Configuration of the FL SWITCH 2000 and FL NAT 2000 product family

User manual

PHOENIX CONTACT
INSPIRING INNOVATIONS

User manual

Configuration of the FL SWITCH 2000 and FL NAT 2000 product family

UM EN SW FL SWITCH 2000, Revision 01 2020-07-07

This user manual is valid for:

Designation	Order No.	Designation	Order No.
FL SWITCH 2005	2702323	FL SWITCH 2306-2SFP	2702970
FL SWITCH 2008	2702324	FL SWITCH 2306-2SFP PN	1009222
FL SWITCH 2008F	1106707	FL SWITCH 2304-2GC-2SFP	2702653
FL SWITCH 2016	2702903	FL SWITCH 2316	2702909
FL SWITCH 2105	2702665	FL SWITCH 2316 PN	1031673
FL SWITCH 2108	2702666	FL SWITCH 2314-2SFP	1006191
FL SWITCH 2116	2702908	FL SWITCH 2314-2SFP PN	1031683
FL SWITCH 2205	2702326	FL SWITCH 2312-2GC-2SFP	2702910
FL SWITCH 2208	2702327	FL SWITCH 2408	1043412
FL SWITCH 2208C	1095627	FL SWITCH 2408 PN	1089133
FL SWITCH 2208 PN	1044024	FL SWITCH 2406-2SFX	1043414
FL SWITCH 2207-FX	2702328	FL SWITCH 2406-2SFX PN	1089126
FL SWITCH 2207-FX SM	2702329	FL SWITCH 2404-2TC-2SFX	1088853
FL SWITCH 2206-2FX	2702330	FL SWITCH 2416	1043416
FL SWITCH 2206C-2FX	1095628	FL SWITCH 2416 PN	1089150
FL SWITCH 2206-2FX SM	2702331	FL SWITCH 2414-2SFX	1043423
FL SWITCH 2206-2FX ST	2702332	FL SWITCH 2414-2SFX PN	1089139
FL SWITCH 2206-2FX SM ST	2702333	FL SWITCH 2412-2TC-2SFX	1088875
FL SWITCH 2206-2SFX	2702969	FL SWITCH 2508	1043484
FL SWITCH 2206-2SFX PN	1044028	FL SWITCH 2508 PN	1089134
FL SWITCH 2204-2TC-2SFX	2702334	FL SWITCH 2506-2SFP	1043491
FL SWITCH 2216	2702904	FL SWITCH 2506-2SFP PN	1089135
FL SWITCH 2216 PN	1044029	FL SWITCH 2504-2GC-2SFP	1088872
FL SWITCH 2214-2FX	2702905	FL SWITCH 2516	1043496
FL SWITCH 2214-2FX SM	2702906	FL SWITCH 2516 PN	1089205
FL SWITCH 2214-2SFX	1006188	FL SWITCH 2514-2SFP	1043499
FL SWITCH 2214-2SFX PN	1044030	FL SWITCH 2514-2SFP PN	1089154
FL SWITCH 2212-2TC-2SFX	2702907	FL SWITCH 2512-2GC-2SFP	1088856
FL SWITCH 2308	2702652	FL NAT 2008	2702881
FL SWITCH 2308 PN	1009220	FL NAT 2208	2702882
		FL NAT 2304-2GC-2SFP	2702981

108998_en_01

PHOENIX CONTACT GmbH & Co. KG • Flachsmarktstraße 8 • 32825 Blomberg • Germany
phoenixcontact.com

Table of contents

1 For your safety

Read this user manual carefully and keep it for future reference.

1.1 Identification of warning notes

This symbol indicates hazards that could lead to personal injury.

There are three signal words indicating the severity of a potential injury.

DANGER
Indicates a hazard with a high risk level. If this hazardous situation is not avoided, it will result in death or serious injury.

WARNING
Indicates a hazard with a medium risk level. If this hazardous situation is not avoided, it could result in death or serious injury.

CAUTION
Indicates a hazard with a low risk level. If this hazardous situation is not avoided, it could result in minor or moderate injury.

This symbol together with the **NOTE** signal word warns the reader of actions that might cause property damage or a malfunction.

Here you will find additional information or detailed sources of information.

1.2 Qualification of users

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

– Electrically skilled persons or persons instructed by them. The users must be familiar with the relevant safety concepts of automation technology as well as applicable standards and other regulations.
– Qualified application programmers and software engineers. The users must be familiar with the relevant safety concepts of automation technology as well as applicable standards and other regulations.

1.3 Product changes

Modifications to hardware and firmware of the device are not permitted.

Incorrect operation or modifications to the device can endanger your safety or damage the device. Do not repair the device yourself. If the device is defective, please contact Phoenix Contact.

2 Startup and function

2.1 Delivery state/factory settings

2.1.1 Initial IP configuration in the delivery state

2.1.1.1 Firmware revision 2.72 and earlier

The device does not have an initial IP configuration.

2.1.1.2 Firmware revision 2.80

In the delivery state, the device has an initial static IP configuration, which enables you to access the web-based management and to assign an IP address.

– IP address: 169.254.2.1
– Subnet mask: 255.255.0.0

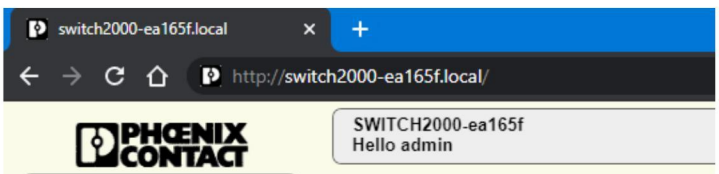
This initial IP configuration is deactivated as soon as the switch is assigned an IP configuration via a different IP address assignment mechanism, e.g., via BootP, DHCP, DCP, web-based management. Depending on the switch version, BootP or DCP is activated for address assignment in the delivery state (see “Configuration in the delivery state” on page 8).

