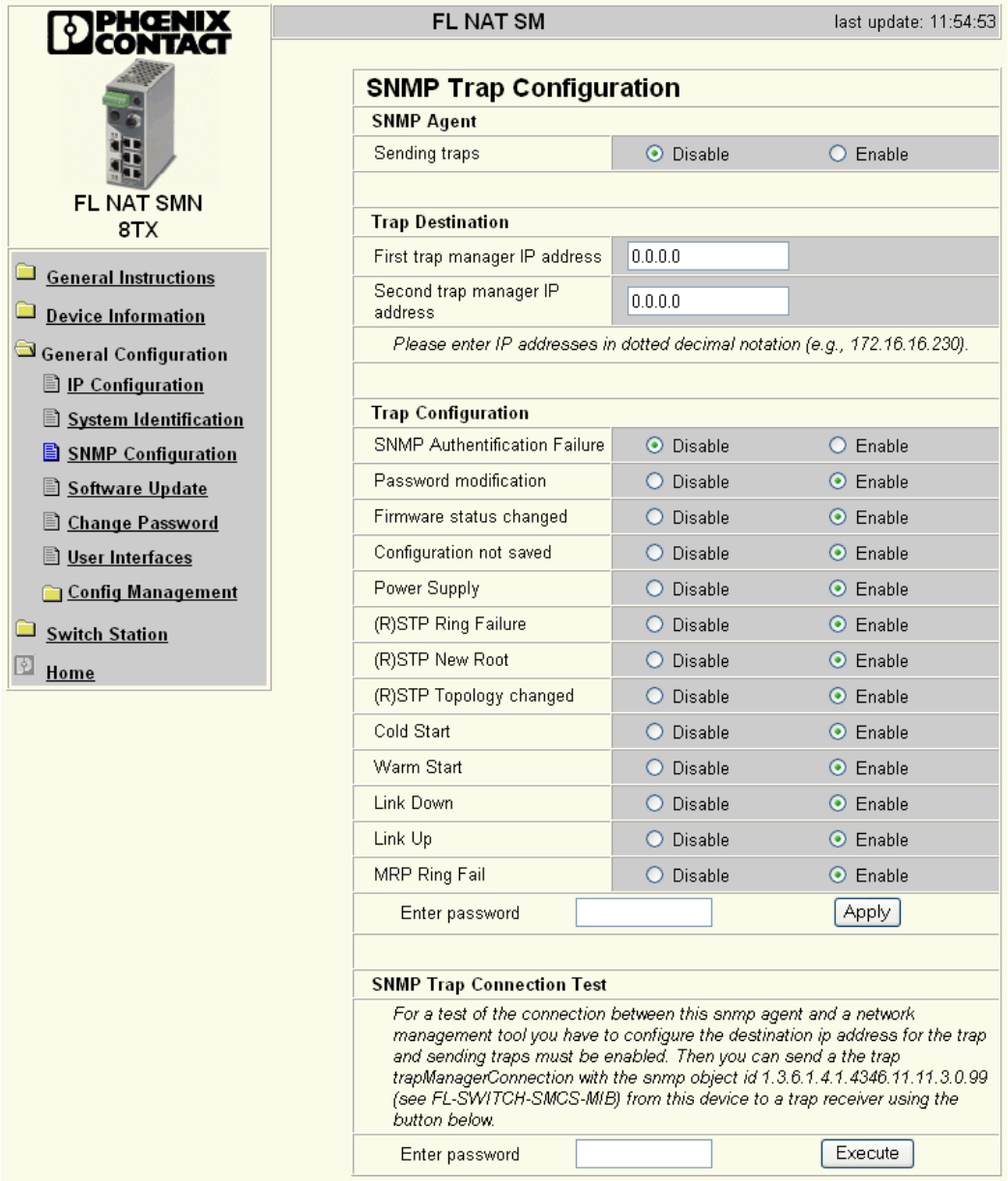


Figure 4-10 “SNMP Configuration” web page

Trap Destination This part of the table is used to view or modify the IP addresses of the two trap receivers.

Trap Configuration Sending of traps can be individually enabled/disabled here.

SNMP Trap Connection Test Once the “Sending traps” function has been activated and the trap managers have been defined using the IP addresses, test traps can now be sent using “Execute” to test the communication path from the switch to the trap receiver.

“Software Update” menu

This page is used to view or modify the parameters for a software update and to trigger the update.

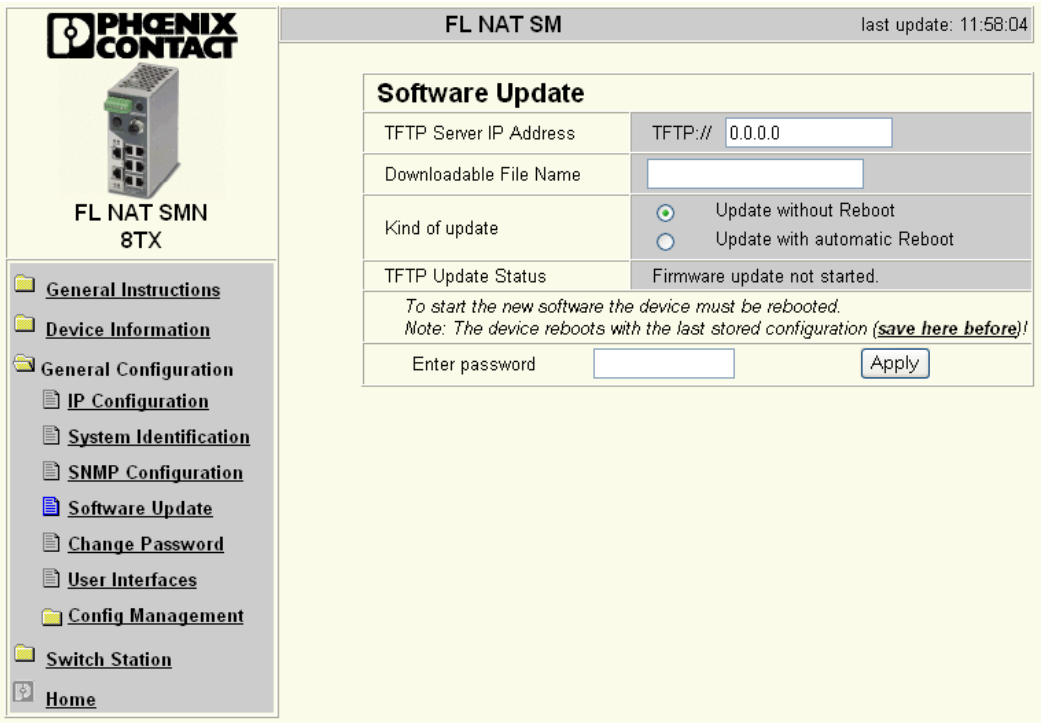


Figure 4-11 “Software Update” web page

A reset is **not** carried out **automatically** following a firmware update. The desired option can be selected in WBM.

For firmware updates, a TFTP server is required.

Following a firmware update, it is recommended that you check any configuration settings that were previously made. If necessary, reset the device to the default state upon delivery.

NOTE:

A voltage failure during a firmware update results in the destruction of the firmware on the FL NAT SMN 8TX(-M).

“Change Password” menu

By default upon delivery, the password is “private”.

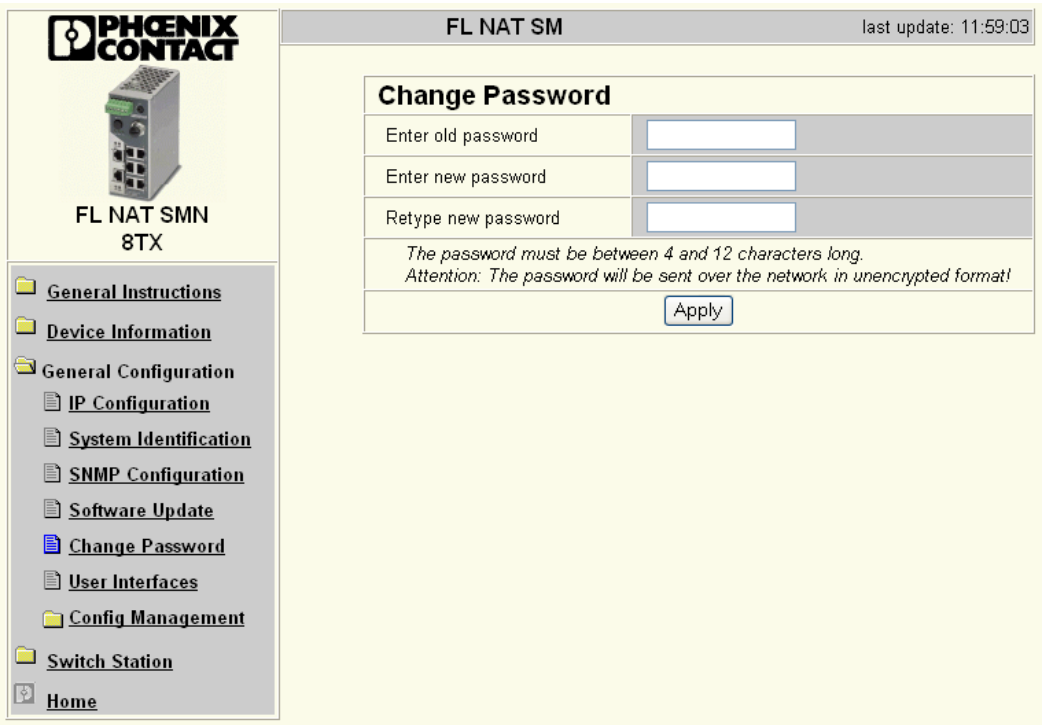


Figure 4-12 “Change Password” web page

The password must be between four and twelve characters long. Note that the password is always transferred via the network in unencrypted format.

“User Interfaces” menu

The following actions can be executed here:

– Activation/deactivation of the web server.
– Activation/deactivation of the SNMP agent.
– Setting the refresh interval for the automatic updating of the web pages. Here, you can also set the refresh interval for automatic update of different web pages. If the interval is set to “0”, the pages will no longer be updated.

Automatic update of web pages is only possible when using Internet Explorer Version 5.5 or later.

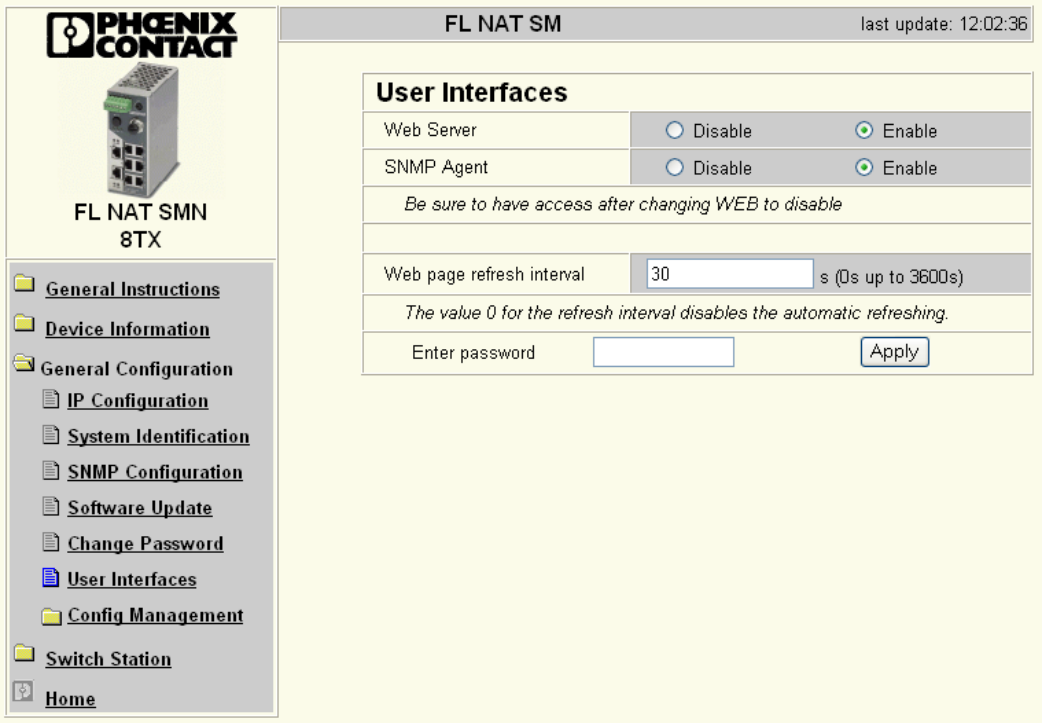


Figure 4-13 “User Interfaces” web page

“Config Management/General” menu

This table is used to view all parameters that are required to save the active configuration or load a new configuration, and to modify them (by entering a valid password). It can also be used to restart the system with the relevant configuration or to reset the FL NAT SMN 8TX(-M) to the default state upon delivery.

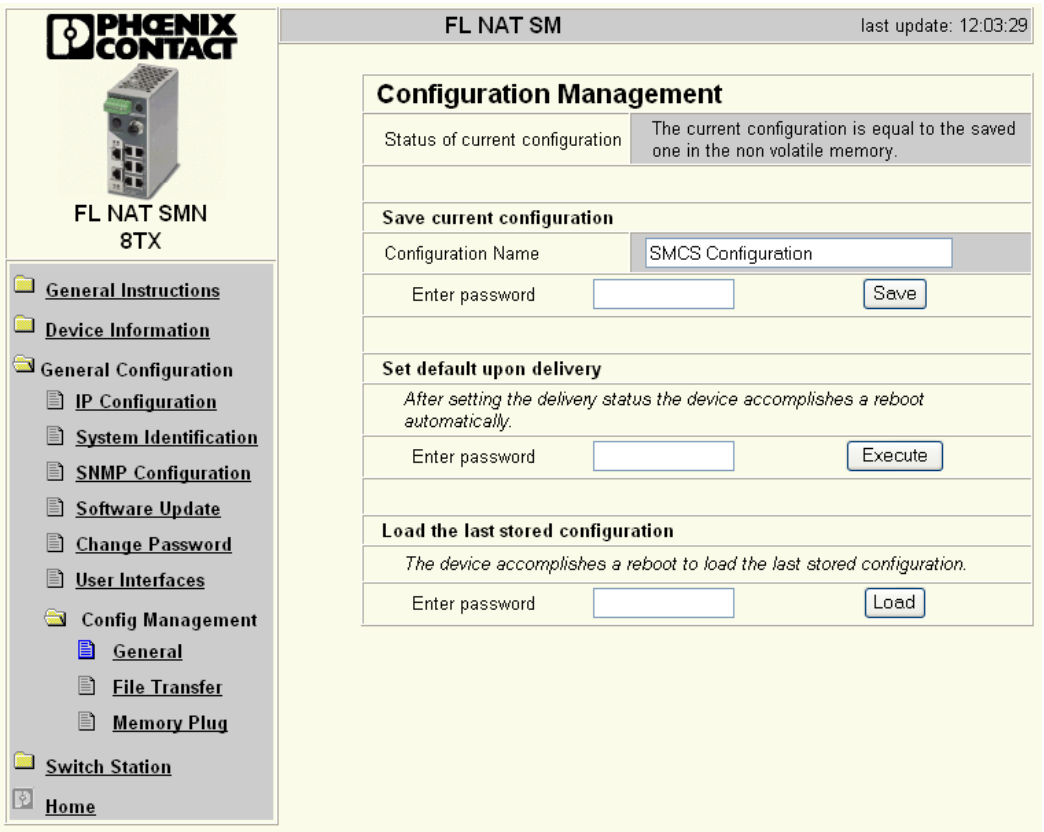


Figure 4-14 “Configuration Management” web page

Possible states for “Status of current configuration”:

– The configuration has been modified but not saved (also indicated by the flashing floppy disk icon).
– Saving the current configuration.
– The current configuration is equal to the saved one in the non volatile memory of the switch.
– The current configuration was saved.

Save current configuration

The active configuration together with the corresponding configuration name can be saved here by entering a valid password.

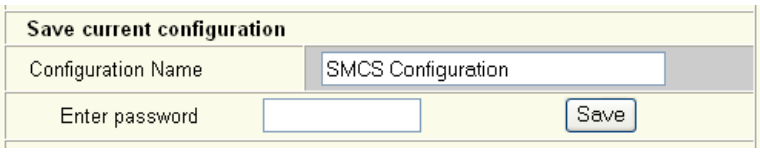


Figure 4-15 “Save current configuration” web page

If the new configuration was not activated by a reset after a configuration download, the “Save current configuration” command overwrites the previously loaded configuration and instead saves the active configuration of the FL NAT SMN 8TX(-M).

Set default upon delivery

This option can be used to reset the switch to its default settings (default upon delivery) by entering a valid password.

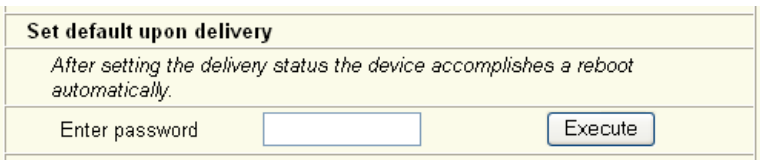


Figure 4-16 “Set default upon delivery” web page

WBM can only be called using a valid IP address. Once the NAT router has been reset to its default settings, it is in the default state upon delivery.

Load the last stored configuration

The last configuration stored on the device can be reactivated. All modifications made to the configuration since it was last saved are lost.

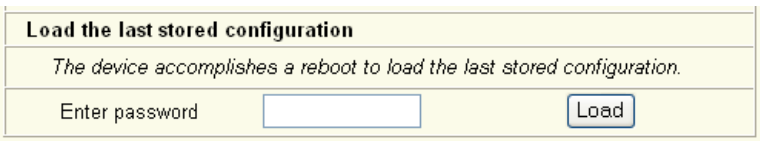


Figure 4-17 “Load the last stored configuration” web page

“Config Management/File Transfer” menu

Configuration file transfer

This option can be used to save your device configuration on a PC or to operate the switch using a stored configuration.

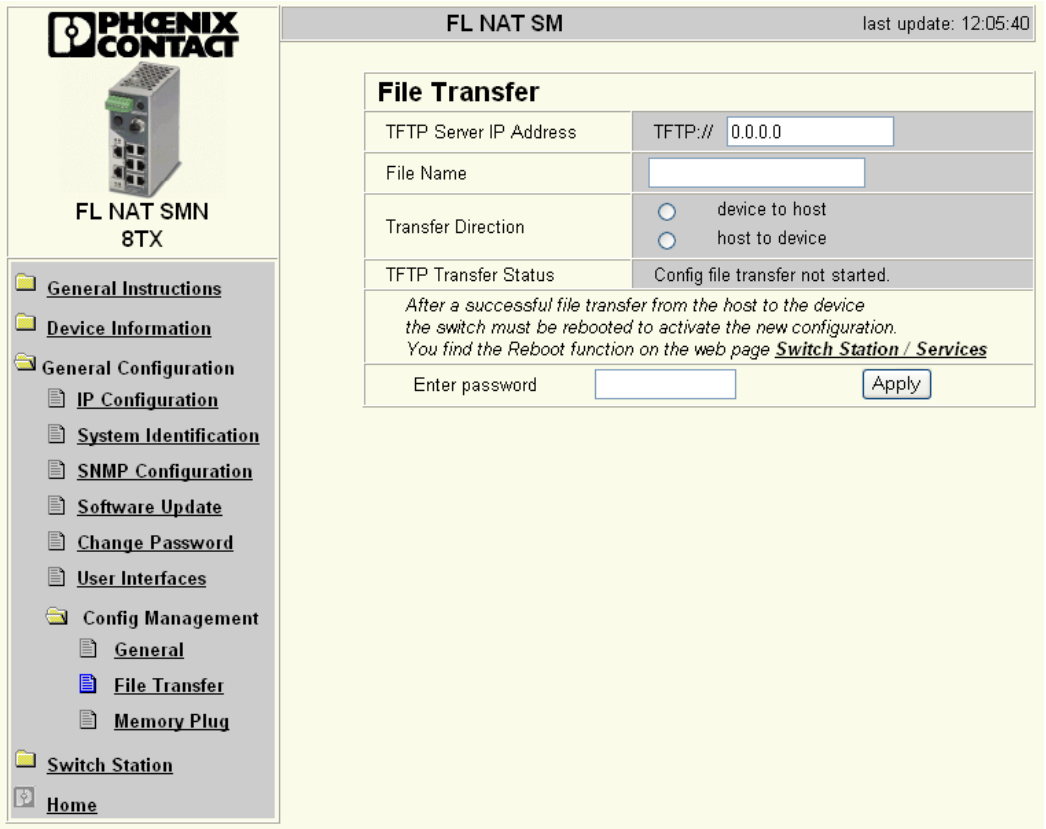


Figure 4-18 “File Transfer” web page

When a configuration is uploaded from the FL NAT SMN 8TX(-M) to a PC (device to host), the last saved version is transmitted. If you want to transmit the active configuration, first save it again (“Save current configuration” function).

When a configuration is downloaded from the PC to an FL NAT SMN 8TX(-M) (host to device), the new configuration is only activated once the switch has been reset.

The use of a configuration file does not affect an existing (“old”) password.

Device replacement

Configuration using a configuration file is used when replacing devices. To duplicate devices using a configuration file, observe the following:

– Create a point-to-point connection between an FL NAT SMN 8TX(-M) and the management station.
– Load the configuration file on the FL NAT SMN 8TX(-M).
– Reset the FL NAT SMN 8TX(-M).
– Adjust the IP parameters.
– Save the configuration (“Save current configuration” function).

The duplicated switch can now be operated in the network using the adjusted IP parameters.