2.1.1.3 Firmware revision 2.90 or later

In the delivery state, the device has an initial IP configuration and an individual DNS host name. You can therefore access the web-based management and configure the device.

In the factory default configuration, the device adopts an IP address from the link-local network (169.254.0.0/16). The IP address 169.254.2.1 is preferably selected, provided it is not already present in the network. You can thus specifically configure individual devices via this IP address. To avoid IP address conflicts when starting multiple devices simultaneously, conflict detection is also active. If the switch detects that the adopted IP address is already assigned, it chooses another at random.

With this dynamic method, it is difficult to find out which switch has which IP address when dealing with multiple devices. You can therefore also access the device via a DNS host name. In the factory default configuration, this name is made up of the device family and the individual part of the MAC address, e.g., SWITCH2000-ea165f or NAT2000-ef245c. Access is then possible using a browser, for example, via http://SWITCH2000-ea165f.local. For name resolution, mDNS (standard for Linux and macOS systems) and LLMNR (usually used for Windows systems) are supported.



This initial IP configuration is deactivated as soon as the switch is assigned an IP configuration via a different IP address assignment mechanism, e.g., via BootP, DHCP, DCP, web-based management. Depending on the switch version, BootP or DCP is activated for address assignment in the delivery state (see “Configuration in the delivery state” on page 8).

If you want to reactivate the initial IP configuration at a later date, this **only** works through a reset (factory default) of the switch using web-based management (see “System – Configuration Handling” on page 31).
A reset using the Smart mode button does not activate the initial IP configuration.

2.1.2 Configuration in the delivery state

In the delivery state or after the system is reset to the factory settings, the following functions and properties are available:

- All IP parameters are deleted. The switch has no valid IP address. An exception is the initial IP configuration in the delivery state (see “Initial IP configuration in the delivery state” on page 7).
- BootP for assigning IP parameters is activated.
- DNS name resolution is activated and the device can be accessed via the individual host name.
- The DHCP server is deactivated.
- There is a user account with the user name “admin” and the password “private”.
- The available RJ45 ports are set to auto negotiation and auto crossing.
- All counters of the SNMP agent are reset.
- The web server (HTTP) and SNMPv2 are activated.
- CLI (Telnet) is activated.
- Port mirroring and MRP are deactivated.
- Rapid Spanning Tree (RSTP) is activated (firmware version 2.01 or later).
- The digital alarm output/signal contact is activated for the “Power Supply Lost” event.
- The MAC address table does not contain any entries.
- LLDP is activated.
- SNTP is deactivated.
- 802.1x and port-based security are deactivated.
- The “Universal” Quality of Service profile is activated.
- Syslog is deactivated.
- Port statistics have been reset.

Delivery state of the NAT versions in relation to the layer 3 functions:

- Routing globally activated.
- LAN1 created (IP addressing: BOOTP, ports: 2 ... 8)
- LAN2 created (IP addressing: DHCP, port: 1)

The delivery state of the PROFINET versions (PN) differs as follows:

– PROFINET mode is activated.
– PROFINET device is activated.
– DCP for assigning the device name and the IP parameters is activated.
– The “PROFINET” Quality of Service profile is activated.

2.2 Using Smart mode

In Smart mode, you can change the operating mode of the switch, without having access to one of the management interfaces.

Press the Mode button to enter Smart mode, select the desired setting, and exit Smart mode. The four Mode LEDs indicate the setting that is currently selected, which will also apply when exiting Smart mode.

The following setting options can be selected via Smart mode:

– Reset the IP configuration
– Operation in EtherNet/IP mode
– Operation in PROFINET mode
– Operation with static IP address
– Operation in Unmanaged mode
– Reset to factory settings

A reset to the factory settings (factory reset), **including the activation of the initial IP configuration**, and the individual host name, is not possible via Smart mode. This is only possible via web-based management.

2.2.1 Entering Smart mode

- Following the boot phase of the switch, as soon as the LEDs of all ports go out, press and hold down the Mode button for more than five seconds. If Smart mode is active, the four LEDs of port XF1 and XF2 will flash. The active state is indicated alternately by the flash sequence of all four LEDs.

  When Smart mode is started, the switch is initially in the “Exit without changes” state.

2.2.2 Selecting the desired setting

- To select the various settings, press the Mode button briefly and select the desired operating mode (see Table “Operating modes in Smart mode” on page 10).

2.2.3 Possible operating modes in Smart mode

The switch supports the selection of the following operating modes in Smart mode:

Table 2-1 Operating modes in Smart mode

Mode	LED 1[1]	LED 2[1]	LED 3[1]	LED 4[1]
Exit Smart mode without changes	**On**	Off	Off	Off
Set Universal mode (factory setting on standard versions)	Off	**On**	Off	Off
Set PROFINET mode (factory setting on PROFINET versions)[2]	**On**	**On**	Off	Off
Set EtherNet/IP mode	Off	Off	**On**	Off
Operation with default IP address	Off	**On**	**On**	Off
Reset IP configuration	**On**	**On**	**On**	Off
Operation in Unmanaged mode	Off	**On**	Off	**On**

1 On the 20xx/21xx/22xx/23xx versions, the two LEDs (LNK/ACT and SPD) of port 1 and 2 respectively are used – the reading direction on the device is from top to bottom (LED 1 = LNK/ACT of port 1, LED 4 = SPD of port 2).
On the 24xx/25xx versions, the four LNK/ACT LEDs of port 1 - 4 are used – the port number corresponds to the LED number.