“Config Management/Memory Plug” menu

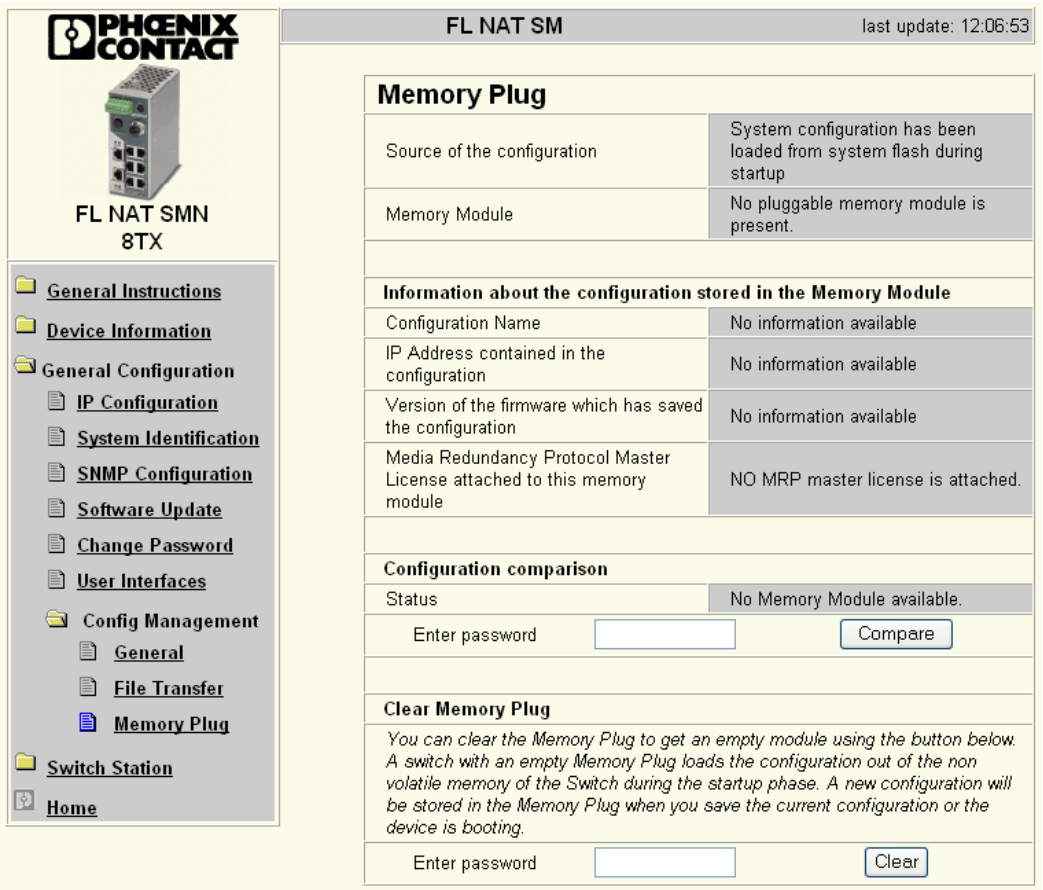


Figure 4-19 “Memory Plug” web page

Configuration comparison

Here you can compare the configuration on the memory plug with the configuration in the FL NAT SMN 8TX(-M) memory. The result is displayed in text format.

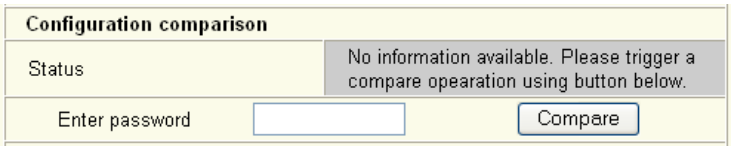


Figure 4-20 “Configuration comparison” web page

If you replace a memory plug with another memory plug within a few seconds, the configuration comparison must be updated manually.

Clear Memory Plug

Here, you can delete the memory plug by entering a valid password.

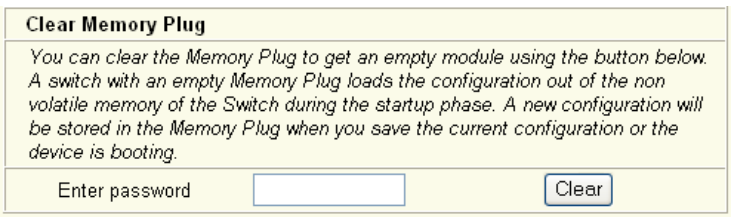


Figure 4-21 “Clear Memory Plug” web page

4.1.3.5 Switch Station

“Services” menu

The desired router mode can be selected or a device reboot triggered in the “Services” menu.

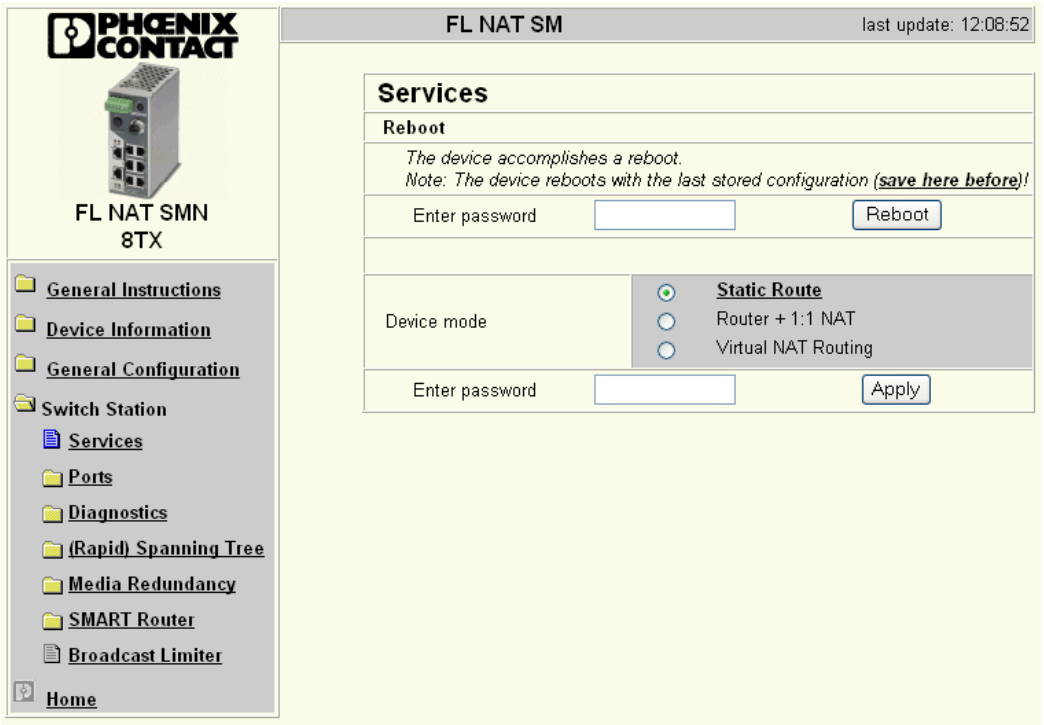


Figure 4-22 “Services” web page

Reboot To trigger a reboot via the web interface, enter a valid password. Save the configuration beforehand, so that configuration modifications are retained or can be activated via a restart.

Device mode The following modes are available:

- Static Route - Standard routing without address translation
- Router + 1:1 NAT - Block-by-block address translation with adjustable number of devices
- Virtual NAT Routing - Address translation on a virtual network

Please note that some of the configuration pages in WBM depend on the settings made under “Services”.

“Ports/Port Table” menu

Overview of all available ports. Clicking on the relevant port number opens a port-specific page (“Port Configuration”).

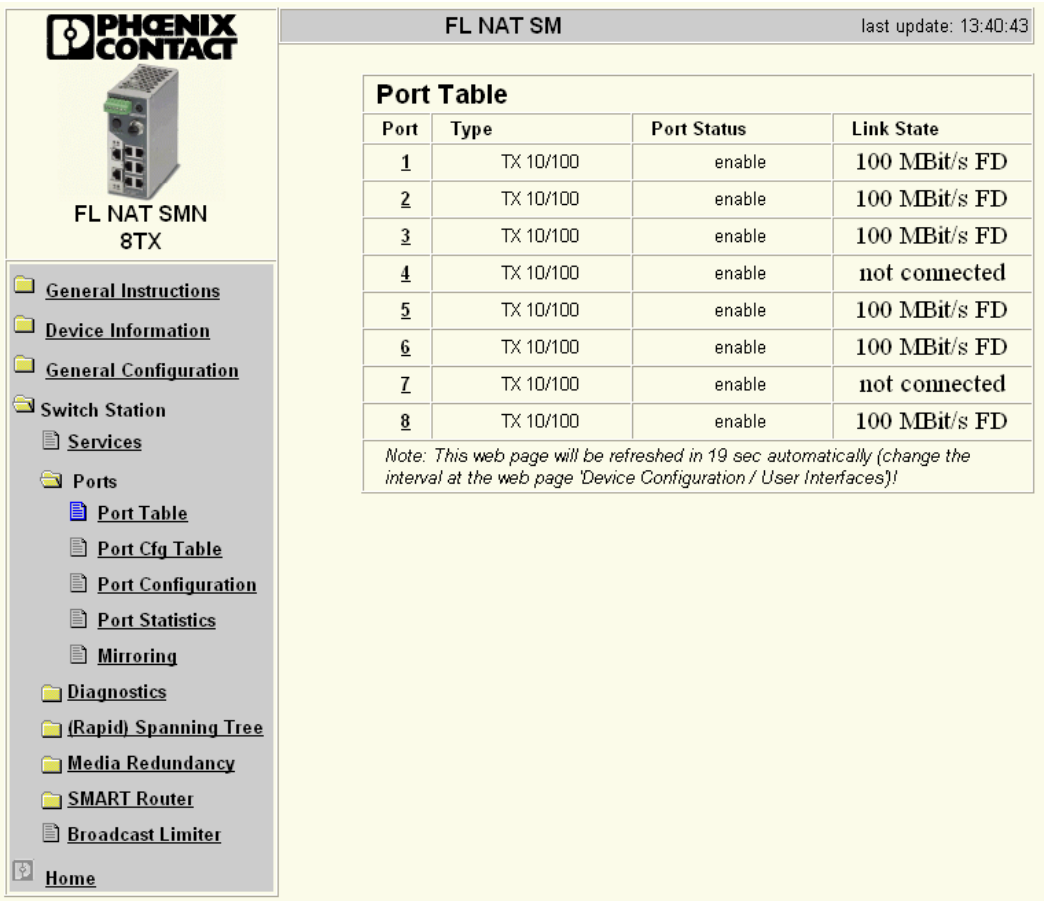


Figure 4-23 “Port Table” web page

“Ports/Port Cfg Table” menu

This menu provides an overview of the important configuration settings for all ports and also offers the option of setting the status, transmission mode, and link monitoring function for all existing ports.

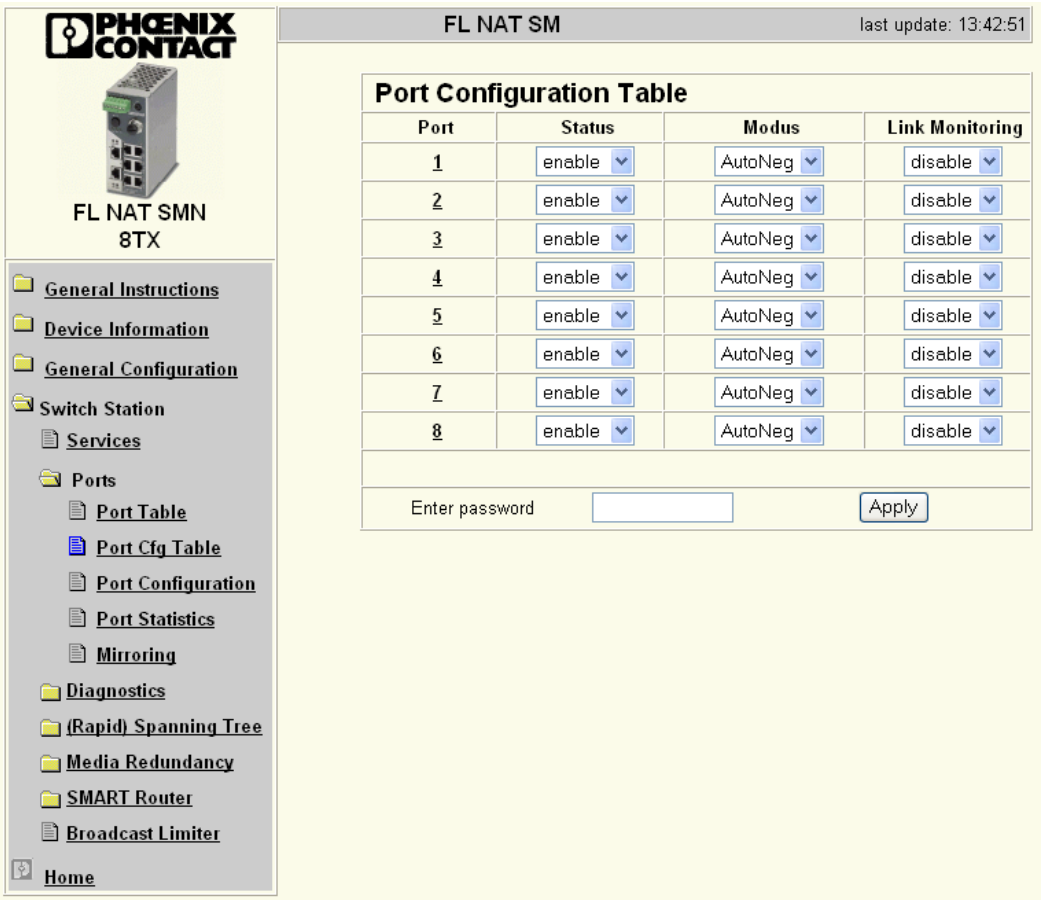


Figure 4-24 “Port Configuration Table” web page

When setting the transmission mode, make sure that the same settings have been made at both ends of the connection. If the settings are not the same, this can result in increased collisions or CRC errors and can adversely affect network performance.

“Ports/Port Configuration” menu

Offers individual configuration options for each port.

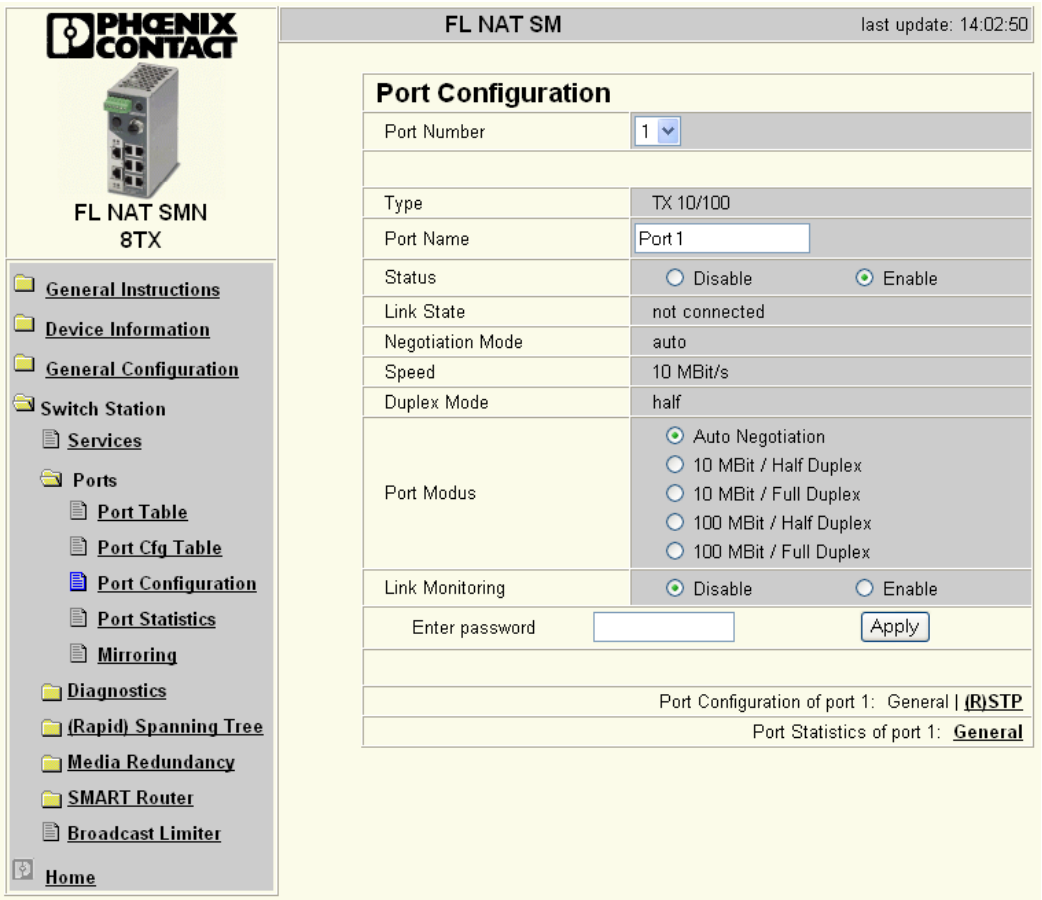


Figure 4-25 “Port Configuration” web page

“Ports/Port Statistics” menu

This menu provides detailed statistical information about the volume of data for each individual port. On this page, counter states can also be set to zero for all ports.

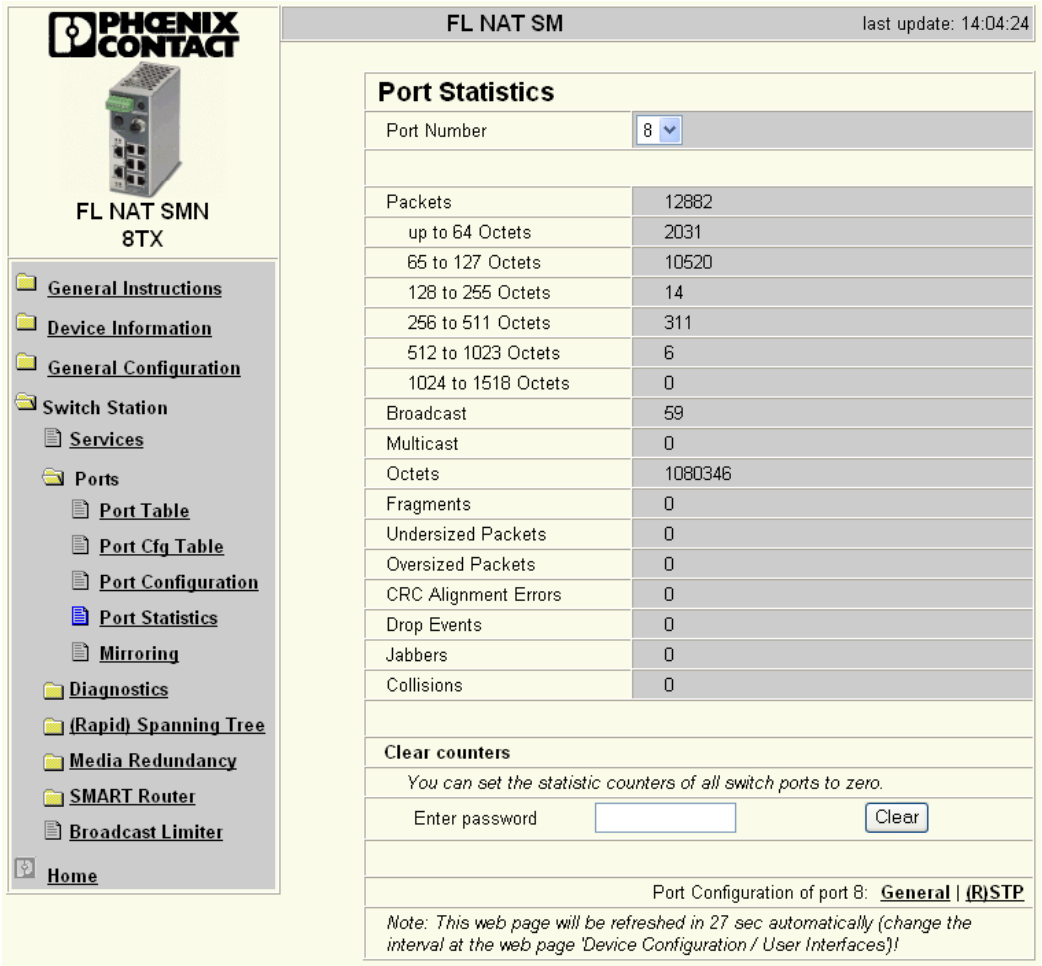


Figure 4-26 “Port Statistics” web page

“Ports/Port Mirroring” menu

Activation/deactivation and setting of port mirroring. Port mirroring is used to passively read input or output data that is being transmitted via a selected port. To do this a measuring instrument (PC) is connected to the destination port, which records the data, yet must not itself be activated.

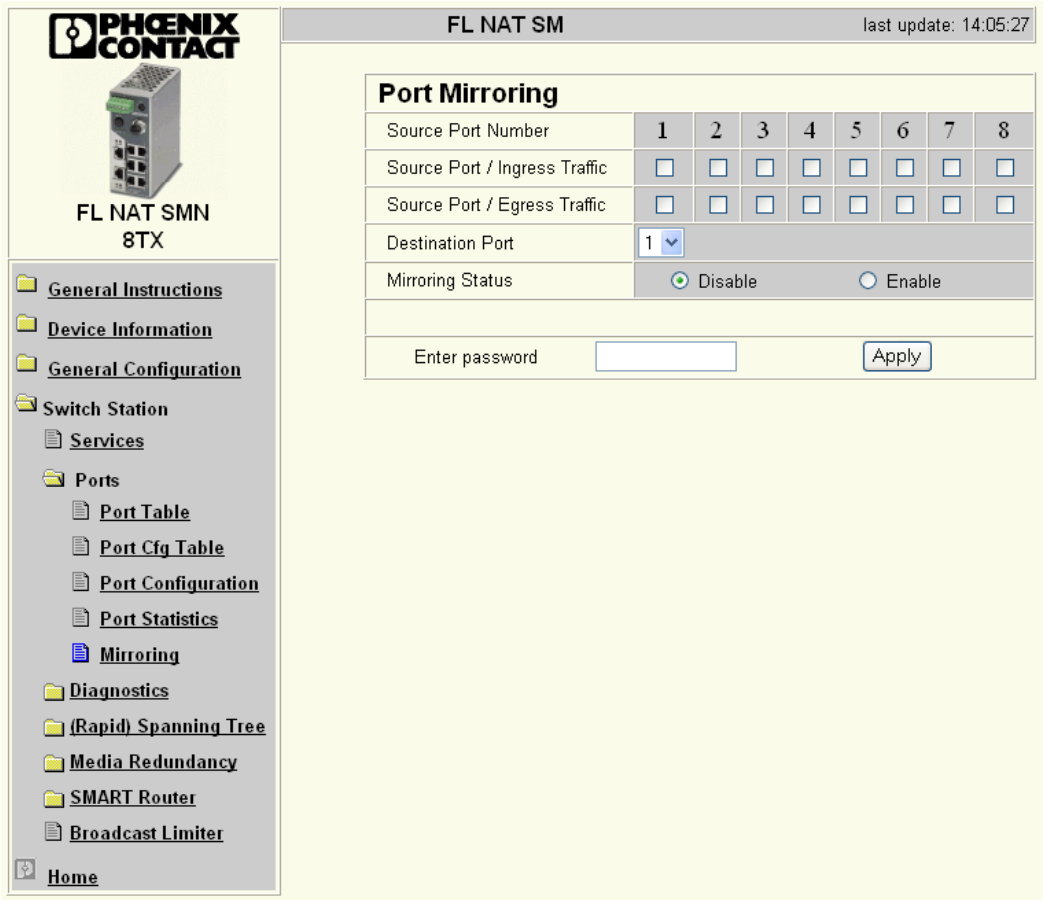


Figure 4-27 “Port Mirroring” web page

WBM prevents the same ports from being set, i.e., the source port and destination port must differ.