2 The 20xx/21xx versions do not support PROFINET mode.

2.2.4 Exiting Smart mode

- To exit this mode, press and hold down the Mode button for at least five seconds. The previously selected operating mode is saved and activated as soon as you release the button.

2.2.5 Operation in Universal mode

Activating Universal mode resets the device as described in “Configuration in the delivery state” on page 8. This deletes any configurations stored on the device. An automation protocol is not activated in this mode.

2.2.6 Operation in PROFINET mode

Activating PROFINET mode resets the device as described in “Configuration in the delivery state” on page 8 and activates the PROFINET device and DCP functions for IP address assignment. In addition, the “PROFINET” Quality of Service profile is activated. This deletes any configurations stored on the device. The PROFINET automation protocol is activated in this mode.

2.2.7 Operation in EtherNet/IP mode

Activating EtherNet/IP mode resets the device as described in “Configuration in the delivery state” on page 8 and activates the IGMP snooping and IGMP querier (version 2) functions. In addition, the “EtherNet/IP” Quality of Service profile is activated. This deletes any configurations stored on the device.

2.2.8 Operation with default IP address

For operation with a default IP address, the device is assigned a fixed IP address. A DHCP server is activated on the switch and assigns an IP address to the connected PC via DHCP.

To start up the device with a default IP address, activate the “Operation with static IP address” Smart mode as described in section “Using Smart mode” on page 9.

1. In the network settings on your PC, select the “Obtain an IP address automatically” option.

Deactivate all other network interfaces on your PC.

2. Connect the switch to your PC.
3. Select the “Operation with default IP address” smart mode as described in section “Using Smart mode” on page 9.
4. The switch assigns an IP address to the PC via DHCP
5. The switch can now be accessed via IP address “192.168.0.254”.

Set the desired IP address via web-based management.

2.2.9 Reset IP configuration

When the “Reset IP configuration” Smart mode is activated, the IP address, subnet mask, and default gateway are reset to 0.0.0.0 and BootP is activated. Any other configurations stored on the device are retained and are not deleted.

2.2.10 Operation in Unmanaged mode

When operating in Unmanaged mode, the switch can be used without an IP address. Here, the switch adopts the static IP address 0.0.0.0. The subnet mask and gateway are also configured to 0.0.0.0. This means that web-based management can no longer be accessed and the switch no longer sends BootP and DHCP requests.

The main functions remain active in Unmanaged mode:

- Redundancy mechanisms for loop suppression (RSTP, FRD, LTS)
- Functions for hardening the network (broadcast/multicast limiter)
- Functions for reducing the network load (IGMP snooping)

Use of IGMP in Unmanaged mode is limited to IGMP snooping. The switch requires an IP address if the device is also to be used as an IGMP querier.

The functions must be configured in Managed mode and will remain active when switching to Unmanaged mode. Alternatively, Unmanaged mode can be activated using a configuration file and SD card.

Unmanaged mode can only be exited by switching to a different Smart mode or by resetting the switch to the factory settings.

2.3 Assigning IP parameters via BootP

On the standard versions, BootP is activated in the delivery state. On the PROFINET versions, DCP is activated in the delivery state.

The device uses the BootP protocol for IP address assignment. Numerous BootP servers are available on the Internet. You can use any of these programs for address assignment.

This section explains IP address assignment using the “FL NETWORK MANAGER BASIC” (Order No. 2702889) and the “IP Assignment Tool” software tools from Phoenix Contact.

Notes on BootP

During initial startup, the device sends BootP requests without interruption until it receives a valid IP address. As soon as the device receives a valid IP address, it stops sending further BootP requests.

After a restart, the device sends three BootP requests and will only then adopt the old IP address if there is no BootP response.

2.3.1 Assigning the IP address using FL NETWORK MANAGER BASIC

Requirements

The device is connected to a PC with a Microsoft Windows operating system and the FL NETWORK MANAGER has been successfully installed.

Step 1: Parameterizing the BootP server

- Open the FL NETWORK MANAGER software
- Open a new project in the software
- Under Extras → Options, select the BOOTP/DHCP SERVER menu item
- Configure the network interface on your PC to which the device is connected and select “BootP” operating mode. You can also adjust the subnet mask and configure a default gateway.
- Click “OK” to confirm the parameterization