The port capacity is calculated according to the set transmission parameters. Example: A source port is operated at 100 Mbps and reaches a capacity of 5%. The destination port is operated at 10 Mbps. Therefore, with the same volume of data the destination port reaches a capacity of 50%.

“Diagnostics/Display” menu

The “Display” web page contains status information about the firmware, the alarm contact, and the power supply.

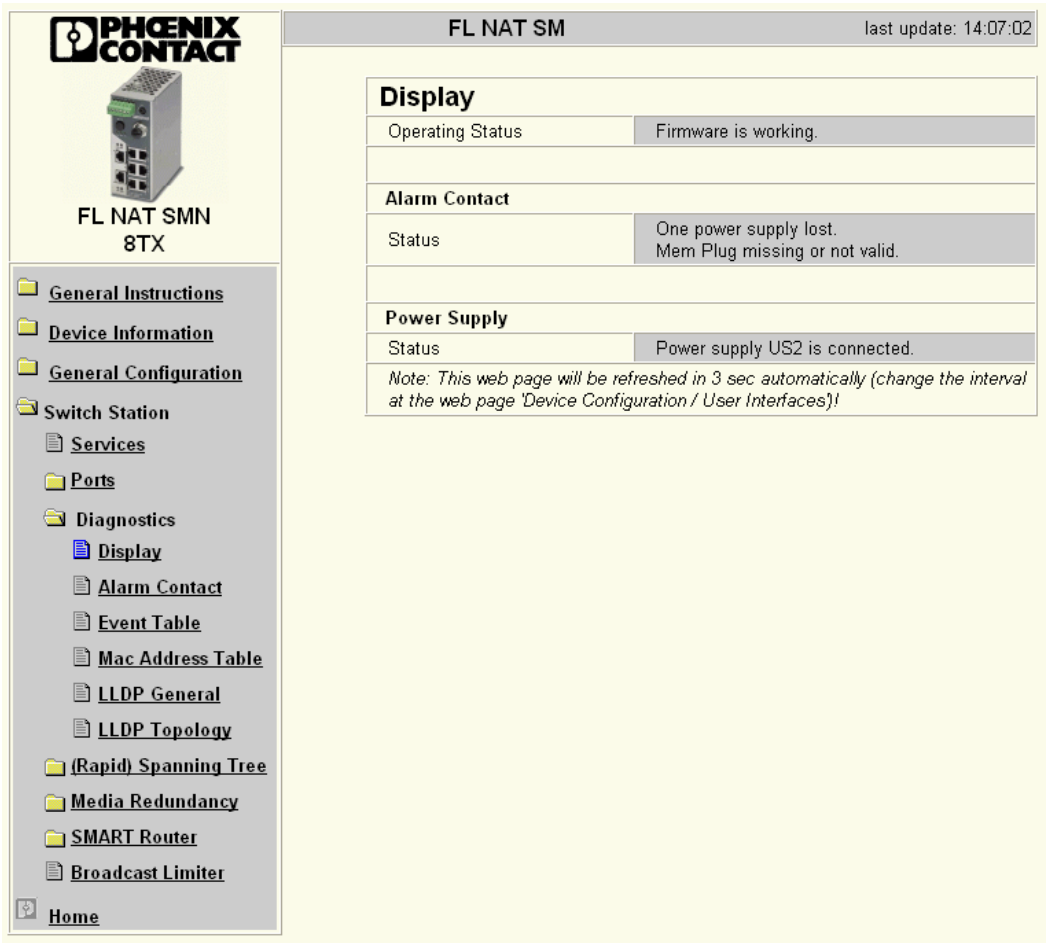


Figure 4-28 “Display” web page

“Diagnostics/Alarm Contact” Menu

Here, you can set whether and for which events the alarm contact can be used.

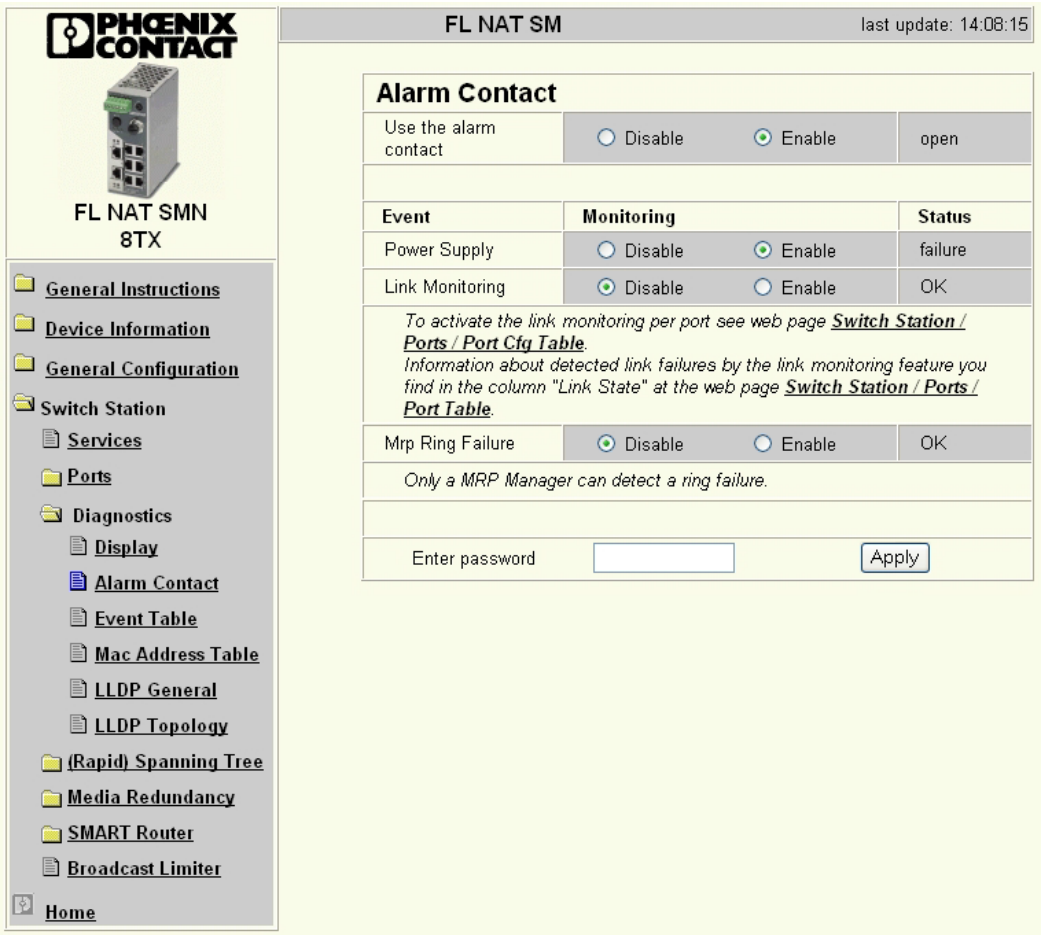


Figure 4-29 “Alarm Contact” web page

“Diagnostics/Event Table” menu

Here you will find a list of the latest important events. The list contains up to 200 entries, from the 200th entry onwards the oldest entries are overwritten (FIFO principle - first in, first out). If old entries are overwritten by new entries, a corresponding note is displayed under the event table. Restarting the device deletes all entries.

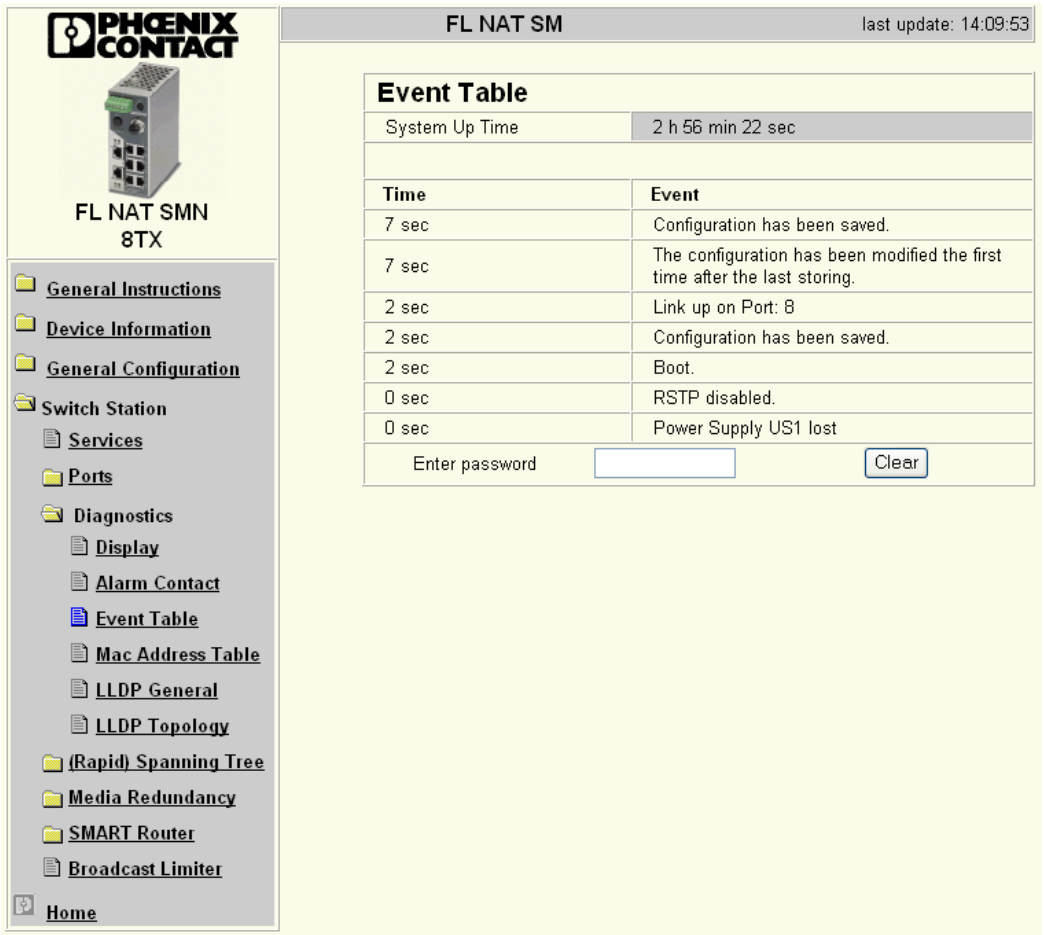


Figure 4-30 “Event Table” web page

The “Clear” button can be used to delete entries in the event table.

The following events are listed in the event table:

– Event Table cleared.
– Password has been changed.
– Password has not been changed successfully.
– Configuration has been saved.
– The configuration has been modified the first time after the last storing.
– Configuration File Transfer successfully executed.
– Configuration File Transfer was not successfully executed.
– Firmware Update was successfully executed.
– Firmware Update was not successfully executed.

- Link up at port xy.
- Link down at port xy.
- Enabling port xy.
- Disabling port xy.
- RSTP enabled.
- RSTP disabled.
- RSTP topology changed.
- RSTP elected this switch as new root.
- Power Supply US1 lost.
- Power Supply US2 lost.
- Power Supply US1 and US2 are connected now.
- LLDP Agent enabled.
- LLDP Agent disabled.
- LLDP recognized new neighbor at port xy.
- LLDP neighborhood information become obsolete at port xy.
- LLDP neighborhood information changed at port xy.

“Diagnostics/Mac Address Table” menu

Here, you will find a list indicating which MAC address has been detected at which switch port. If no packets are received at a port for a duration longer than the aging time, the entry is deleted.

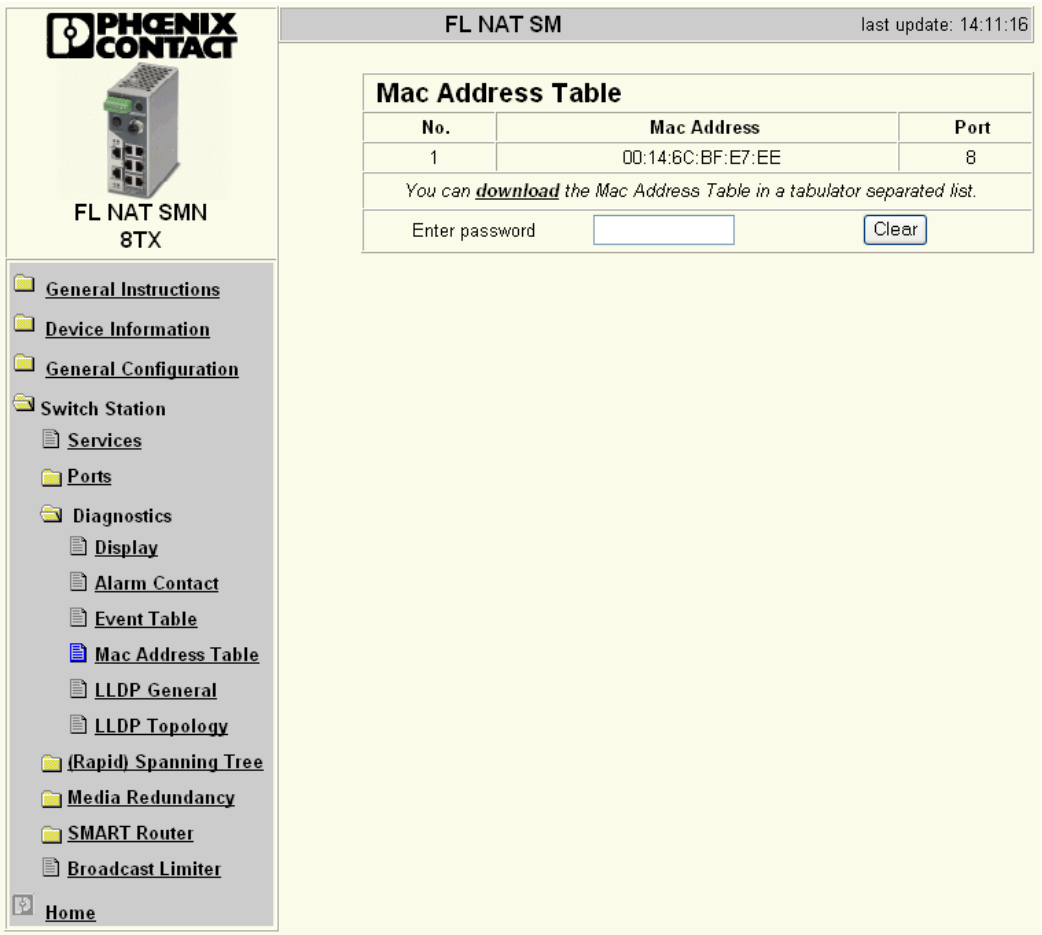


Figure 4-31 "MAC Address Table" web page

The "Clear" button can be used to delete entries in the MAC address table.

4.1.3.6 LLDP General

For information about LLDP, please refer to Section “LLDP (Link Layer Discovery Protocol)” on page 7-1.

4.1.3.7 (Rapid) Spanning Tree

The Rapid/Spanning Tree Protocol (RSTP) is a standardized method (IEEE 802.1w/IEEE 802.1d). For information, please refer to Section 5 “(Rapid) Spanning Tree”.

4.1.3.8 Media Redundancy

For information, please refer to Section 6 “Media Redundancy Protocol (MRP)”.

4.2 Routing - SMART Router

4.2.1 Static routing

4.2.1.1 "SMART Router/Static Routing" menu

Select the desired router mode on the “Services” web page, see also Section ““Services” menu” on page 4-19. Then set the desired router configuration.

The IP address area of this device to which the router should be assigned, and which standard routes are to be used can be selected on the “Static Routing” web page.

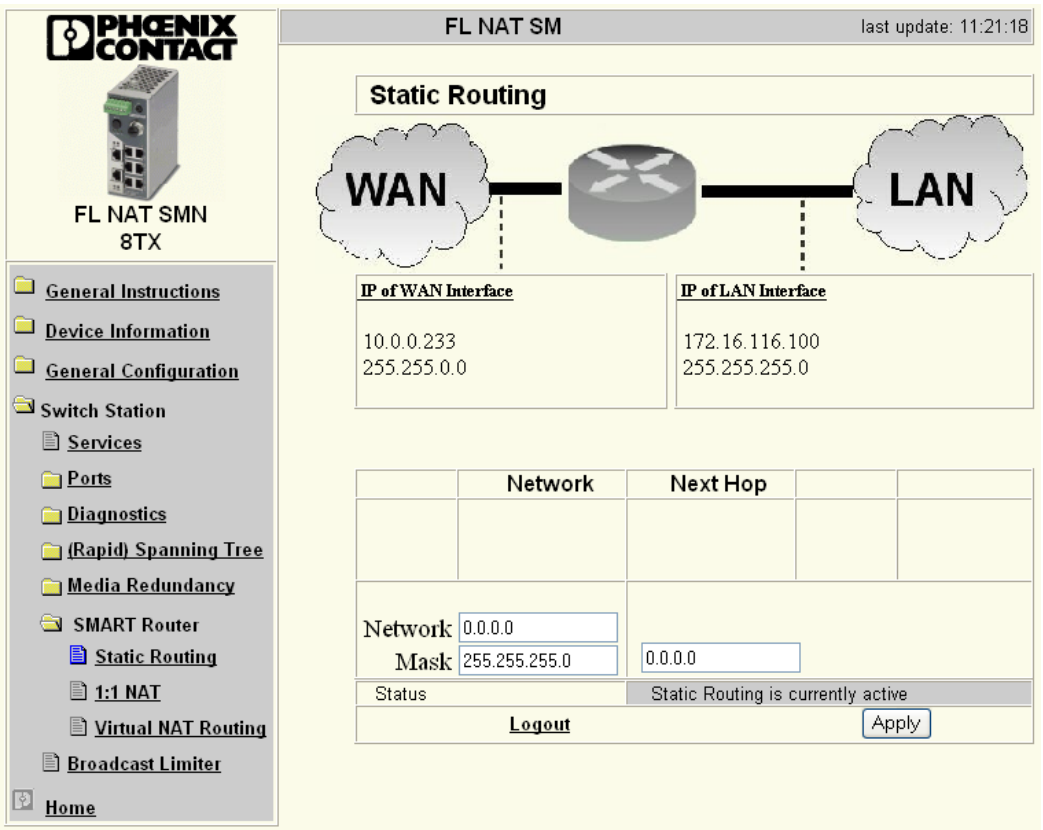


Figure 4-32 “SMART Router/Static Routing” web page

4.2.2 1:1 NAT routing

1:1 NAT enables the static mapping of an internal IP address from the LAN to an external IP address from the WAN. An external host thus accesses an internal device as if both were in the same subnetwork.

The password must be verified in order to define NAT rules and activate this feature.

4.2.2.1 Startup/activation of 1:1 NAT

Select the desired router mode on the “Services” web page, see also Section ““Services” menu” on page 4-19. Then set the desired router configuration.

Before activating 1:1 NAT, make sure that the WAN and LAN port have an IP address and can therefore be accessed in the network.

“1:1 NAT” menu

The settings for 1:1 NAT can be made here. In 1:1 NAT mode, the IP address area is mirrored in other areas.

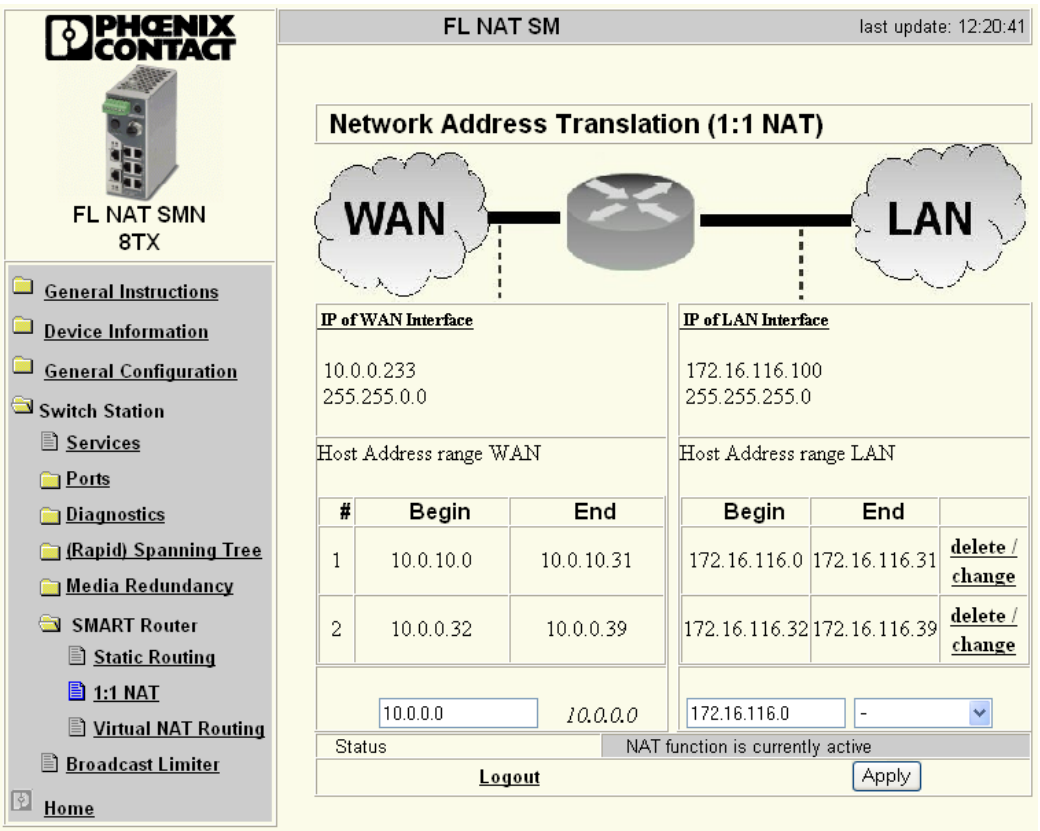


Figure 4-33 “1:1 NAT” menu

The start address of the address area in the WAN network that is to be mapped is specified in the lower input field on the left-hand side (the IP addresses must not be used by another device in the WAN network).

– The length of the address area can be specified in the selection box by the number of devices. By combining several address areas, any address areas can be defined.

– The start address of the LAN address area is specified in the input field on the right-hand side.
– The rule is added and activated by clicking “Apply”.
– So that a connection can be established to the devices in the LAN, the LAN IP address of the FL NAT SMN 8TX(-M) must be set as the gateway address on the devices in the LAN network.

Devices in the LAN network that are not mapped via the 1:1 NAT configuration cannot communicate with devices from the WAN network.

The IP address of the WAN port is not mapped, so that the device can always be accessed from the WAN network.

If address areas overlap, the order according to the first relevant rule is used (if configured).

4.2.3 Virtual NAT routing

The “Virtual NAT Routing” function can be used to map network areas that are mirrored by 1:1 NAT to a virtual network. Only one IP address from the higher-level network is required for the FL NAT SMN 8TX(-M) so that all IP addresses can be accessed from the virtual network.

4.2.3.1 Configuration of virtual NAT routing

Select the desired router mode on the “Services” web page, see also Section ““Services” menu” on page 4-19. Then set the desired router configuration.

Before activating virtual NAT, make sure that the WAN and LAN port have an IP address and can therefore be accessed in the network.

“Virtual NAT Routing” menu

The virtual network address is configured in the “Virtual NAT Routing” menu.

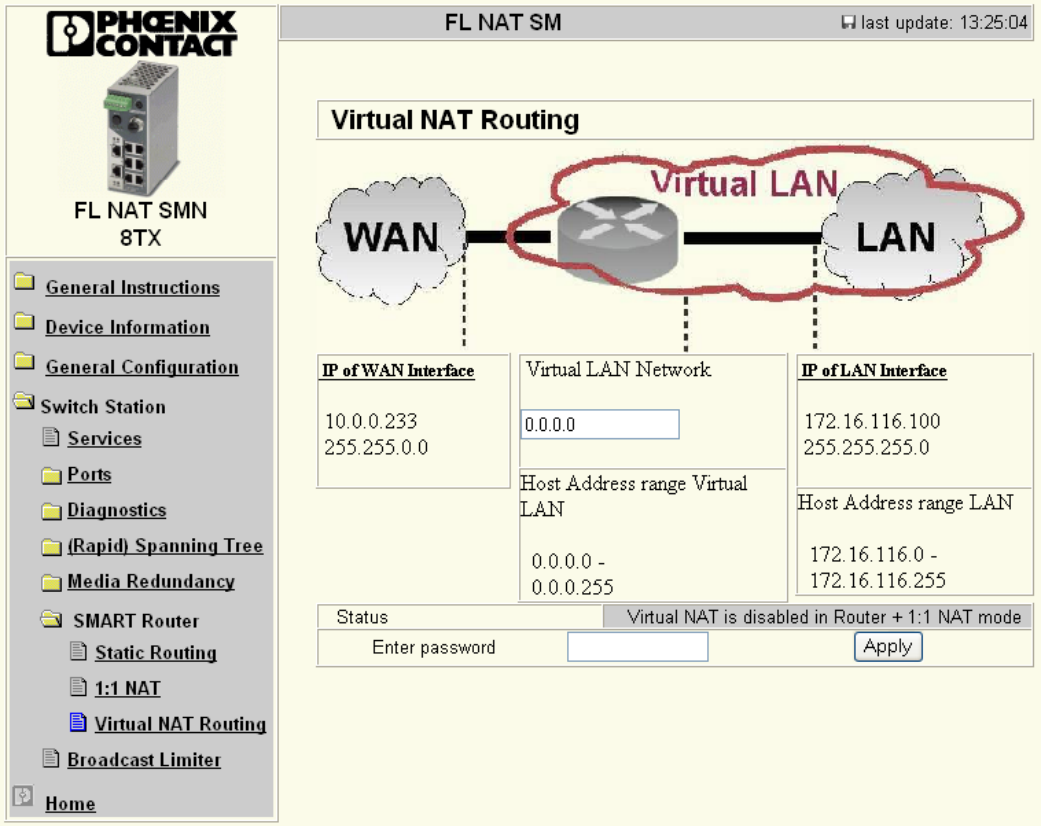


Figure 4-34 “Virtual NAT Routing” menu

So that a connection can be established between the devices in the LAN and WAN, the LAN IP address of the FL NAT SMN 8TX(-M) must be set as the gateway address on the devices in the LAN network. For the devices in the WAN network, the WAN IP address of the FL NAT SMN 8TX(-M) must be set as the route to the virtual network.

“Broadcast Limiter” menu

The “Broadcast Limiter” function can be used to limit broadcast and multicast traffic to an adjustable level in order to prevent a loss in performance on termination devices.

If the configurable bandwidth limit is reached, further broadcast or multicast packets are rejected. The set bandwidth applies for the incoming data traffic of each individual port.

The following configuration options are provided via WBM and SNMP:

– Activation/deactivation of broadcast traffic limitation on all ports
– Activation/deactivation of multicast traffic limitation on all ports

The bandwidth is selected from a drop-down list and is specified in kbps.

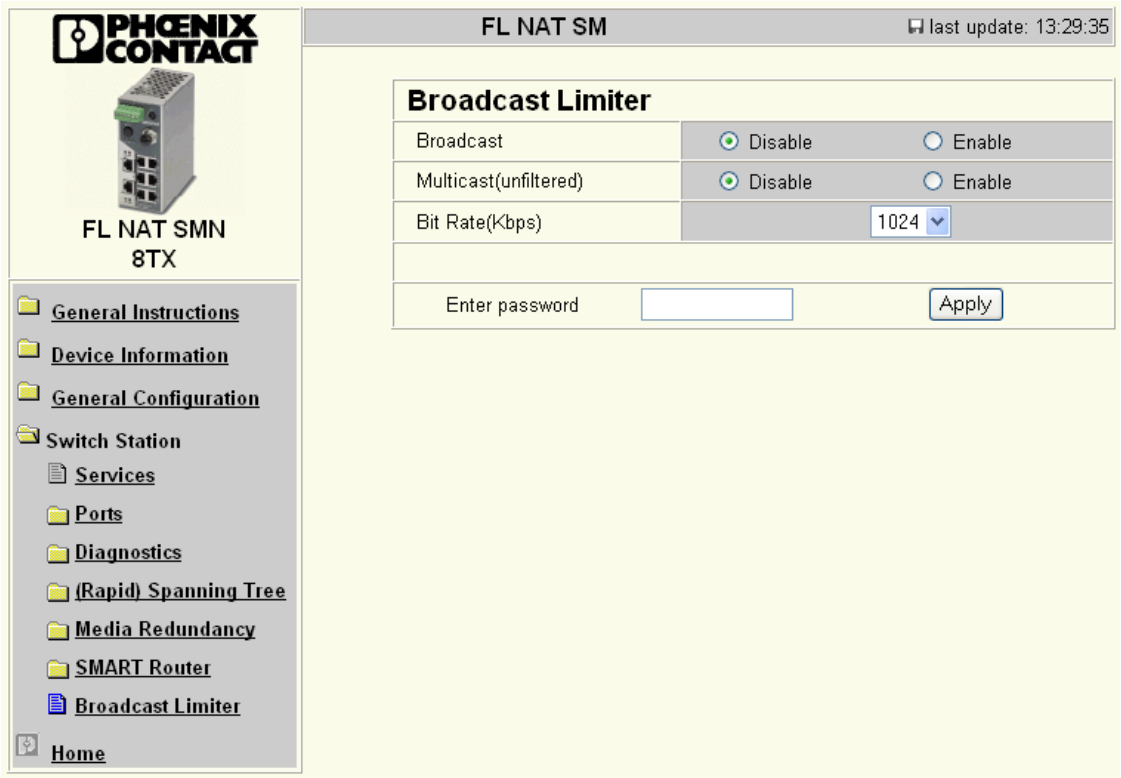


Figure 4-35 “Broadcast Limiter” menu

4.3 Simple Network Management Protocol (SNMP)

4.3.1 General function

SNMP is a manufacturer-neutral standard for Ethernet management. It defines commands for reading and writing information, and defines formats for error and status messages. SNMP is also a structured model that comprises agents, their relevant Management Information Base (MIB) and a manager. The manager is a software tool, which is executed on a network management station. The agents are located inside switches, bus terminal modules, routers, and other devices that support SNMP. The task of the agents is to collect and provide data in the MIB. The manager regularly requests and displays this information. The devices can be configured by writing data from the manager to the MIB. In the event of an emergency, the agents can also send messages (traps) directly to the manager.

All configuration modifications, which are to take effect after an FL NAT SMN 8TX(-M) restart, must be saved permanently using the “flWorkFWCtrlConfSave” object.

4.3.2 Schematic view of SNMP management

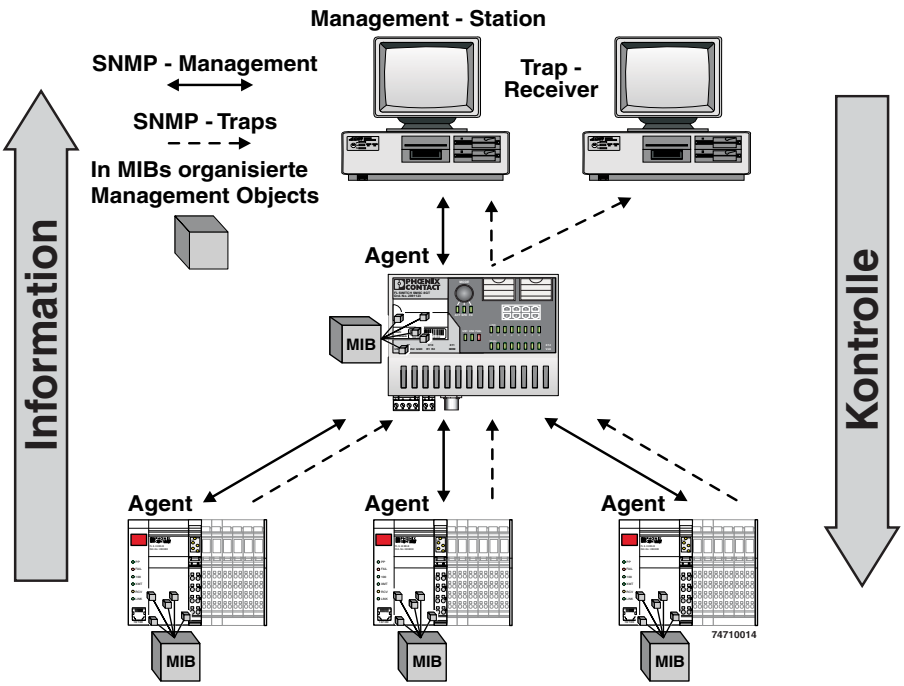


Figure 4-36 Schematic view of SNMP

SNMP interface

All managed Factoryline components have an SNMP agent. This agent of a device manages Management Information Base II (MIB 2) according to RFC1213, RMON MIB, bridge MIB, If MIB, Etherlike MIB, SNMPv2 MIB, SNMP FRAMEWORK MIB, P bridge MIB, Q bridge MIB, RSTP MIB, LLDP MIB, and private SNMP objects from Phoenix Contact (FL SWITCH M MIB).

Network management stations can read and modify configuration and diagnostic data from network devices via the Simple Network Management Protocol. In addition, any SNMP tools or network management tools can be used to access Factoryline products via SNMP. To do this, the MIBs supported by the relevant device must be made available to the SNMP management tools.

On the one hand, these are globally valid MIBs, which are specified and described in RFC (Request for Comments) standards. This includes, for example, MIB2 according to RFC1213, which is supported by all SNMP-compatible network devices. On the other hand, manufacturers can specify their own SNMP objects, which are then assigned to a private manufacturer area in the large SNMP object tree. Manufacturers are then responsible for their own private (enterprise) areas, i.e., they must ensure that only one object is assigned to an object ID (object name and parameters) and can be published. If an object is no longer needed, it can be labeled as “expired”, but it cannot be reused with other parameters under any circumstances.

Phoenix Contact provides notification of ASN1 SNMP objects by publishing their descriptions on the Internet.

Reading SNMP objects is not password-protected. However, a password is required for read access in SNMP, but this is set to “public”, which is usual for network devices, and cannot be modified. By default upon delivery, the password for write access is “private” and can be changed by the user.

SNMP, the web interface, and the serial terminal all use the same password, which can be changed by the user.

Another benefit for the user is the option of sending traps using the Simple Network Management Protocol.

Management Information Base (MIB)

Database which contains all the data (objects and variables) required for network management.

Agent

An agent is a software tool, which collects data from the network device on which it is installed, and transmits this data on request. Agents reside in all managed network components and transmit the values of specific settings and parameters to the management station. On a request of a manager or on the occurrence of a specific event, the agent transmits the collected information to the management station.

Traps

Traps are spontaneous SNMP alarm or information messages that are sent by an SNMP-compatible device when specific events occur. Traps are transmitted with maximum priority to various addresses (if required) and can then be displayed by the management station in plain text. The IP addresses that are to receive these traps (trap targets/receivers) must be set by the user on the relevant device. The following traps are sent when required:

- Modification or attempted modification of the device password
  trapPasswdAccess
- Information about the firmware status
  trapFWHealth
- Failure of the redundant power supply
  trapPowerSupply
- A disabled MAC address accesses a port
  trapSecurityPort
- Link interrupt in the redundant RSTP ring
  trapRstpRingFailure
- Status of an MRP ring port changes (MRP manager only)
  trapMrpStatusChange
- The connection between the SNMP agent and the network management station is tested
  trapManagerConnection

Not all devices support all object classes. If an unsupported object class is requested, “not supported” is generated. If an attempt is made to modify an unsupported object class, the message “badValue” is generated.

The following table provides an overview of the information contained in the various MIB files.

Table 4-1 Overview of the MIB structure of the MIBs

What information?	In which MIB file?	For which objects?
Information about the manufacturer	FL-NAT-Router-V320-MIB.mi2	pxcBasic
Serial number of the device	FL-NAT-Router-V320-MIB.mi2	flWorkBasicSerialNumber
Hardware version of the device	FL-NAT-Router-V320-MIB.mi2	flWorkBasicHWRevision
Status information for supply voltages	FL-NAT-Router-V320-MIB.mi2	flWorkBasicPowerStat
MAC address of the switch	FL-NAT-Router-V320-MIB.mi2	flWorkNetIfParamPhyAddress
Firmware information	FL-NAT-Router-V320-MIB.mi2	flWorkFWInfo Group
IP address settings	FL-NAT-Router-V320-MIB.mi2	flWorkNetIfParamIpAddress
Subnet mask settings	FL-NAT-Router-V320-MIB.mi2	flWorkNetIfParamSubnetmask
Default gateway settings for the IP address	FL-NAT-Router-V320-MIB.mi2	flWorkNetIfParamGwIpAddress
LLDP settings, activation/deactivation	FL-NAT-Router-V320-MIB.mi2	flSwitchCtrlLldp
Large tree support, activation/deactivation	FL-NAT-Router-V320-MIB.mi2	flSwitchCtrlRSTPLargeTreeSupport
Fast ring detection support, activation/deactivation	FL-NAT-Router-V320-MIB.mi2	flSwitchCtrlRSTPFastRingDetection
DHCP relay agent, activation/deactivation	FL-NAT-Router-V320-MIB.mi2	flSwitchCtrlDhcpRelayAgentUi
DHCP relay agent, settings and parameters	FL-NAT-Router-V320-MIB.mi2	flSwitchRelayAgentDhcp
Delete switch MAC address table	FL-NAT-Router-V320-MIB.mi2	flSwitchCtrlMacTableErase
Setting and parameterization for IGMP snooping	FL-NAT-Router-V320-MIB.mi2	flSwitchIgmpSnoop
Setting for port mirroring	FL-NAT-Router-V320-MIB.mi2	flSwitchPortMirr
Broadcast limiter - settings, activation/deactivation	FL-NAT-Router-V320-MIB.mi2	flSwitchRateCtrlBroadcast

Table 4-1 Overview of the MIB structure of the MIBs [...]

What information?	In which MIB file?	For which objects?
Router - selection of the operating mode, router, NAT, bridge, etc.	FL-NAT-Router-V320-MIB.mi2	flWorkSecurityCtrlDevMode
Router - mode settings: router and masquerading	FL-NAT-Router-V320-MIB.mi2	flWorkSecurityRouterForwarding
Router - mode settings: router and 1:1 NAT	FL-NAT-Router-V320-MIB.mi2	flWorkSecurityRouterNat
Router - mode settings: virtual NAT router	FL-NAT-Router-V320-MIB.mi2	flWorkSecurityRouterVRouter
Router - mode settings: router	FL-NAT-Router-V320-MIB.mi2	flWorkSecurityRouterStatic
Event table - information and parameterization	FL-NAT-Router-V320-MIB.mi2	flWorkFWInfoEventTable
Device web browser, activation/deactivation	FL-NAT-Router-V320-MIB.mi2	flWorkFWCtrlHTTP
Web browser, refresh interval of the web pages	FL-NAT-Router-V320-MIB.mi2	flWorkFWCtrlWebPageRefresh
Detailed information about LLDP	LLDP-MIB.mi2	
Ethernet, broadcast, and multicast packets - information	rfc1757-RMON-MIB.mib	
Alarm Konfiguration	rfc1757-RMON-MIB.mib	
System information, time, and contact, manufacturer ID	RFC1213-MIB2.mib	
MRP configuration options	pnoRedundancy.mib	
MRP specification of role, client, master, etc.	pnoMRPDomainAdminRole	
Ethernet data traffic information	RFC2665-EtherLike-MIB.mi2	
SNMP management architecture	RFC2571-SNMP-Framework-MIB.mi2	
SNMPv2 functions	RFC1907-SNMPv2-MIB.mi2	

4.4 Management via local RS-232 communication interface

4.4.1 General function

A local communication connection can be established to an external management station via the RS-232 interface in Mini-DIN format. Use the “PRG CAB MINI DIN” programming cable (Order No. 2730611). The communication connection is established using a corresponding emulation between the switch and a PC (e.g., HyperTerminal under Windows) and enables access to the user interface.

The reference potentials of the RS-232 interface and the supply voltage are not electrically isolated.

4.4.1.1 Interface configuration

Make the following settings on your Windows PC.

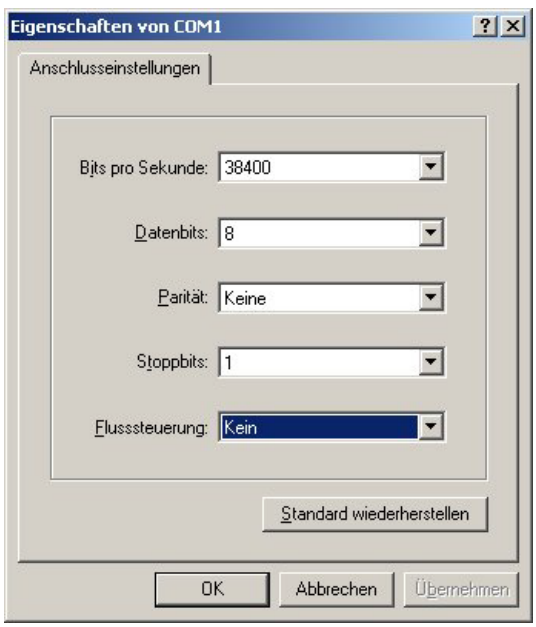


Figure 4-37 HyperTerminal configuration

4.4.1.2 Calling the user interface

Connect the PC and the switch using a suitable cable (PRG CAB MINI DIN, Order No. 2730611). Once you have established the connection, select the Ctrl+L key combination on the PC. The switch then requests the screen contents.

4.4.2 User interface functions

4.4.2.1 Functions during the boot process after a restart

If you open the user interface in the first five seconds immediately after an FL NAT SMN 8TX(-M) restart, you have the option of triggering a firmware update.

Functions during operation

The following functions are available in the user interface:

– Setting the IP parameters of the WAN port
– Selecting the addressing mechanism (static, BootP)
– Resetting to the default settings
– Activating/deactivating the web server and SNMP
– Activating/deactivating the RSTP redundancy mechanism
– Reset

All settings are applied using “APPLY”, but are **not** saved permanently. Use the “SAVE” function to save the active configuration settings permanently.

4.4.2.2 Structure of the user interface screens

Login screen

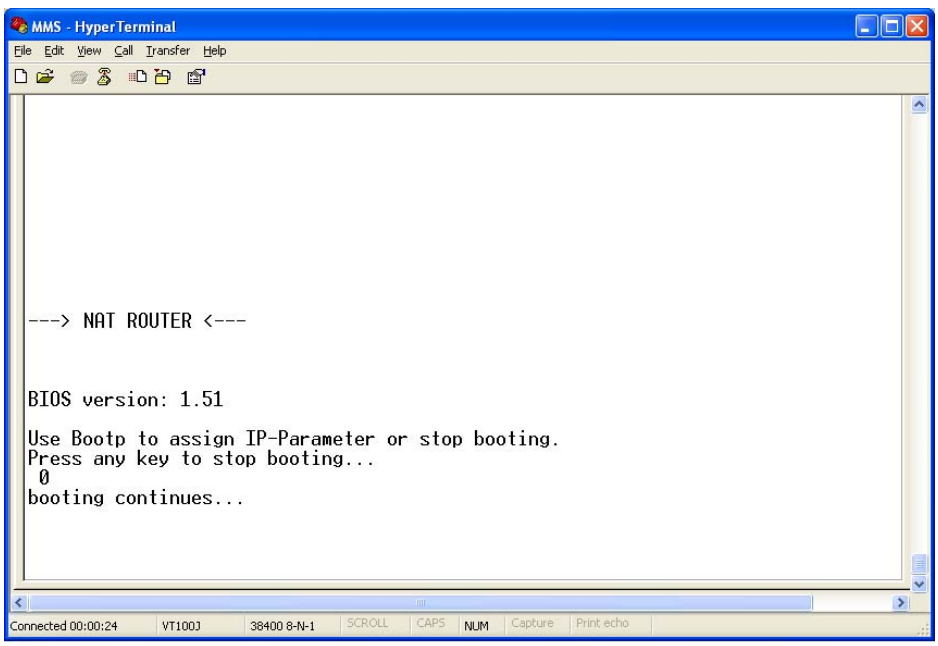


Figure 4-38 User interface login screen

The login screen indicates the version of the firmware used. A password must be entered to make other settings. By default upon delivery, the password is “private”. Please note that it is case-sensitive. We strongly recommend that you change the password (via SNMP or WBM).