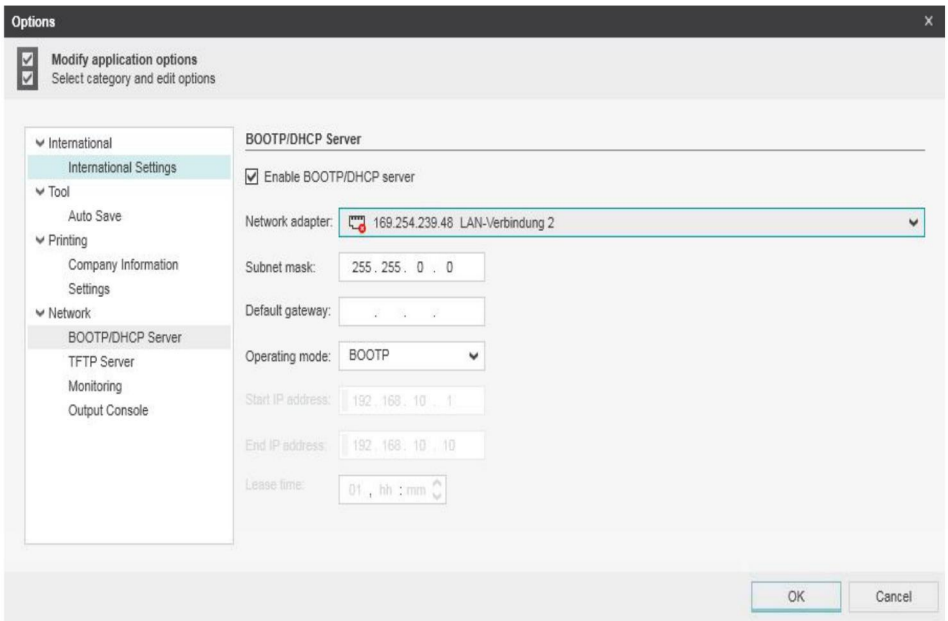


Figure 2-1 Settings for the BootP server

Step 2: Starting the BootP server

- In your project in the BOOTP/DHCP SERVER window, click on the “play” icon next to the selected network interface. The BootP server is now activated.
- BootP requests that are received are listed in the BOOTP/DHCP SERVER window in table format

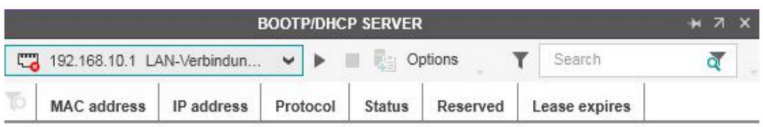


Figure 2-2 BootP server

Step 3: Inserting incoming BootP requests in the reservation list and assigning IP parameters

- If you would now like to assign IP parameters to a device, such as IP address, subnet mask or default gateway, right-click on an incoming BootP request in the BOOTP/DHCP SERVER window and select “Add to BOOTP/DHCP reservations”.
- Enter the IP address to be assigned in the BOOTP/DHCP reservations window. The IP parameters are immediately transferred to the device.
- You can check whether IP address assignment was successful in the “IP address” column in the BOOTP/DHCP SERVER window.

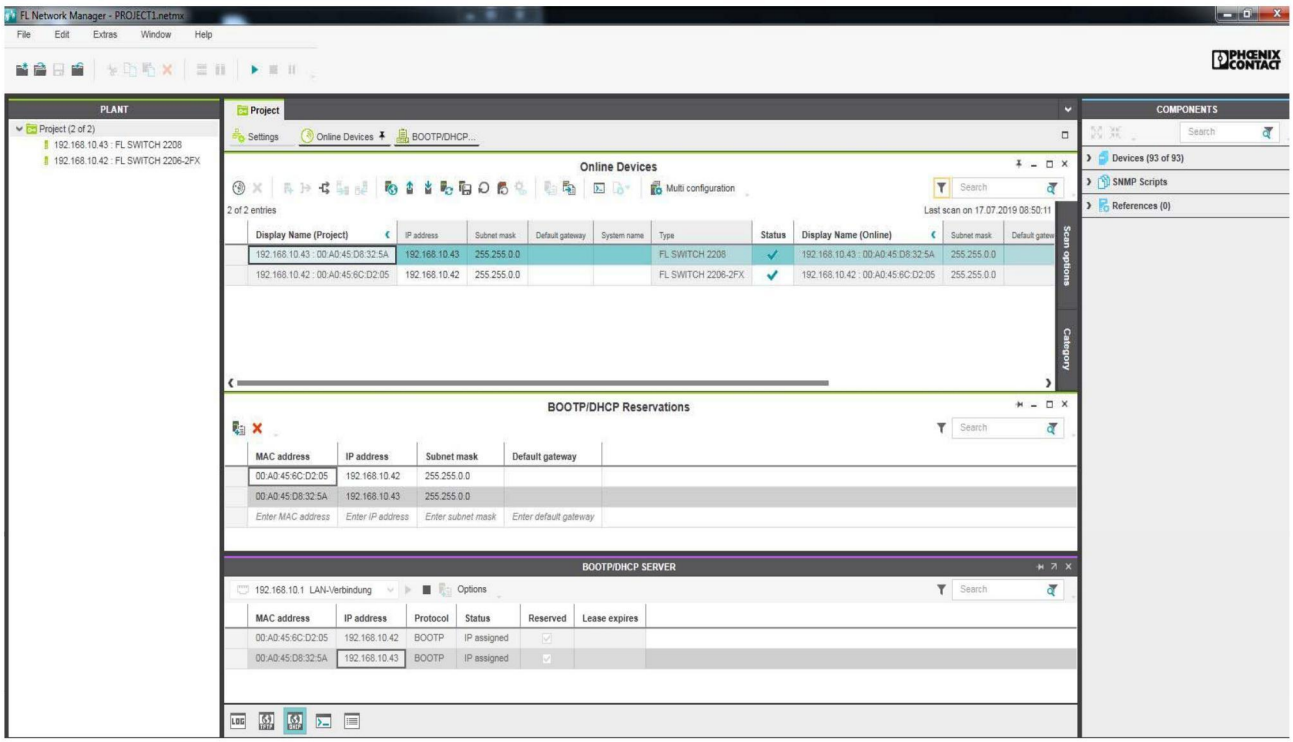


Figure 2-3 FL Network Manager with BootP/DHCP reservation list shown

The IP parameters set here can be changed in web-based management, if required (see section “Network” on page 37).

2.3.2 Assigning the IP address using IPAssign.exe

Requirements

The device is connected to a computer with a Microsoft Windows operating system.

Step 1: Downloading and running the program

- On the Internet, select the link phoenixcontact.net/products.
- Follow further instructions to access the search field.
- Enter order number 2702323 in the search field, for example.

The BootP IP addressing tool can be found among the various downloads for the product.

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

Step 2: “IP Assignment Wizard”

The program opens and the start screen of the addressing tool appears. The program is mainly 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 subsequent steps.

- Click on the “Next” button.