Basic switch configuration

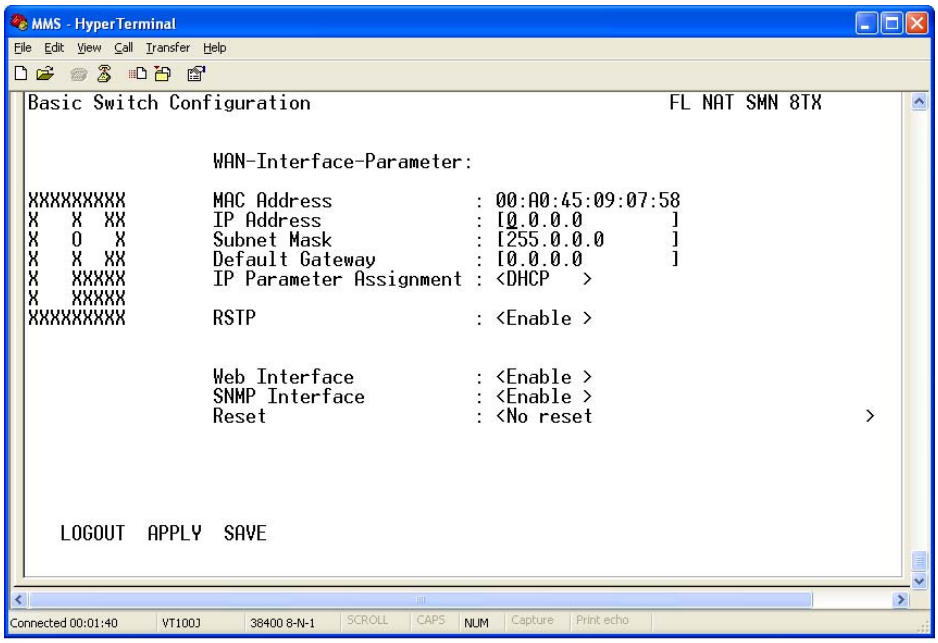


Figure 4-39 IP configuration in the user interface

As well as displaying the set MAC address, this screen can be used to view or modify the IP parameters.

In order to set the IP parameters, the “Static” option must be selected for “IP Parameter Assignment”.

This user interface screen can be used to determine the addressing mechanism or to trigger a device restart.

All settings are applied using “APPLY”, but are **not** saved permanently. Use the “SAVE” function to save the active configuration settings permanently.

4.4.2.3 IP address assignment of the WAN port via RS-232

IP address assignment via RS-232 is only supported by the WAN port (port 1).

In order for the switch to perform its function, it requires an IP address, which can be assigned via the serial interface. If the switch already has an IP address, it uses this existing IP address following a restart if it does not receive another address via BootP or RS-232.

5 (Rapid) Spanning Tree

5.1 (R)STP startup

Startup consists of two parts that must be executed in the specified order:

1 Enable (R)STP on all switches that are to be operated as active (R)STP components in the network.

2 Connect the switches to form a meshed topology.

Only create the meshed topology after activating (R)STP.

5.1.1 Enabling (R)STP on all switches involved

(R)STP can be activated via web-based management, via the SNMP interface or via the serial interface.

While learning the network topology, the switch temporarily does not participate in network communication.

Now switch to the “(R)STP General” page in the “Switch Station” menu. Here, you will find various information about the Spanning Tree configuration.

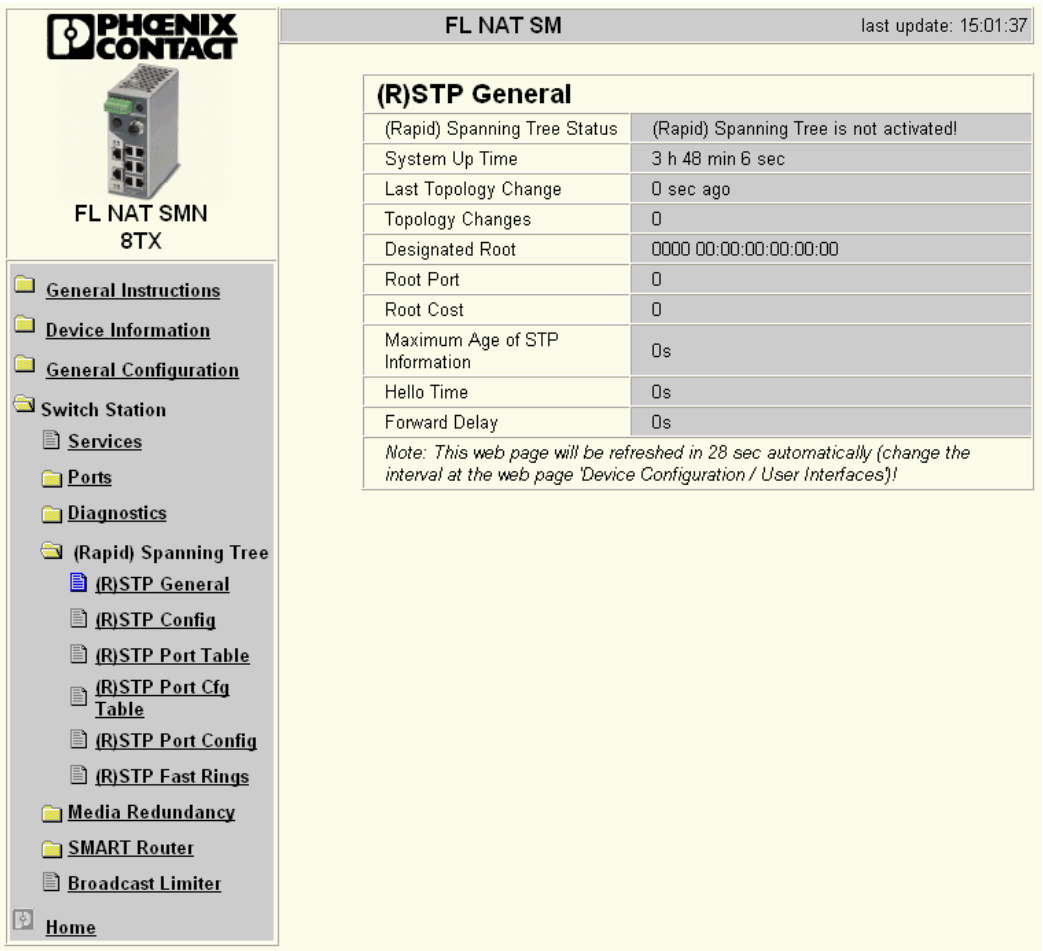


Figure 5-1 “(R)STP General” web page

The web page displays the parameters with which the switch is currently operating.

(R)STP Configuration

It is sufficient to set the “Rapid Spanning Tree Status” to “Enable” in order to start (R)STP using default settings. Priority values can be specified for the switch. The bridge and backup root can be specified via these priority values.

Only multiples of 4096 are permitted. The desired value can be entered in the “Priority” field. The value will be rounded automatically to the next multiple of 4096. Once you have confirmed the modification by entering your password, the initialization mechanism is started.

Redundant connections can now be created.

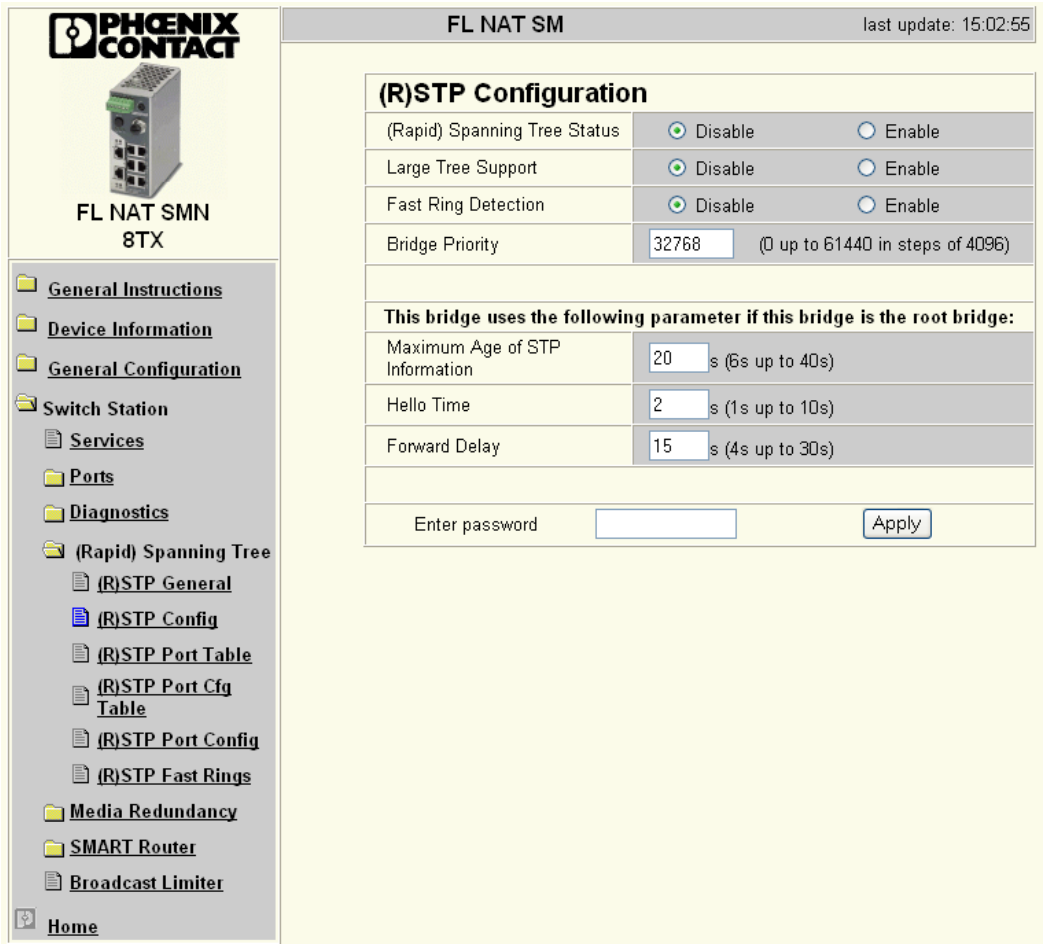


Figure 5-2 “(R)STP Configuration” web page

Large Tree Support

If RSTP is operated using the default values, it is suitable for up to seven switches along the relevant path (see Figure 5-15 on page 5-23 and Figure 5-16 on page 5-24 as an example for the relevant path). The RSTP protocol would therefore be possible in a ring topology for up to 15 switches.

The “Large Tree Support” option makes the ring topology suitable for 28 switches along the relevant path if RSTP is used. The “Large Tree Support” option could provide an RSTP ring topology with up to 57 devices. When using large tree support, please note the following:

– In the large tree support RSTP topology, do **not** use devices that do **not** support large tree support.
– Enable the “Large Tree Support” option on **all** devices.
– If RSTP is to be activated as the redundancy mechanism in an existing network with more than seven switches along the relevant path, then the “Large Tree Support” option must first be enabled on all devices.
– It is recommended that large tree support is not activated in networks with less than seven switches along the relevant path.

Maximum Age of STP Information
The parameter is set by the root switch and used by all switches in the ring. The parameter is sent to make sure that each switch in the network has a constant value, against which the age of the saved configuration is tested.

The “Maximum Age of STP Information”, “Hello Time”, and “Forward Delay” fields have the same meaning as for STP. These values are used when this switch becomes a root. The values currently used can be found under (R)STP General.

Hello Time
Specifies the time interval within which the root bridge regularly reports to the other jumpers via BPDU.

Forward Delay
The forward delay value indicates how long the switch is to wait in order for the port state in STP mode to change from “Discarding” to “Listening” and from “Listening” to “Learning” (2 x forward delay).

The “Max Age of STP”, “Hello Time”, and “Forward Delay” parameters are optimized by default upon delivery. They should not be modified.

(R)STP Port Table

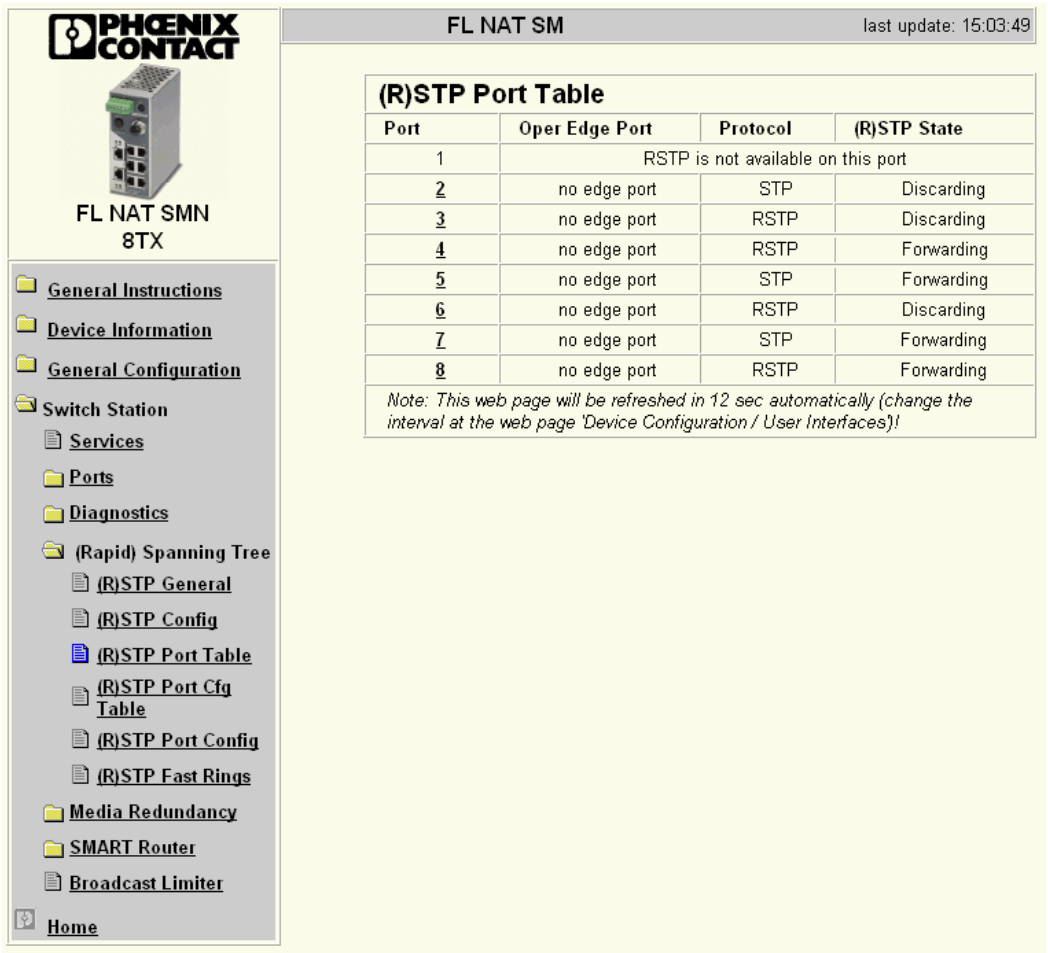


Figure 5-3 "(R)STP Port Table" web page

Oper Edge Port
All ports that do not receive any (R)STP BPDUs (e.g., termination device ports) become edge ports, i.e., ports that go to the “Forwarding” state immediately after restart.

Protocol
Indicates the redundancy protocol used.

(R)STP State
Indicates the current (R)STP state of the relevant port.

Possible states:

– “Forwarding”
The port is integrated in the active topology and forwards data.
– “Discarding”
The port does not take part in data transmission.

– “Learning”
The port does not take part in data transmission of the active topology, however, MAC addresses are learned.
– Blocking/Discarding
The port has a link, but has not been set to the “Discarding” state by RSTP.

(R)STP Port Configuration Table

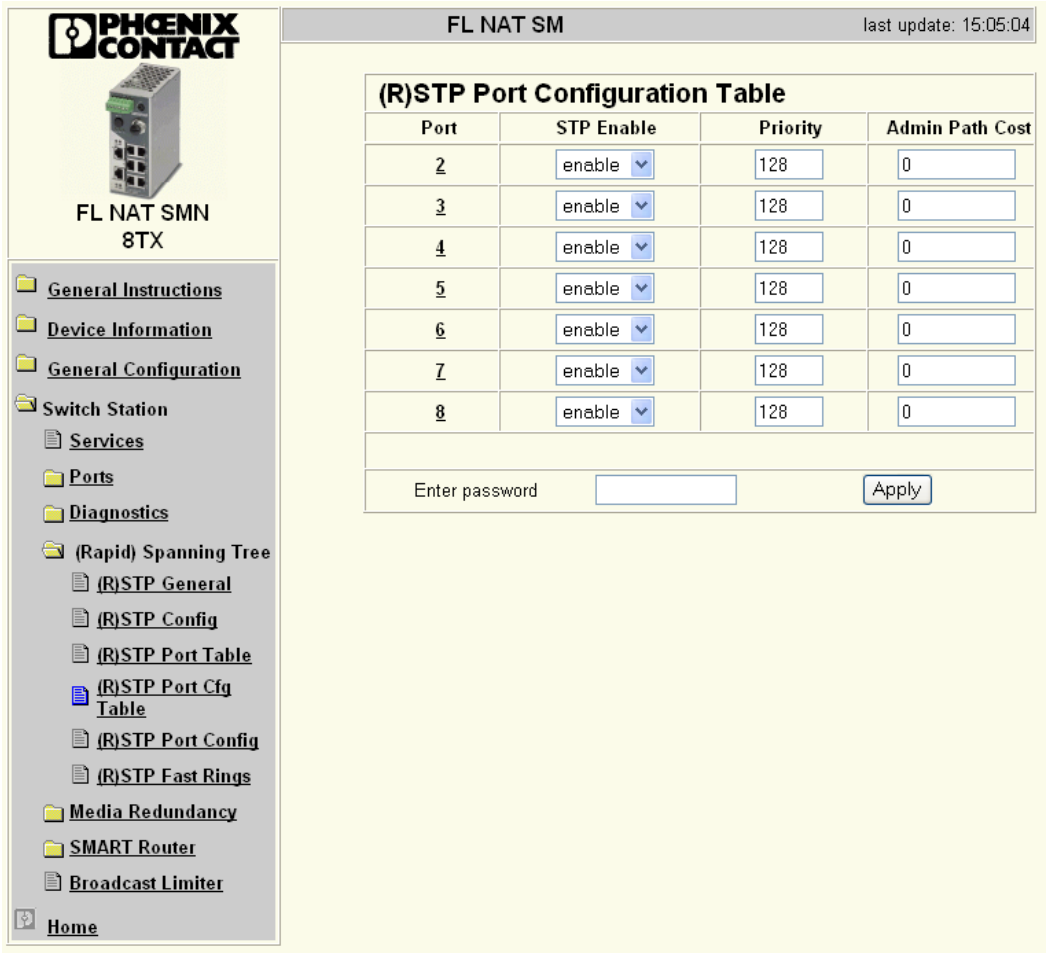


Figure 5-4 “(R)STP Port Configuration Table” web page

An overview of the main settings for each port is provided here.

5.1.1.1 (R)STP Port Configuration

Modifications of properties can result in complete reconfiguration of (Rapid) Spanning Tree.

It is recommended that a suitable root switch and a backup root switch are specified using corresponding priority assignment.

This page displays the valid (R)STP configuration settings for the selected port.

If termination devices or subnetworks are connected without RSTP or STP via a port, it is recommended that the “Admin Edge Port” be set to “Edge Port”. A link modification at this port will therefore not result in a topology modification.

5.1.1.2 Switch/port ID

The validity of switches and ports is determined according to priority vectors.

Bridge identifier

A switch ID consists of eight bytes as an unsigned integer value. When comparing two switch IDs, the one with the lowest numeric value is of higher, i.e., “better”, priority.

The first two bytes contain the priority.
The last six bytes contain the MAC address and thus ensure the uniqueness of the switch ID in the event of identical priority values.

The switch with the lowest numerical switch ID becomes the root. It is recommended that the root port and alternate port are specified using the priority.

Port identifier

The port ID consists of four bits for the port priority and twelve bits for the port number. The port ID is interpreted as an unsigned integer value. When comparing two port IDs, the one with the lowest numeric value is of higher, i.e., “better”, priority.

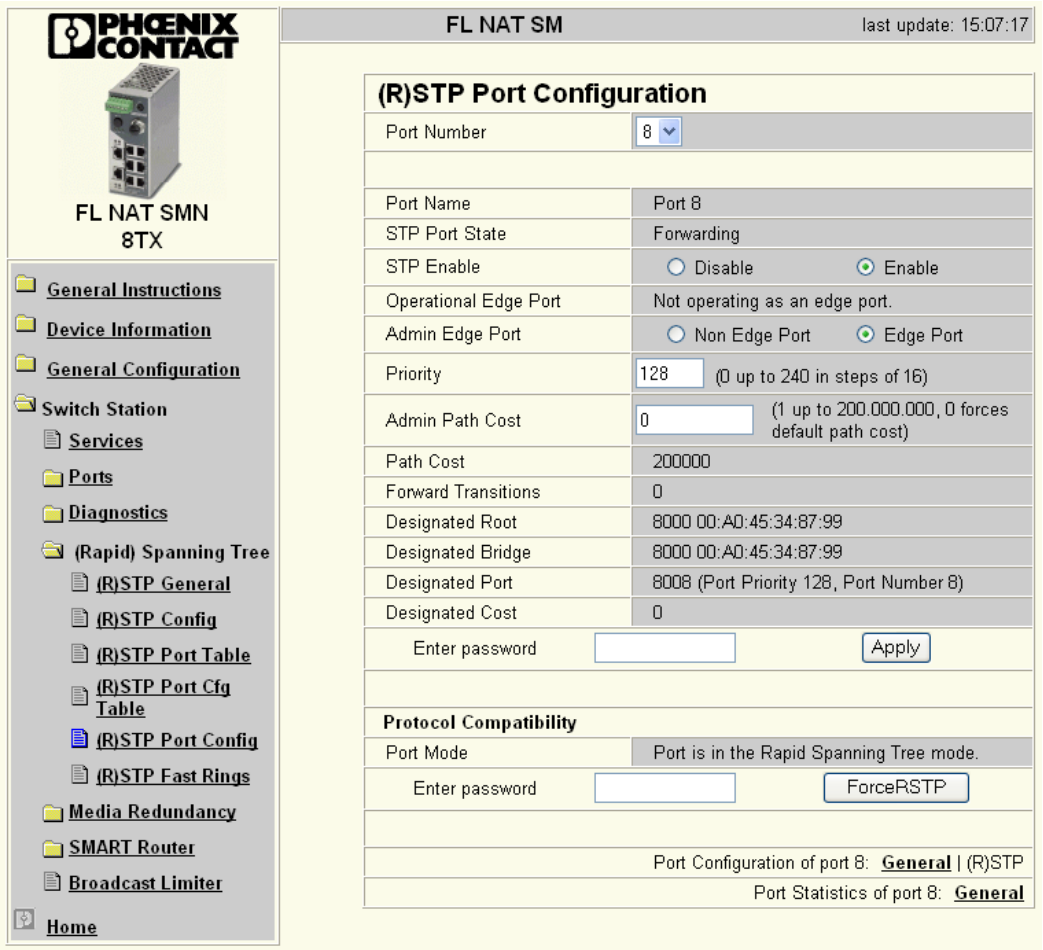


Figure 5-5 “(R)STP Port Configuration” web page

Port Number
Indicates the number of the port currently selected.

Port Name
Indicates the name of the port.

STP Port State
Indicates the status in which this port takes part in STP.

Operational Edge Port
Indicates whether this port is operated as an edge port.