Step 3: “IP Address Request Listener”

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

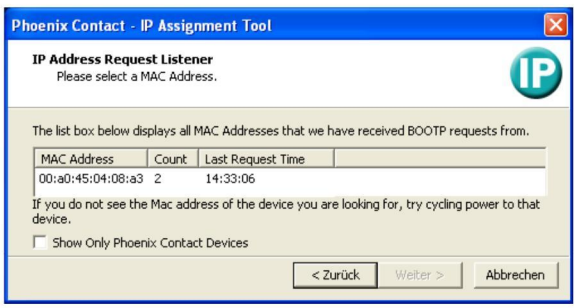


Figure 2-4 “IP Address Request Listener” window

The MAC address of your switch can be found on the sticker on the side.

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

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

Step 4: “Set IP Address”

The following information is displayed in the window that 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

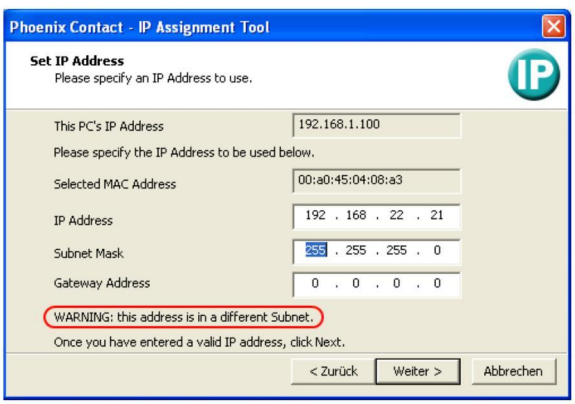


Figure 2-5 “Set IP Address” window with incorrect settings

- 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 the “Next” button.

Step 5: “Assign IP Address”

The program attempts to transfer the set IP parameters to the device.

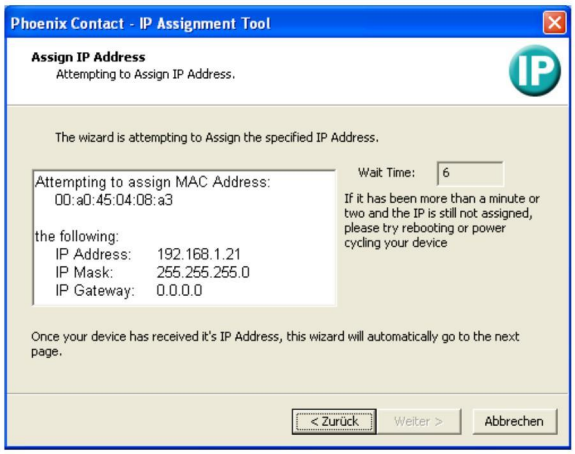


Figure 2-6 “Assign IP Address” window

Following successful transfer, the next window opens.

Step 6: Completing IP address assignment

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

To assign IP parameters for additional devices:

- Click on the “Back” button.

To exit IP address assignment:

- Click on the “Finish” button.

The IP parameters set here can be changed in web-based management, if required (see Section “Network” on page 37).

3 Frame switching

The switch operates in store-and-forward mode. When receiving a data packet, the switch analyzes the source and destination addresses. The switch stores up to 8192 MAC addresses in its address table with an adjustable aging time of 10 to 825 seconds.

3.1 Store and forward

All data telegrams received by the switch are stored and their validity is checked. Invalid or faulty data packets (for example: CRC errors) and fragments (<64 bytes) are discarded. Valid data telegrams are forwarded by the switch.

3.2 Multi-address function

The switch learns all the source addresses for each port. Only packets with the following addresses in the destination address field are forwarded via the relevant port:

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

The switch can learn up to 8192 addresses. This is necessary if more than one end device is connected to one or more ports. Several independent subnets can be connected to one switch.

3.2.1 Learning addresses

The switch independently learns the addresses of the end devices that are connected via this port. The switch does this by evaluating the source addresses in the data telegrams. When the switch receives a data telegram, it forwards this data telegram only to the port that connects to the specified device (if the address could be learned beforehand).
The switch monitors the age of the learned addresses. The switch automatically deletes address entries that exceed a specific age (default: 40 seconds, adjustable from 10 to 825 seconds, aging time) from its address table.

All learned address entries are deleted upon restart.
A link down deletes all the entries of the respective port.

A list of detected MAC addresses can be found in the MAC address table. The MAC address table can be deleted via the “Clear” button.

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

3.2.2 Prioritization

The switch supports eight priority queues (traffic classes in accordance with IEEE 802.1Q) for the purpose of influencing the internal packet processing sequence. Data telegrams that are received are assigned to these classes according to the priority of the data packet, which is specified in the VLAN/prioritization tag, where value “0” in the tag indicates the lowest priority and value “7” indicates the highest priority.

Furthermore, the switch also supports the detection and high prioritization of automation protocols (PROFINET and EtherNet/IP™) in certain profiles.

Processing rules

The switch controller in the device forwards received packets to the available receive queues according to the following decisions:

– BPDU packets are always assigned to the high-priority queue.
– Provided the corresponding Quality of Service profile is activated, PROFINET and EtherNet/IP packets will also be assigned to a high queue.
– Packets with VLAN/prioritization tag are forwarded according to the queues specified above.
– All remaining data is assigned to the low-priority queue.

3.2.2.1 Class of Service – CoS

Class of Service refers to a mechanism used to take into consideration the value of the priority field (values 1 to 7) in VLAN data packets with a tag. The switch assigns the data streams to various processing queues, depending on the priority information contained in the CoS tag. The switch supports eight internal processing queues.