Admin Edge Port
Here you can specify whether this port is to be operated as an edge port (default setting), if possible.

Priority
Indicates the priority set for this port (default 128). Due to backward compatibility with STP, priority values can be set that are not configurable in RSTP.

Admin Path Cost
Indicates the path cost set for this port. A path cost equal to “0” activates the cost calculation according to the transmission speed (10 Mbps = 2000000; 100 Mbps = 200000; 1000 Mbps = 20000).

Path Cost
Indicates the path cost used for this port.

Forward Transitions
Indicates how often the port switches from the “Discarding” state to the “Forwarding” state.

Additional parameters provide information about the network paths in a stable topology that are used by the BPDU telegrams.

Designated Root
Root bridge for this Spanning Tree.

Designated Bridge
The switch from which the port receives the best BPDUs. The value is based on the priority value in hex and the MAC address.

Designated Port
Port via which the BPDUs are sent from the designated bridge. The value is based on the port priority (2 digits) and the port number.

Designated Cost
Indicates the path cost of this segment to the root switch.

Protocol Compatibility

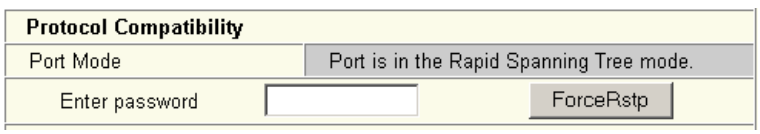


Figure 5-6 Protocol compatibility

If a port receives STP BPDUs, it switches automatically to STP mode. Automatic switching to (R)STP mode does not take place. Switching to (R)STP mode can only be forced via “ForceRSTP” or via a restart.

RSTP fast ring detection

The “RSTP Fast Ring Detection” function can be activated on the “RSTP Configuration” web page (see page 5-3).

This function speeds up the switch-over to a redundant path in the event of an error and provides easy diagnostics. RSTP fast ring detection provides each ring with an ID, this ID is made known to each switch in the relevant ring. A switch can belong to several different rings at the same time.

Structure of the ring ID

The ring ID consists of the port number of the blocking port and the MAC address of the corresponding switch. Advantages of the ring ID:

– Easier to identify redundant paths and locate blocking ports.
– Possible to check whether the desired topology corresponds to the actual topology.

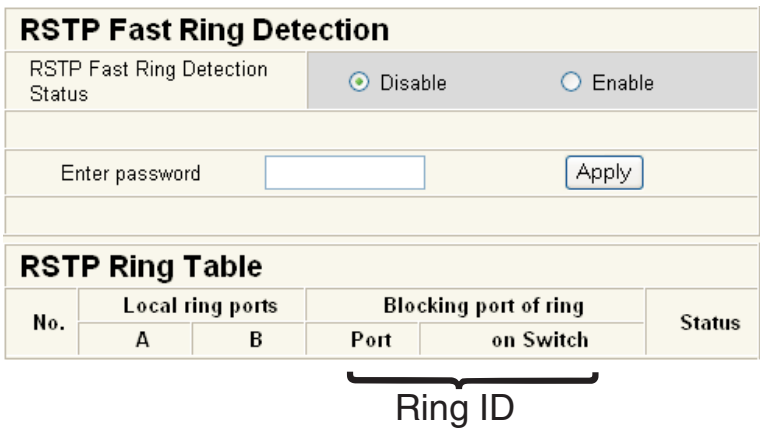


Figure 5-7 RSTP ring table

Information in WBM

The following information is displayed on the web page (and via SNMP):

Local ring ports
These two ports of this switch belong to the ring that is listed (ring ID).

Blocking port
This port deliberately breaks the loop.

	A blocking port does not receive LLDP BPDUs, but does send LLDP BPDUs.

Ring detection states

The following states can occur for ring detection:

– **Not Ready** - Ring detection has not yet been completed.
– **OK** - Ring detection has been completed and quick switch-over is possible in the event of an error.
– **Broken** - The ring is broken on this branch in the direction of the root switch.
– Failed on Port A - The ring was broken on this switch at port A.

	In the event of a link failure in the ring, the “trapRstpRingFailure” trap is sent.
	If “Broken” or “Failed” status lasts for longer than 60 seconds, it is no longer displayed after the next topology modification, since these rings no longer exist.

When using RSTP fast ring detection, please note the following:

– For RSTP fast ring detection, do **not** use devices that do **not** support this function.
– Enable RSTP fast ring detection on **all** devices.
– All data paths must be in full duplex mode.

5.1.2 Connection failure - Example

The following diagram illustrates an RSTP ring with six switches, where switch 1 is the root. The ring extends over port 1 and port 2 for each switch. On switch 4, the loop is broken by a blocking port.

If a cable interrupt occurs at the point indicated by the star, this produces the following entries on the “RSTP Fast Ring Detection” web page:

Switch 3 - Failed on Port A

Switch 4 - Broken

In addition, switch 3 would also generate the “flWorkLinkFailure” trap, as long as the sending of traps is not disabled.

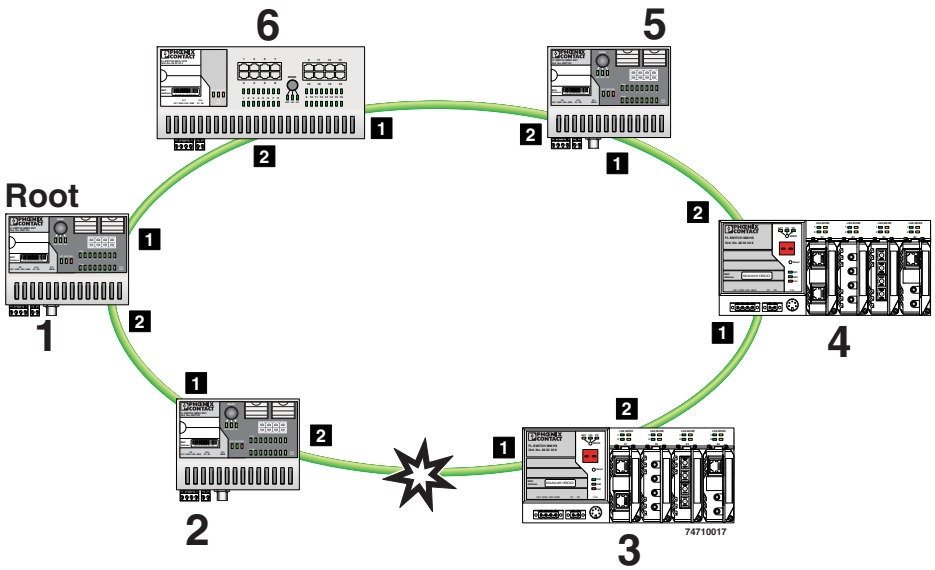


Figure 5-8 Connection failure with RSTP ring detection

5.1.3 Mixed operation of RSTP and STP

If a device with STP support is integrated into the network, only switch ports that receive STP BPDUs are set to STP mode. All other ports that receive RSTP BPDUs remain in RSTP mode.

5.1.4 Topology detection of a Rapid Spanning Tree network (RSTP)

(Rapid) Spanning Tree switches continually exchange information about the network topology using special messages (BPDUs - Bridge Protocol Data Units). In this way the switches “learn” the current network topology and - based on this information - make the following decisions:

– Which switch is selected as root switch
– Which data paths are disabled

If a switch is started using the (Rapid) Spanning Tree Protocol, it first expects to be the root switch. However, no data communication is possible during the startup phase until the current network topology has been learned and until the decisions described above have been made. Therefore loops which could otherwise occur during the network startup phase because no data path is interrupted, are prevented.

5.1.4.1 Topology modification

A topology modification can be triggered by the following:

– Adding a data path
– Failure of a data path
– Adding a Spanning Tree switch
– Failure of a Spanning Tree switch.

A topology modification is automatically detected and the network is reconfigured so that another tree is created and all the devices in this tree can be accessed. During this process, loops do not even occur temporarily.

If the sending of traps was not deactivated, two traps are generated:

– newRoot (OID: 1.3.6.1.2.1.17.0.1)
– topologyChange (OID 1.3.6.1.2.1.17.0.2)

5.1.4.2 Interrupted data paths and port states

The described data path interruption by the Spanning Tree protocol is created by disconnecting individual ports that no longer forward any data packets. A port can have the following states:

– Learning
– Forwarding
– Blocking/Discarding
– Disabled (link down or disconnected by the user)

The current port states are shown in the WBM.

The properties of the various port states are shown in the table below.

Table 5-1 Properties of the port states

	Receiving and evaluating BPDUs (learning the topology)	Learning the MAC addresses of connected devices and creating switching table	Forwarding data packets (normal switching function)
Disabled			
Blocking/Discarding	X		
Learning	X	X	
Forwarding	X	X	X

The sequence of the five port states defined in the Spanning Tree protocol cannot be assigned freely. The following diagram illustrates the possible sequence of the port states.

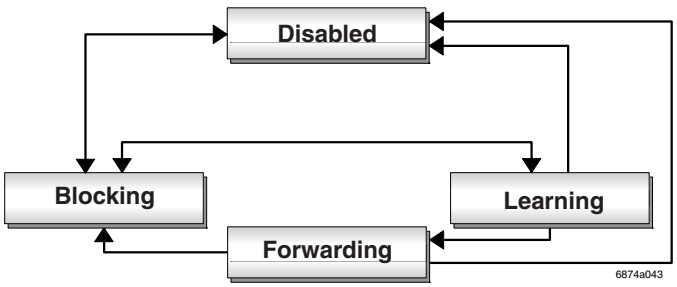


Figure 5-9 Sequence of the possible port states in STP

After device startup and, if necessary, also during topology modification, a port passes through the states in the following order:

Learning → Forwarding

or

Disabled → Blocking/Discarding

Due to the edge property of ports, they switch to “Forwarding” immediately. In the second case, the port generates a data path interruption in order to suppress loops accordingly.

At least one port in the “Forwarding” state is always at a data path between two Spanning Tree switches so that the data path can be integrated into the network.

5.1.4.3 Fast forwarding

If the Spanning Tree protocol is deactivated at a port, the corresponding port is in "fast forwarding" mode.

A fast forwarding port:

– Ignores all BPDUs that are received at this port
– Does not send any BPDUs
– Switches to the “Forwarding” state immediately after establishing the data link. Termination devices connected to this port can be accessed immediately.

“Port STP Status” in WBM on the “STP Port Configuration” page must be set to “Disabled” to activate fast forwarding.

Frame duplication

Due to the fast switch-over times of RSTP, frames may be duplicated and the order of frames may be changed.

5.1.4.4 Enabling via serial interface

Establish a connection to the switch. The procedure is described in Section “Management via local RS-232 communication interface” on page 4-39. Set “Spanning Tree, Enabled” on the following page in the “Redundancy” field and select “Save”.

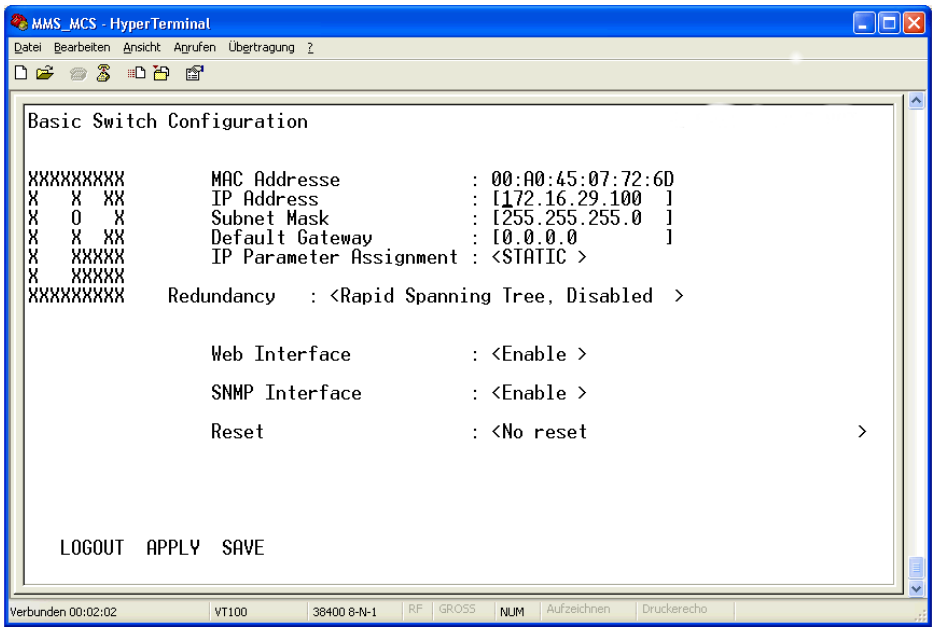


Figure 5-10 Activating rapid Spanning Tree

5.1.5 Configuration notes for Rapid Spanning Tree

In contrast to the Spanning Tree method, the Rapid Spanning Tree method supports event-controlled actions that are no longer triggered based on a timer.

If one cable fails (link down), the Rapid Spanning Tree method can respond more quickly to this failure and thus the switch-over time can be kept low.

A link down or link up must be detected at the switch so that the RSTP switches can detect a line failure and a restored line quickly. Please take into consideration, in particular, paths where media converters are used. If required, media converters offer setting options to transmit the link status of the fiber optic side to the twisted pair side.

If a link down is not detected at the switch because the cable interrupt is between the media converters, and no link down is forced at the switch, timer-based detection is activated, which may result in longer switch-over times.

- For short switch-over times, structure your network in such a way that a maximum of seven switches are located in a cascade up to the root switch. The switch-over times can range from 100 ms to 2 s.
- Use priority assignment to specify a central switch as the root.
- It is also recommended to assign a switch as the backup root.
- For short switch-over times, all switches in the redundant topology should support the Rapid Spanning Tree Protocol and should not use hubs.

5.1.5.1 Connecting the switches to form a meshed topology

Having activated (Rapid) Spanning Tree for all switches, you can create a meshed topology with redundant data paths. Any data links can now be created without taking loops into consideration. Loops can even be added on purpose in order to create redundant links.

A data path between Spanning Tree switches can be:

- A direct connection.
- A connection via one or more additional switches that do not support Spanning Tree.

If Spanning Tree is not supported by all of the switches used, the reconfiguration time for Spanning Tree is extended by the aging time of the switches without Spanning Tree support.

- A connection via one or more hubs that do not support Spanning Tree.

Furthermore, a data path can also consist of a connection of a Spanning Tree switch to:

- A termination device.
- A network segment in which **no** loops may occur, which consists of several infrastructure components (hubs or switches) without Spanning Tree support.

For the last two data path options, no specific precautionary measures are necessary. If necessary, you can use the “Fast Forwarding” option for the respective ports (see Section “Fast forwarding” on page 5-13).

For the first three cases, the following rules must be observed:

- **Rule 1: Spanning Tree transparency for all infrastructure components**
  All infrastructure components used in your network that do not actively support Spanning Tree must be transparent for Spanning Tree messages (BPDUs) and must forward all BPDUs to all ports without modifying them. When Spanning Tree is disabled, the switch is transparent for BPDUs.

– **Rule 2: At least one active Spanning Tree component per loop**
  An active Spanning Tree component supports the Spanning Tree protocol, sends/receives and evaluates BPDUs, and sets its ports to the relevant STP states. Each loop in a network must have at least one active Spanning Tree component to disintegrate the loop.
  Example:

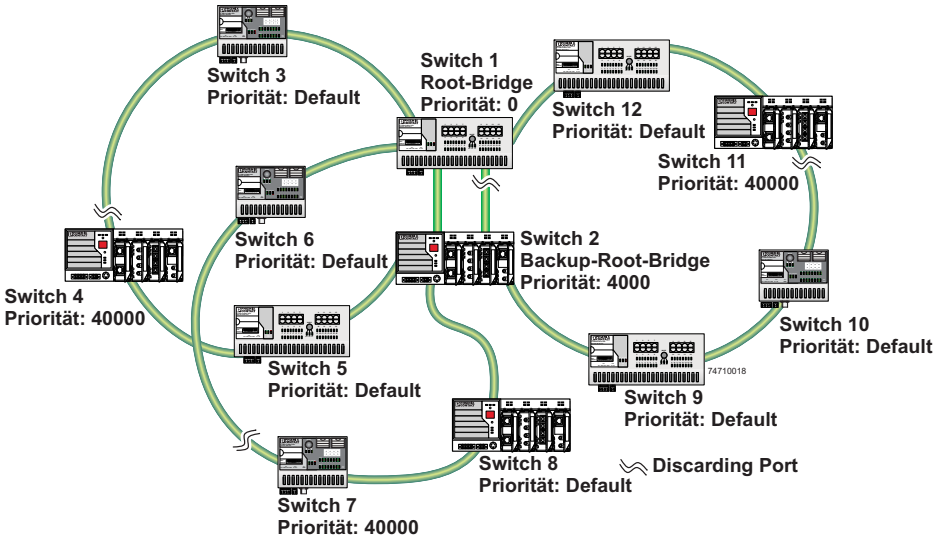


Figure 5-11 Example topology

The loops in the example topology illustrated are disabled by active RSTP components. The example topology contains three rings, the root and the backup root are components in each of the three rings. The three rings do not affect one another, a modification to the topology in one ring does not affect the topology of the other two rings.

– **Rule 3: No more than ten active Spanning Tree components in the topology when using Spanning Tree default setting**
  The ability to disintegrate any topology to form a tree without loops requires a complex protocol that works with several variable timers. These variable timers are dimensioned using the default values recommended by the IEEE standard so that a topology with a maximum of fifteen active Spanning Tree components always results in a stable network. When using large tree, please note the following (see also Section “Large Tree Support” on page 5-3):
– In the large tree support RSTP topology, **only** use devices that **support** large tree.
– Enable the “Large Tree Support” option on **all** devices.
– If RSTP is to be activated as the redundancy mechanism in an existing network with more than seven switches along the relevant path, then the “Large Tree Support” option must first be enabled on all devices.
– It is recommended that large tree support is not activated in networks with less than seven switches along the relevant path.

5.1.5.2 Example topologies

5.1.5.3 Redundant coupling of network segments

In this example, two network segments are connected via redundant data paths. Two RSTP components have ports in the “Blocking/Discarding” state (highlighted in gray). This is sufficient to operate the network.

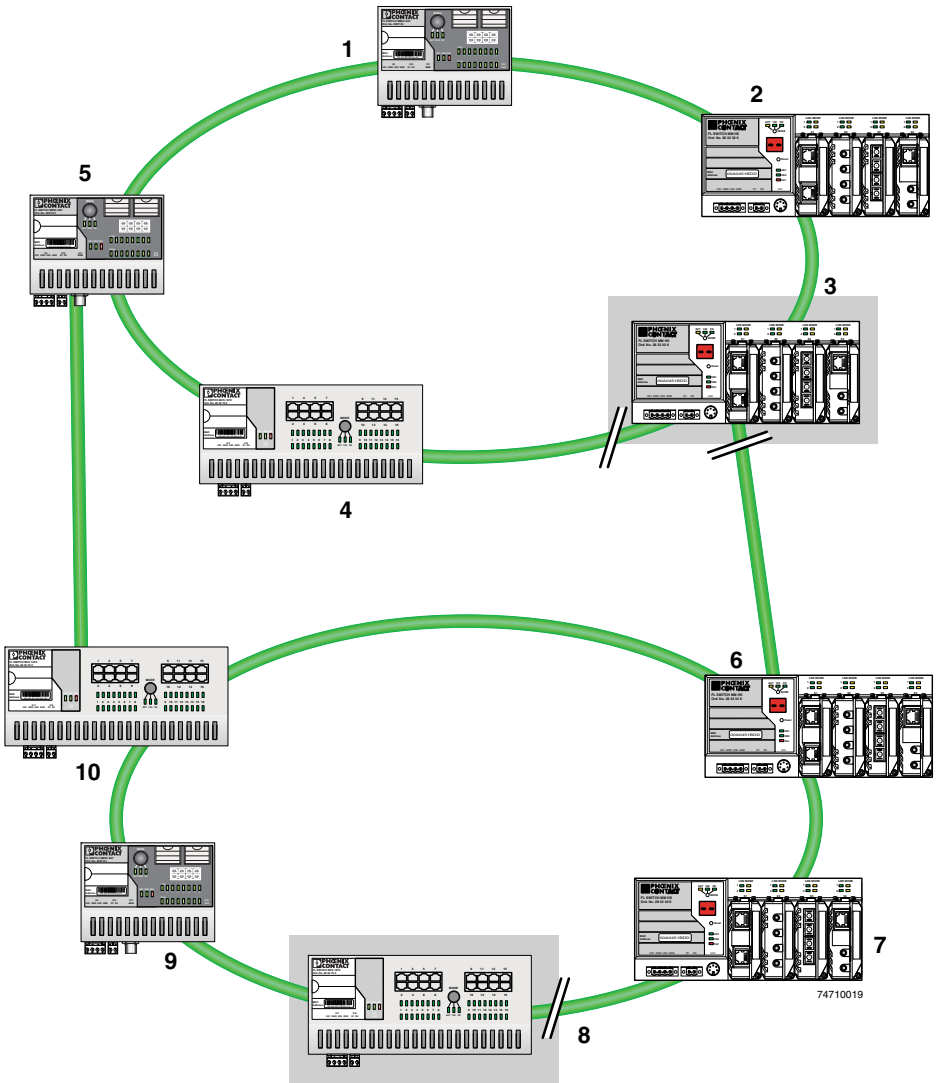


Figure 5-12 Redundant coupling of network segments

Example with fast ring detection

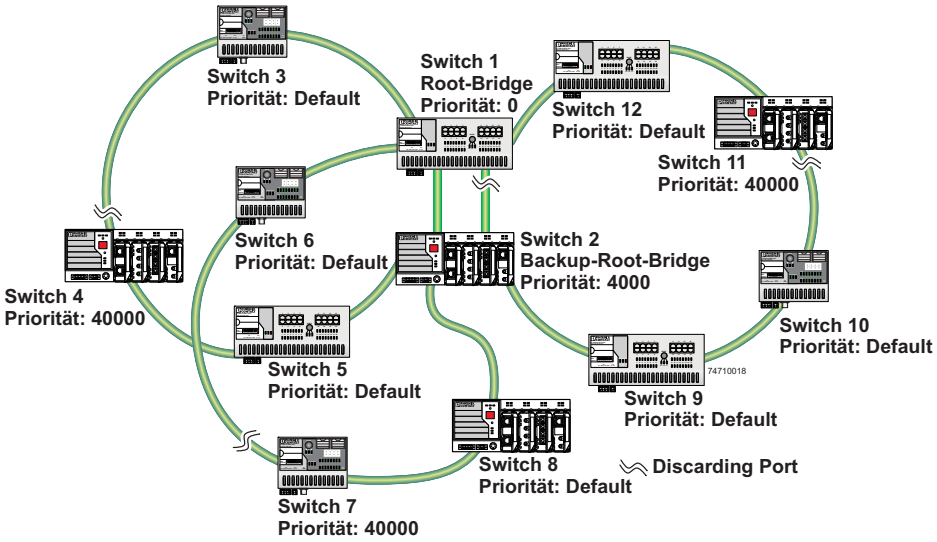


Figure 5-13 Example with fast ring detection

The switches in the illustrated example are arranged in such a way that two devices at the central position are configured as the root bridge and as the backup root bridge (via the priority).