3.2.2.2 Quality of Service – QoS

Quality of Service affects the forwarding and handling of data streams and results in individual data streams being treated differently (usually preferential). One possible use of QoS is to guarantee a transmission bandwidth for individual data streams. The switch uses QoS in connection with prioritization.

4 Configuration and diagnostics in web-based management

You can use the convenient web-based management (WBM) interface to manage the switch from anywhere in the network using a standard browser (e.g., Microsoft Edge). The configuration and diagnostic functions are clearly displayed in a graphical user interface. Every user with a network connection to the device has read/write access to that device via a browser. A wide range of information about the device itself, the set parameters, and the operating state can be viewed.

Modifications to the device can only be made by entering the valid password. In the delivery state, there is a user account with the user name “admin” and the password “private”.

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

4.1 Requirements for the use of WBM

Requirements for WBM

As the web server operates using the Hyper Text Transfer Protocol, a standard browser can be used. Access is via URL “http://IP address of the device”. Example: “http://172.16.29.112”. If the web server is set to the secure HTTPS protocol in WBM, access is via URL “http**s**://IP address of the device”. To enjoy the full features of the web pages, the browser must support JavaScript 1.2 and Cascading Style Sheets Level 1. We recommend using Microsoft Edge (version 80.0 or later).

WBM can only be accessed using a valid IP address.

Device login is only possible if cookies are enabled in the browser settings.

Some functions are opened in pop-up windows. It is therefore only possible to use all of the functions if pop-ups are permitted in the browser settings.

You need to log into the device in order to make changes. To do so, click on the “Login” button.

In the delivery state, there is a user account with the user name “admin” and the password “private”.

Figure 4-1 Login window

Depending on the configuration of the switch, a user may be locked out for a period of time after a certain number of failed login attempts. During this time, it is not possible to access WBM, even if the correct user data is entered (see “User Management” on page 27).

4.2 Functions/information in WBM

Areas of WBM

WBM is split into the following areas:

– Information: General device information
– Configuration: Device configuration
– Diagnostics: Device-specific diagnostics

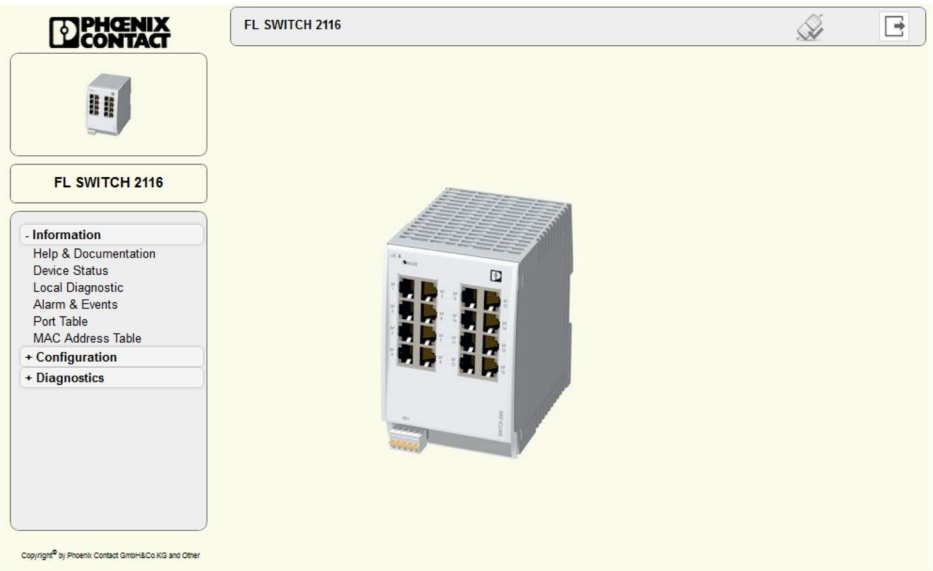


Figure 4-2 Start page for web-based management (example)

4.2.1 Description of the header

The header is always shown and displays basic status information, e.g., about the connection to the device, the configuration, the device name, and the user that is currently logged in.

WBM header

Figure 4-3 Web-based management header

The following status icons and buttons may appear in the header:

There is an active connection to the device.

The connection to the device has been disconnected.

The “admin” user has not yet changed the initial password “private” set in the factory default configuration.
For security reasons this password must be changed immediately after logging in for the first time. Click the button to go directly to the System web page where you can change the password.

A configuration change has not been saved retentively yet (e.g., by clicking an “Apply” button).
Click the button to save the configuration retentively. The configuration changes are retained even in the event of a device restart.

You are not logged into the device.
Click the button to go directly to the Login web page.

You are logged into the device.
Click the button to log out.

4.2.2 WBM information area

4.2.2.1 Help & Documentation

Here you will find useful information about using web-based management.