The root bridge has the lowest priority, the backup root bridge has the second lowest priority. The root bridge and the backup root bridge are connected together redundantly. The remaining switches are networked in several rings in a ring topology. The end points of the ring are implemented on the root bridge and on the backup root bridge. The switch furthest away from the root bridge has a low priority as its default setting, e.g., 40000.

The advantage of this constellation is that the individual rings are not adversely affected in the event of an error.

5.1.5.4 Method of operation of the Spanning Tree Protocol (STP)

Path costs

In a LAN segment, data is distributed with different speeds and methods, e.g., 100 Mbps full duplex or 10 Mbps half duplex. The interconnection of network devices involves different transmission bandwidths and different performance characteristics - which means there are also different “path costs”.

“High path costs” are associated with low-performance connections, e.g., 10 Mbps half duplex, while “low path costs” are associated with connections with a high total transmission speed, e.g., 100 Mbps full duplex.

Components of a Spanning Tree domain

Designated switch

The switch that connects a specific LAN segment (with the lowest path costs) to the root switch.

Root port

The other switches set the port with the lowest path costs (or with the highest total transmission speed) as the root switch in the forwarding state.

There always is only one root port per switch.
Exception: The switch supports several Spanning Tree domains.

Designated ports

Ports in the forwarding state of the designated switch.
These are the ports with the “best” way to the root switch.

Switch ID

Priority and MAC address

The switch with the lowest bridge identifier is the root switch. The bridge identifier consists of the MAC address and the priority. Since the priority appears before the MAC address, the assignment of the appropriate priority clearly identifies the root switch, independent of the MAC address. The switch with the highest priority (lowest value) becomes the root switch. For every switch port within the network, a unique cost calculation is created. These root path costs are the sum of all path costs for one packet on the path between the root switch and corresponding switch port. The port of a switch with the lowest root path costs is always the active port. If the same root path costs have been calculated for two or more ports, the switch priority followed by the port priority determine the priority of the path.

Port ID

The port identifier consists of the path costs and the priority. Since the priority appears before the path costs, the assignment of the appropriate priority clearly identifies the root port, independent of the path costs. The port with the highest priority (lowest value) becomes the root port.

5.1.5.5 Processes in the Spanning Tree Protocol (STP)

Selecting the root switch

For every topology modification, every switch first assumes that it is the root switch and thus sends its own switch ID (e.g., the MAC address) into the network. All switches receive these messages (MAC multicast) and store the contents of the “best” message. The “best” message contains the following topology information: The root ID information and the cost information.

Having received the root ID information, the switch compares the following:

– The new root ID is saved if it has a higher priority than the IDs that are already saved (including its own ID).
– The path costs are checked if the root ID is the same as the one already saved. If they are lower, the ID is saved.
– If the root ID and the costs are the same, the ID of the sender is checked. If the ID is lower than the switch's own ID, it is saved.

– If the root ID, costs, and sender ID are the same, the priority of the sender port is the decisive criterion.

Selecting a designated switch

For every network the switch with the most favorable root connection is selected. This switch is called the designated switch.
The root switch is the designated switch for all directly connected networks.

Selecting a root port

Once the root switch has been specified by processing the root IDs, the switches now specify the root ports.

The most favorable path is specified by minimizing all connection costs on the path to the root switch. In addition, transmission speeds can also serve as costs. For the switch, the path costs added by each port for every HOP (the hop of a data packet from one point to the next) are preset to a value of 19 (default setting/recommended for 100 Mbps) and can be modified at any time by the user.

Selecting a designated port

At every “designated switch” the port with the most cost-effective data link in the direction of the root switch is called the designated port.

Port costs

The port costs can be set according to two different standards, 802.1D (STP) or 801.1W (RSTP).

If, in addition to Phoenix Contact devices, devices from other manufacturers are also used, it is recommended that the port costs are set according to a uniform standard.

The “dot1dstpPathCostDefault” SNMP object (OID 1.3.6.1.2.1.17.2.18) can be used to change the standard that is used.

Table 5-2 Port costs according to 802.D

Transmission speed	Recommended value	Recommended range
10 Mbps	100	50 - 600
100 Mbps	19	10 - 60

Table 5-3 Port costs according to 802.W

Transmission speed	Recommended value	Recommended range
10 Mbps	2 000 000	200 000 - 20 000 000
100 Mbps	200 000	20 000 - 2 000 000
1000 Mbps	20 000	2 000 - 200 000

5.1.5.6 Flowchart for specifying the root path

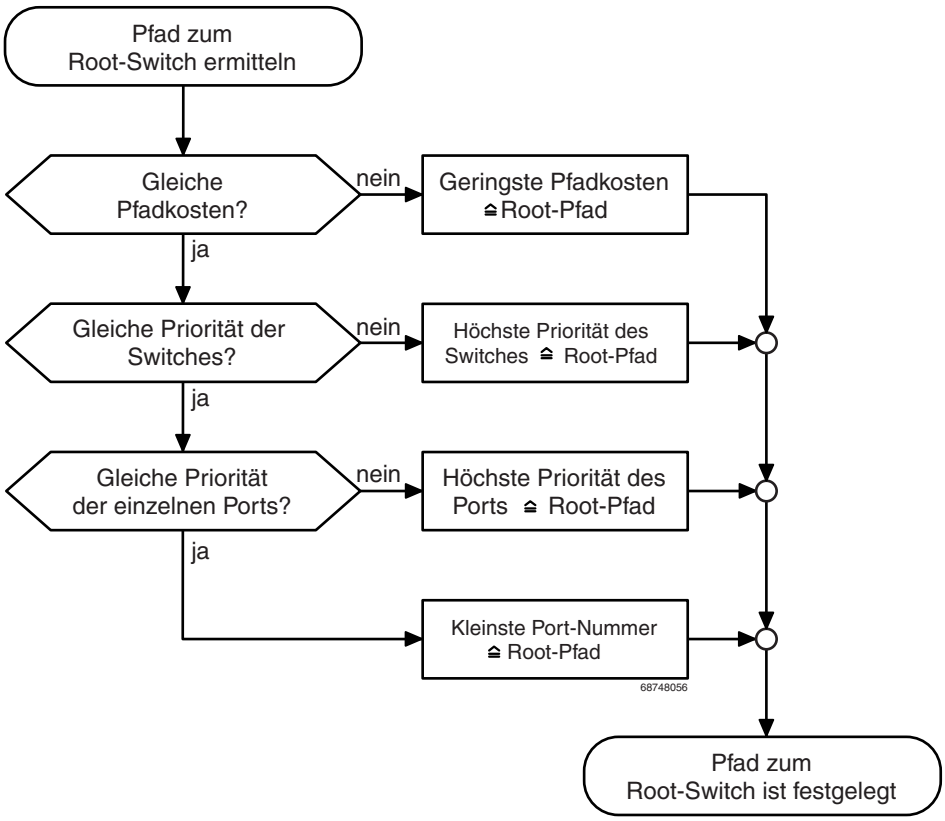


Figure 5-14 Flowchart for specifying the root path

5.1.5.7 Extended configuration

It may be practical to actively specify the topology that forms from the Spanning Tree protocol and not to leave it to the random MAC addresses of the switches involved. Non-blocking/blocking data paths can thus be influenced and a load distribution specified. It may also be practical to explicitly deactivate the Spanning Tree protocol at those ports that do not participate in Spanning Tree so as to benefit from the fast forwarding function. The Spanning Tree protocol also must be deactivated at individual ports if two different network segments - both using Spanning Tree - are to be coupled via these ports without the two tree structures melting to a large Spanning Tree.

Specifying the root switch

The root switch is assigned via the assignment of an appropriate priority for the Spanning Tree segment. Set the highest priority (lowest value) in the “Priority” field on the “STP Bridge Configuration” page in WBM for the switch selected as the root switch. Make sure that all the other network switches have a lower priority (higher value). Here, the set path costs are not evaluated.

Specifying the root port or designated port

The root port and designated port are always the ports with the lowest path costs. If the costs are the same, the priority is the decisive criterion. If the priorities are also the same, the port number is the decisive criterion. Specify an appropriate combination of costs and

priority on the “STP Port Configuration” page in WBM for the port specified as the root port or designated port. Make sure that all the other network switches either have higher costs or a lower priority (higher value).

5.1.5.8 Disabling the Spanning Tree protocol/using the fast forwarding function

One of the following requirements must be met so that the Spanning Tree protocol can be disabled for a port:

- A termination device is connected to the port.
- Additional infrastructure components are connected to the port. The corresponding network segment does not contain any loops.
- Additional infrastructure components are connected to the port, forming a Spanning Tree of their own. No additional redundant connections to this network segment are permitted.

5.1.5.9 Modifying the protocol timers

Modifying the protocol timers may result in unstable networks.

It may be necessary to modify the protocol timers if, e.g., there are more than ten active Spanning Tree components in a single network. You can also try to reduce the reconfiguration times by modifying the timers. However, care should be taken in order to prevent unstable networks.
Please note that the protocol times are specified by the root switch and that they are distributed to all devices via BPDU. It is therefore only necessary to modify the values in the root switch. If the root switch fails, the timer values of another active STP switch (i.e., the new root switch) will be valid for the entire network segment. Please remember this during component configuration.

Specifying the timer values (STP and RSTP)

– Maximum number of active Spanning Tree components along the path beginning at the root switch (please refer to the following two example illustrations):
= (MaxAge / 2) - Hello Time + 1
– 2 x (Forward Delay - 1 s) ≥ MaxAge
– MaxAge ≥ 2 × (HelloTime + 1 s)

The value ((MaxAge / 2) - Hello Time) for a ring topology corresponds to the maximum number of components with active Spanning Tree.

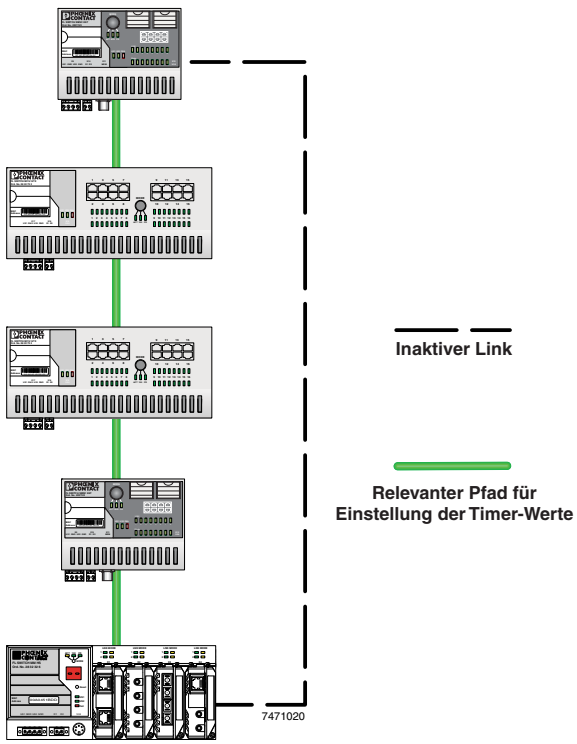


Figure 5-15 Example 1 for the “relevant path”

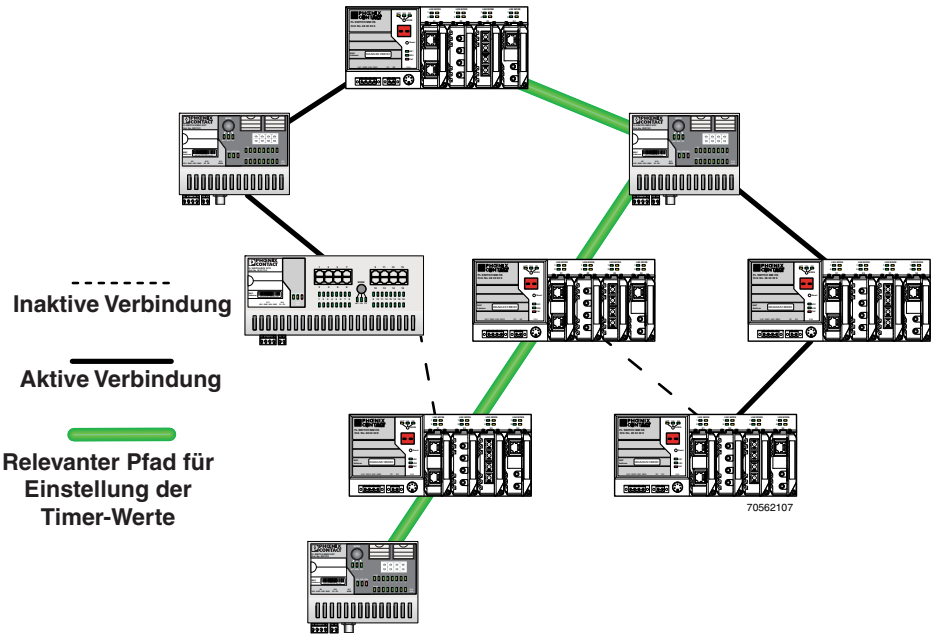


Figure 5-16 Example 2 for the “relevant path”

5.1.5.10 Reconfiguration times

The reconfiguration time for a Spanning Tree depends on the timer values for MaxAge and Forward Delay.

The minimum reconfiguration time is: 2 × ForwardDelay

The maximum reconfiguration time is: 2 × Forward Delay + MaxAge

For the values recommended by the IEEE standard, the value for ten active STP switches along a path beginning with the root switch is between 30 s and 50 s.

Switch-over time response to be expected for RSTP and RSTP with activated fast ring detection

When using **RSTP,** expect switch-over times in the range from **100 ms to 2 s**.

When using **fast ring detection,** expect switch-over times in the range from **100 ms to 500 ms**.

The various roles of ports

The **root port** of a switch connects this switch to the root switch - either directly or via another switch (designated switch).

The **designated port** is the port at a designated switch that is connected to the root port of the next switch.

No additional switches/bridges are connected to **edge ports**. Termination devices are connected to edge ports.

An **alternate port** is a path to the root, which, however, did not become a root port. I.e., this port is not part of the active topology.

6 Media Redundancy Protocol (MRP)

6.1 General function

MRP stands for Media Redundancy Protocol. A ring topology ensures a switch-over time of 200 ms - 500 ms and is part of PROFINET standard IEC 61158.

A ring topology prevails. One switch is defined as the MRP manager, the rest are defined as MRP clients. The MRP manager opens the port logically, i.e., the ring is only logically interrupted (physically, the ring is still present). The data is transmitted over the network.

The MRP manager constantly sends test telegrams, known as watchdogs, via the logically closed port. In the event of an error in the network, this is detected by the MRP manager and the watchdog path is switched as a data cable.

If the error has been removed, this will also be detected by the MRP manager. The watchdog path is automatically switched back and used again for test telegrams.

MRP manager

For licensing reasons, the switch that is configured as the MRP manager in the ring must have a license key (FL MEM PLUG/MRM, Order No. 2891275).

You will require one license key for each MRP manager (for the configuration of the MRP manager, see 6.3 “Configuration of MRP”).

Please note that MRP is disabled by default upon delivery.

6.1.1 Network examples

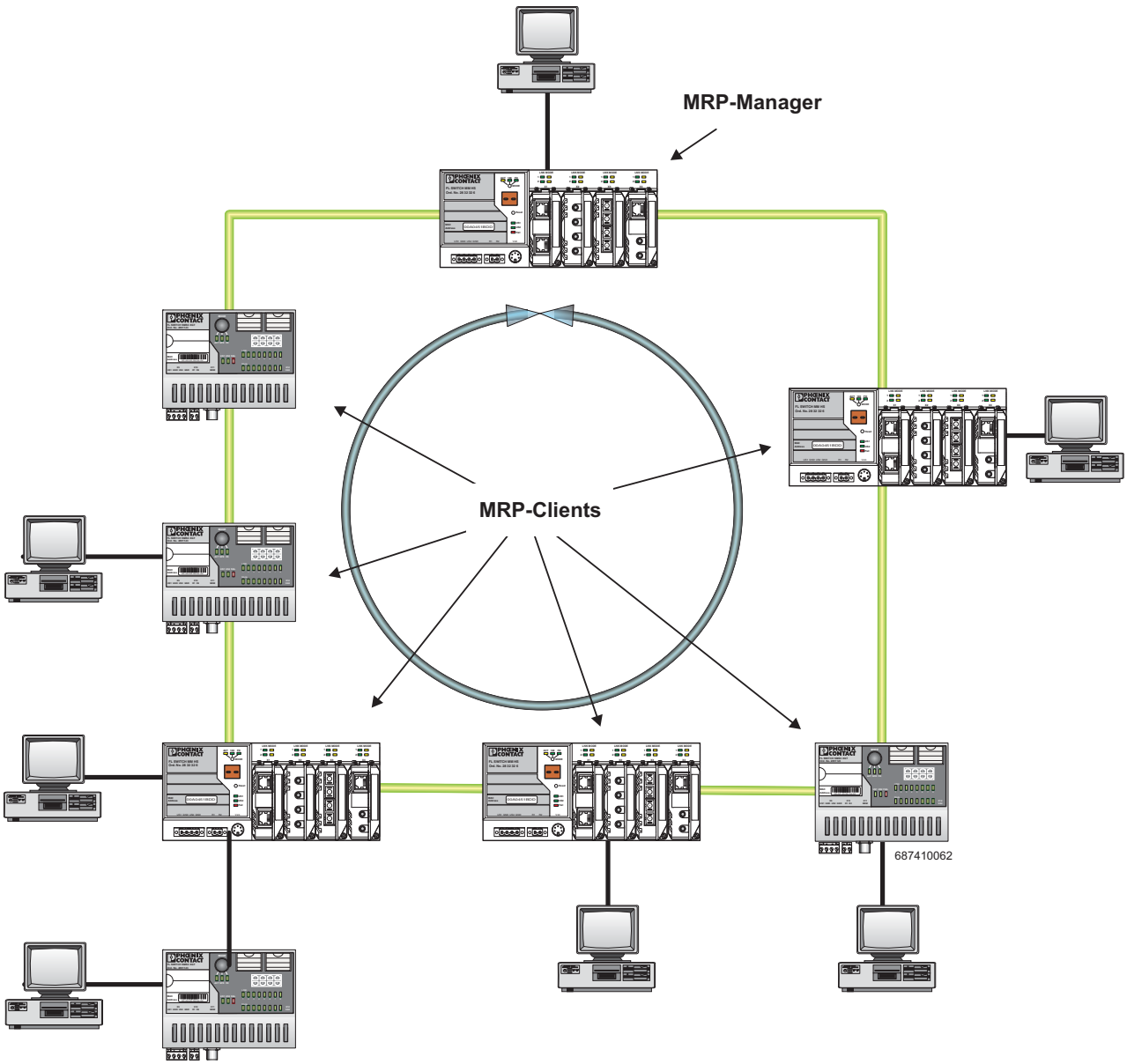


Figure 6-1 Example of an MRP ring

Make sure that the topology used does not contain an invalid mixture of RSTP and MRP, e.g., by **additionally** coupling two of the devices through an RSTP connection rendering them redundant.

6.1.1.1 Example of a permissible network with MRP and (R)STP

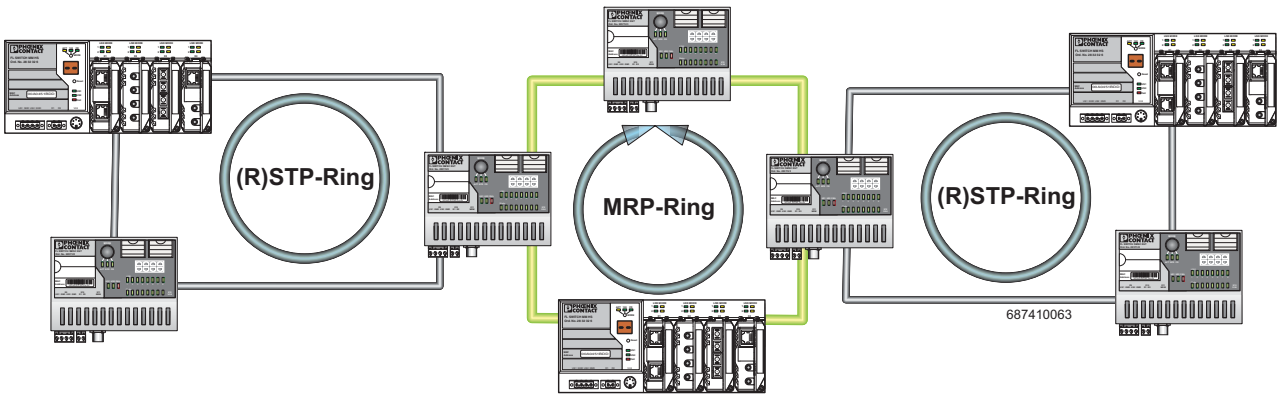


Figure 6-2 Permissible example of MRP with (R)STP

6.1.1.2 Example of an impermissible network with MRP and (R)STP

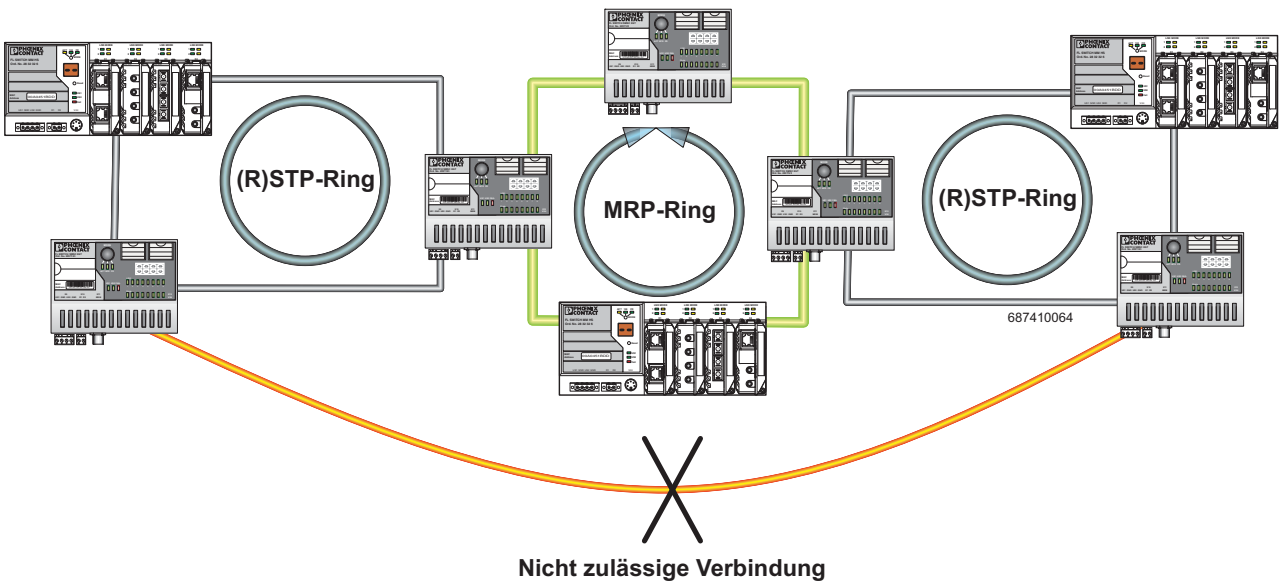


Figure 6-3 Impermissible example

6.2 Enabling web pages for using MRP in WBM

Activate WBM for the switches in a web browser. Switch to the “General Configuration” menu, then to the “User Interfaces” page. Activate “Redundancy” and confirm by entering your password.