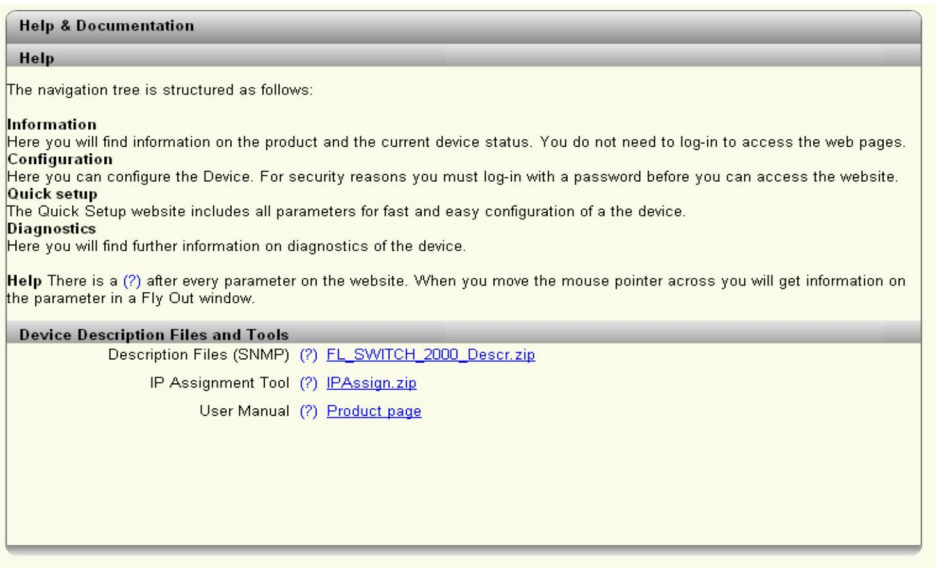


Figure 4-4 “Help & Documentation” web page

On this page, you can also download the following files and software, which are supplied with the device, directly from the device:

– Description files (SNMP, GSDML, FDCML)
– IP Assignment Tool

4.2.2.2 Device Status

Here you will find general information about your device, such as the serial number, firmware version or hardware version.

Device Status		
Device Identification		
Vendor	:	Phoenix Contact GmbH & Co. KG
Address	:	D-32823 Blomberg
Phone	:	+49 -(0)5235 -3-00
Internet	:	www.PhoenixContact.com
Type	:	FL SWITCH 2306-2SFP
Order No	:	2702970
Serial No	:	2033813153
Firmware Version	:	2.85.03 BETA
Hardware Version	:	01
Logic Version	:	0x5
Bootloader Version	:	1.14
Hostname	:	SWITCH2000-ea165f
Device Name	:	SWITCH2000-ea165f
Description	:	
Physical Location	:	
Contact	:	
IP Address	:	169.254.2.1
Subnet Mask	:	255.255.0.0
Gateway	:	0.0.0.0
IP Address Assignment	:	BootP
MAC Address	:	00:A0:45:EA:16:5F
System Status		
Uptime	:	27m:36s

Figure 4-5 “Device Status” web page

4.2.2.3 Local Diagnostics

Here you will find a brief explanation of how to interpret the individual LEDs on the device.

Local Diagnostics		
Power Supply		
US1	:	Supply Voltage 1 (green LED)
US2	:	Supply Voltage 2 (green LED)
Alarm Output		
FAIL	:	Alarm Output failed (red LED)
Ethernet		
PORT LED 1	:	Link and Activity (green LED)
PORT LED 2	:	Speed 10 Mbit/s (LED off)
	:	Speed 100 Mbit/s (green LED)
	:	Speed 1000 Mbit/s (orange LED)

Figure 4-6 “Local Diagnostics” web page

4.2.2.4 Alarm & Events

On this page, you will find a list of alarms and events in a table. You can save event table entries, so that they are also retained after the device is restarted. The Event Table can be downloaded from the device in CSV format.

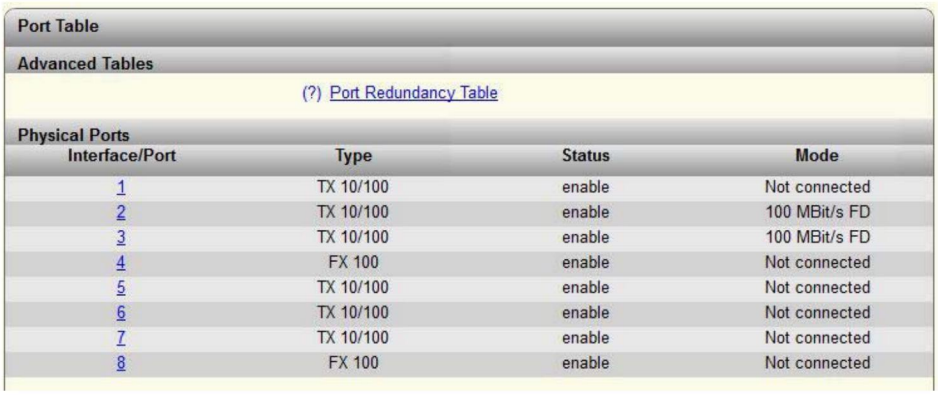
A maximum of 3000 entries can be stored in the Event Table. The oldest entries are then overwritten. If there is a large number of entries, it may take several seconds to load the Event Table.

The persistent storage of events is deactivated in the factory default configuration. The events are lost when the device is restarted. The function can be activated via the “Persistent Event Logging” item on the “Service” web page (see “Service” on page 39).

Figure 4-7 “Alarm & Events” web page

4.2.2.5 Port Table

On this page, you will find a list of the current states of the individual ports.



Port Table

Advanced Tables

(?) Port Redundancy Table

Physical Ports

Interface/Port	Type	Status	Mode
1	TX 10/100	enable	Not connected
2	TX 10/100	enable	100 MBit/s FD
3	TX 10/100	enable	100 MBit/s FD
4	FX 100	enable	Not connected
5	TX 10/100	enable	Not connected
6	TX 10/100	enable	Not connected
7	TX 10/100	enable	Not connected
8	FX 100	enable	Not connected

Figure 4-8 “Port Table” web page

Clicking on the “Port Redundancy Table” button opens a table containing information about the individual ports and their redundancy mechanism assignment.

Interface/Port: Clicking on a port number in the “Interface/Port” column opens the “Port Configuration” web page for the selected port.

Type: The “Type” column indicates whether it is a copper port (e.g., TX 10/100) or a fiberglass port (e.g., FX 100).

Status: The “Status” column shows whether the port is activated or deactivated.

Mode: The “Mode” column indicates the current connection status of the ports.