Activating “Redundancy” under “General Configuration/User Interfaces” does not activate a redundancy mechanism. In the WBM menu, the “Media Redundancy” page - under which the function can be configured and activated - is enabled.

6.3 Configuration of MRP

6.3.1 MRP General

The “MRP General” web page shows the current parameters set for using the protocol. The following information is displayed:

– Operating mode (Disabled or MRP Client)
– License key (Present or Missing)
– Topology modification counter
– Time of last topology modification
– Ring port numbers and status of the ports (Forwarding or Blocking)

The switch with the current firmware can only be operated as an MRP client.

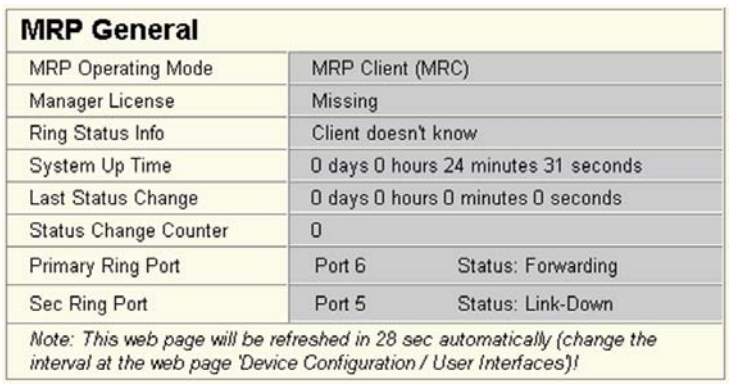


Figure 6-4 “MRP General” web page for an MRP client

6.3.2 MRP Configuration

The “MRP Configuration” web page is used to configure the protocol parameters. The following configuration parameters are displayed:

– Device role (Disabled or MRP Client)
– Selection of the ring ports that are integrated in the MRP ring

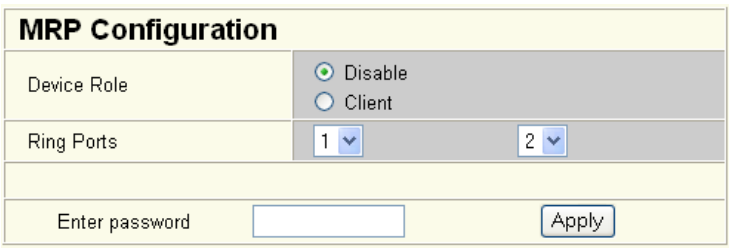


Figure 6-5 “MRP Configuration” web page

7 LLDP (Link Layer Discovery Protocol)

7.1 Basics

LLDP

The switch supports LLDP according to IEEE 802.1ab and enables topology detection of devices that also have LLDP activated.

Advantages of using LLDP:

– Improved error location detection.
– Improved device replacement.
– More efficient network configuration.

The following information is received by neighbors or transmitted to neighbors, as long as LLDP is activated:

– The device transmits its own management and connection information to neighboring devices.
– The device receives management and connection information from neighboring devices.

Displaying LLDP information

The information that is collected is presented in a table in WBM. The table includes the port numbers that are used to connect both devices together, as well as the IP address, the device name of neighboring devices, and the device type.

Please note that a blocking port using RSTP does not receive LLDP BPDUs, but does send them.

LLDP General

The Link Layer Discovery Protocol (LLDP) according to 802.1ab is used by network devices to learn and maintain the individual neighbor relationships.

Function

A network infrastructure component transmits a port-specific BPDU (Bridge Protocol Data Unit), which contains the individual device information, at the “Message Transmit Interval” to each port in order to distribute topology information. The partner connected to the relevant port learns the corresponding port-specific neighbors from these BPDUs.

The information learned from the BPDUs is saved for a defined period of time as the TTL value (TTL - Time To Live). Subsequent receipt of the same BPDUs increases the TTL value again and the information is still saved. If the TTL elapses, the neighbor information is deleted.

An FL NAT SMN 8TX(-M) manages a maximum of 50 items of neighbor information, all other information is ignored.

If several neighbors are displayed on one switch port, then there must be at least **one other** switch/hub, which does not support or has not activated LLDP, installed **between** this switch and the neighbor indicated.

Table 7-1 Event table for LLDP

Event	Activity of the individual LLDP agent	Response of the neighboring LLDP agent
Activate LLDP agent or device startup	Transmit LLDP BPDUs to all ports	Include sender in the list of neighbors
Deactivate LLDP agent or software reset	Transmit LLDP BPDUs with a TTL value of 0 seconds to all ports	Delete sender from the list of neighbors
Link up	Send port-specific LLDP BPDUs	Include sender in the list of neighbors
Link down	Delete all neighbors for this port	-
Timer (Message Transmit Interval)	Cyclic transmission of BPDUs to all ports	Update information
Aging (Time To Live)	Delete neighbor information	-
Receiving a BPDU from a new neighbor	Extend list of neighbors and respond with port-specific BPDU	Include sender in the list of neighbors

Link Layer Discovery Protocol

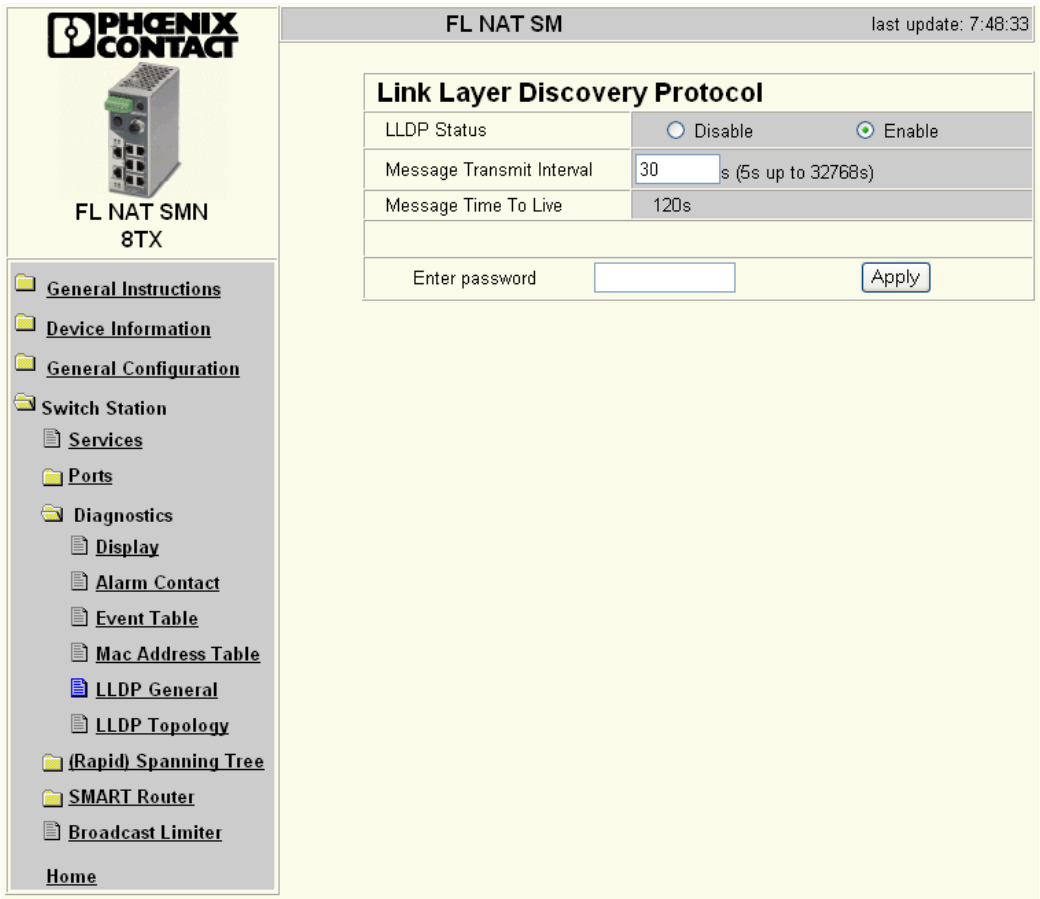


Figure 7-1 “Link Layer Discovery Protocol” web page

The “Message Time To Live” is determined by multiplying the “Message Transmit Interval” with the “Message Transmit Hold Multiplier”. The “Message Transmit Hold Multiplier” can only be modified via SNMP. The default value is four.

LLDP Topology

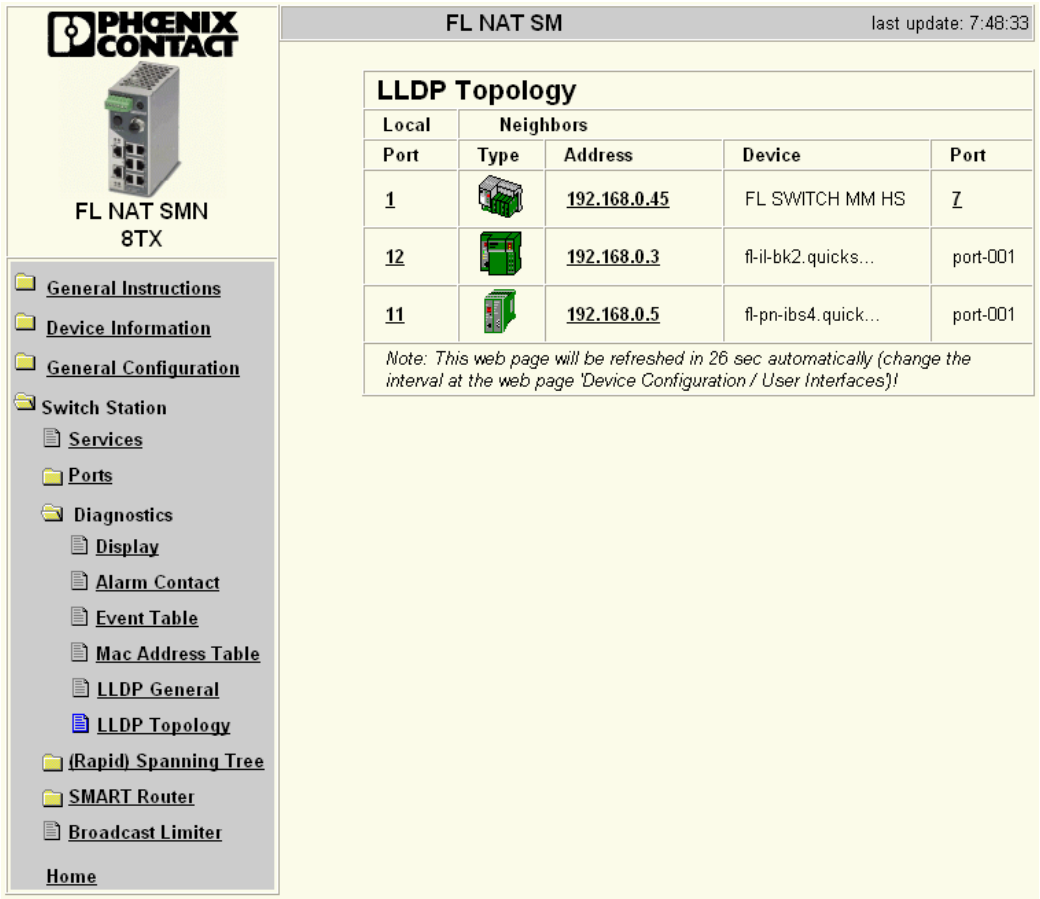


Figure 7-2 “LLDP Topology” web page

A table is created for known neighbors and contains the following five columns:

– Local Port
  Contains the port number of the local switch that is used to connect a neighbor to this switch. The port number is also a link to the local “Port Configuration” web page.
– Type
  An icon is displayed here, which corresponds to the neighboring device type. “Ethernet Device” is displayed in general for devices produced by other manufacturers.
– Address
  Indicates the management IP address for the neighbor.
– Device
  Indicates the system name of the neighbor.
– Indicates the port number of the neighboring switch that is used to connect the neighbor to the local switch. If the neighbor is identified as a Phoenix Contact switch, the port number is implemented as a link to the “Port Configuration” web page for the neighbor.

8 Technical data and ordering data

8.1 Technical data

General data	
Function	Smart Managed Narrow Switch, Ethernet/Fast Ethernet switch with routing; 1:1 NAT; conforms to standard IEEE 802.3/802.3u/802.3ab
Switch principle	Store-and-forward
Address table	4000 MAC addresses
SNMP	Version 2c
Transmission capacity per port 64-byte packet size, half duplex	At 10 Mbps: 14880 pps (packets per second) at 100 Mbps: 148800 pps
Supported MIBs	MIB II and private SNMP objects from Phoenix Contact
Housing dimensions (width x height x depth) in mm	56 x 133 x 120 (depth from top edge of DIN rail) 56 x 133 x 172 (depth from top edge of DIN rail) with FL MEM PLUG (accessories)
Permitted operating temperature	0°C to 55°C
Permitted storage temperature	-40°C to +85°C
Degree of protection	IP20, IEC 60529
Protection class	Class 3 VDE 0106; IEC 60536
Humidity	
Operation	5% ... 95%, non-condensing
Storage	5% ... 95%, non-condensing
Air pressure	
Operation	86 kPa to 108 kPa, 1500 m above sea level
Storage	66 kPa to 108 kPa, 3500 m above sea level
Ambient compatibility	Free from substances that would hinder coating with paint or varnish according to VW specification
Mounting position	Perpendicular to a standard DIN rail
Connection to protective earth ground	By snapping it onto a grounded DIN rail
Weight	650 g, typical

Supply voltage (US1/US2 redundant)	
Connection	Via COMBICON; maximum conductor cross section = 2.5 mm^2
Nominal value	24 V DC
Permissible voltage range	18.0 V DC to 32.0 V DC
Permissible ripple (within the permissible voltage range)	3.6 V_{pp}
Test voltage	500 V DC for 1 minute
Current consumption on US at 24 V DC, maximum	0.6 A
Maximum power consumption	14.5 W

Interfaces on the switch	
Number of Ethernet ports	7+1
RS-232 communication interface	
Connection format	Mini-DIN socket

Interfaces on the switch [...]

Floating alarm contact	
Voltage	24 V DC
Current carrying capacity	100 mA

Ethernet interfaces

Properties of RJ45 ports

Number	7+1 with autocrossing and auto negotiation
Connection format	8-pos. RJ45 socket on the switch
Connection medium	Twisted pair cable with a conductor cross section of 0.14 mm^2 to 0.22 mm^2
Cable impedance	100 ohms
Transmission speed	10/100 Mbps
Maximum network segment length	100 m

Mechanical tests

Shock test according to IEC 60068-2-27	Operation: 25 g, Half-sine shock pulse Storage/transport: 50 g, Half-sine shock pulse
Vibration resistance according to IEC 60068-2-6	Operation/storage/transport: 5g, 10 - 150 Hz
Free fall according to IEC 60068-2-32	1 m

Conformance with EMC directives

Developed according to IEC 61000-6.2, EN 61000-6-3, and 2004/108/EC

Additional certification

RoHS	EEE 2002/95/EC. - WEEE 2002/96/EC

Differences between this version and previous versions

Rev. 00: First version

Rev. 01: Technical data added

Rev. 02: Smart mode added

Rev. 03: Startup information adapted

Rev. 04: Maritim version added

8.2 Ordering data

Products

Description	Order designation	Order No.	Pcs. / Pkt.
Smart Managed Narrow Switch and router with eight TX ports in RJ45 format	FL NAT SMN 8TX	2989365	1
Smart Managed Narrow Switch and router with eight TX ports in RJ45 format and maritim approval	FL NAT SMN 8TX-M	2702443	1
Replaceable configuration memory	FL MEM PLUG	2891259	1
Replaceable configuration memory with MRP manager	FL MEM PLUG/MRM	2891770	1

Accessories

Description	Order designation	Order No.	Pcs. / Pkt.
Configuration cable, for connecting the switch to a PC, RS-232	PRG CAB MINI DIN	2730611	1
Universal end clamp	E/NS 35 N	0800886	1
Network monitoring with HMI/SCADA systems	FL SMNP OPC SERVER V3	2701139	1
Patchbox 8 x RJ45 CAT5e, pre-assembled, can be retrofitted	FL PBX 8TX	2832496	1
Patchbox 6 x RJ45 CAT5e and 4 SC-RJ (fiberglass) pre-assembled, can be retrofitted	FL PBX 6TX/4FX	2832506	1
Angled patch connector with two RJ45 CAT5e network connections including Layer 1 security elements	FL PF SEC 2TX	2832687	1
Angled patch connector with eight RJ45 CAT5e network connections including Layer 1 security elements	FL PF SEC 8TX	2832690	1
Angled patch connector with two RJ45 CAT5e network connections	FL PF 2TX CAT5E	2891165	1
Angled patch connector with eight RJ45 CAT5e network connections	FL PF 8TX CAT5E	2891178	1
Angled patch connector with two RJ45 CAT6 network connections	FL PF 2TX CAT 6	2891068	1
Angled patch connector with eight RJ45 CAT6 network connections	FL PF 8TX CAT 6	2891071	1
Patch cable, CAT**6**, pre-assembled, 0.3 m long	FL CAT6 PATCH 0,3	2891181	10
Patch cable, CAT**6**, pre-assembled, 0.5 m long	FL CAT6 PATCH 0,5	2891288	10
Patch cable, CAT**6**, pre-assembled, 1.0 m long	FL CAT6 PATCH 1,0	2891385	10
Patch cable, CAT**6**, pre-assembled, 1.5 m long	FL CAT6 PATCH 1,5	2891482	10
Patch cable, CAT**6**, pre-assembled, 2.0 m long	FL CAT6 PATCH 2,0	2891589	10
Patch cable, CAT**6**, pre-assembled, 3.0 m long	FL CAT6 PATCH 3,0	2891686	10
Patch cable, CAT**6**, pre-assembled, 5.0 m long	FL CAT6 PATCH 5,0	2891783	10
Patch cable, CAT**6**, pre-assembled, 7.5 m long	FL CAT6 PATCH 7,5	2891880	10
Patch cable, CAT**6**, pre-assembled, 10 m long	FL CAT6 PATCH 10	2891887	10
Patch cable, CAT**6**, pre-assembled, 12.5 m long	FL CAT6 PATCH 12,5	2891369	5
Patch cable, CAT**6**, pre-assembled, 15 m long	FL CAT6 PATCH 15	2891372	5
Patch cable, CAT**6**, pre-assembled, 20 m long	FL CAT6 PATCH 20	2891576	5
Patch cable, CAT5, pre-assembled, 0.3 m long	FL CAT5 PATCH 0,3	2832250	10
Patch cable, CAT5, pre-assembled, 0.5 m long	FL CAT5 PATCH 0,5	2832263	10
Patch cable, CAT5, pre-assembled, 1.0 m long	FL CAT5 PATCH 1,0	2832276	10
Patch cable, CAT5, pre-assembled, 1.5 m long	FL CAT5 PATCH 1,5	2832221	10
Patch cable, CAT5, pre-assembled, 2.0 m long	FL CAT5 PATCH 2,0	2832289	10
Patch cable, CAT5, pre-assembled, 3.0 m long	FL CAT5 PATCH 3,0	2832292	10
Patch cable, CAT5, pre-assembled, 5.0 m long	FL CAT5 PATCH 5,0	2832580	10
Patch cable, CAT5, pre-assembled, 7.5 m long	FL CAT5 PATCH 7,5	2832616	10
Patch cable, CAT5, pre-assembled, 10.0 m long	FL CAT5 PATCH 10	2832629	10

Description [...]	Order designation	Order No.	Pcs. / Pkt.
Color marking for FL CAT5/6 PATCH ..., black	FL PATCH CCODE BK	2891194	20
Color marking for FL CAT5/6 PATCH ..., brown	FL PATCH CCODE BN	2891495	20
Color marking for FL CAT5/6 PATCH ..., blue	FL PATCH CCODE BU	2891291	20
Color marking for FL CAT5/6 PATCH ..., green	FL PATCH CCODE GN	2891796	20
Color marking for FL CAT5/6 PATCH ..., gray	FL PATCH CCODE GY	2891699	20
Color marking for FL CAT5/6 PATCH ..., red	FL PATCH CCODE RD	2891893	20
Color marking for FL CAT5/6 PATCH ..., violet	FL PATCH CCODE VT	2891990	20
Color marking for FL CAT5/6 PATCH ..., yellow	FL PATCH CCODE YE	2891592	20
Lockable security element for FL CAT5/6 PATCH ...	FL PATCH GUARD	2891424	20
Color marker for FL PATCH GUARD, black	FL PATCH GUARD CCODE BK	2891136	12
Color marker for FL PATCH GUARD, blue	FL PATCH GUARD CCODE BU	2891233	12
Color marker for FL PATCH GUARD, green	FL PATCH GUARD CCODE GN	2891631	12
Color marker for FL PATCH GUARD, orange	FL PATCH GUARD CCODE OG	2891330	12
Color marker for FL PATCH GUARD, red	FL PATCH GUARD CCODE RD	2891738	12
Color marker for FL PATCH GUARD, turquoise	FL PATCH GUARD CCODE TQ	2891534	12
Color marking for FL PATCH GUARD, violet	FL PATCH GUARD CCODE VT	2891835	12
Color marker for FL PATCH GUARD, yellow	FL PATCH GUARD CCODE YE	2891437	12
Key for FL PATCH GUARD	FL PATCH GUARD KEY	2891521	1
Security element for FL CAT 5/6 PATCH ...	FL PATCH SAFE CLIP	2891246	20

HOTLINE:

If there are any problems that cannot be solved using this documentation, please call our hotline:


+ 49 - (0) 52 81 - 946 2888