- Not connected: No active link at the port.
- 100 Mbps FD (or comparable status): Displays the transmission speed and duplex mode if there is an active link.
- Far-End Fault: Provides information about a fault on a fiber of a bi-directional fiberglass connection (e.g., due to a defective fiberglass cable). If the device at the other end also supports Far-End Fault, it detects a communication failure on its own receiver connection and sends a Far-End Fault signal pattern to the peer.

4.2.2.6 MAC Address Table

On this page, you will find a list of the current devices in the network. You can download the list from the device in CSV format.

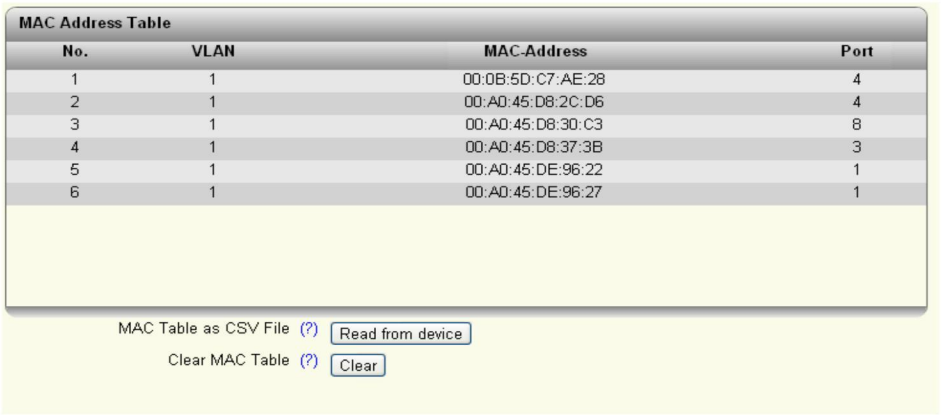


Figure 4-9 “MAC Address Table” web page

4.2.2.7 PROFINET Status

The “PROFINET Status” page is only displayed when PROFINET mode is active.

Here you will find an overview of the PROFINET status of the device.

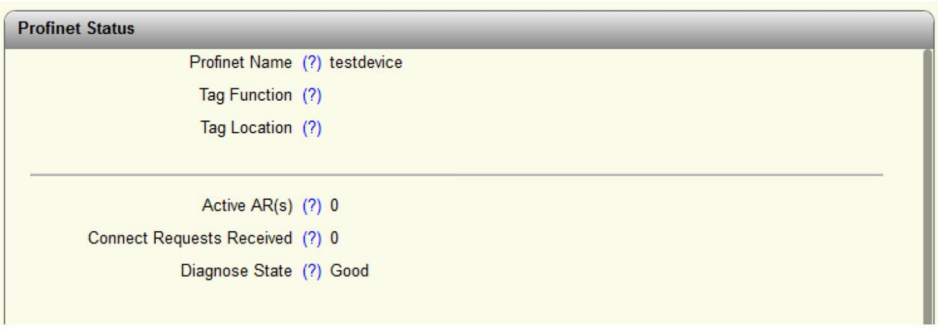


Figure 4-10 “PROFINET Status” web page

PROFINET Name:	Shows the device name assigned via DCP
Tag Function:	Shows the text for the device function set via I&M1
Tag Location:	Shows the text for the device location set via I&M1
Active AR(s):	Shows the number of active PROFINET I/O connections
Connect Requests Received:	Shows the number of connection requests received
Diagnose State:	Shows the current device status

4.2.3 WBM configuration area

4.2.3.1 User Management

Here, you can create and manage user accounts for the web-based management of your switch. You can assign permissions to users via user roles.

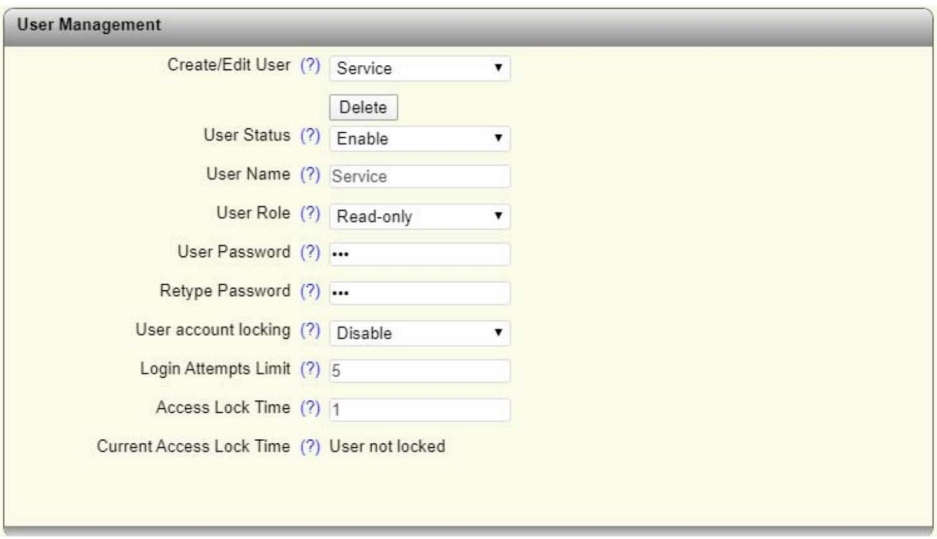


Figure 4-11 “User Management” web page

Create/Edit User:	Here, select the user account that you wish to edit or delete. Select “Create” to create a new user account.
Delete button:	Click here to delete the selected user account. The “admin” account cannot be deleted.
User Status:	Activate or deactivate the selected user account. When a user account is deactivated, access to the device is blocked, even if the correct login parameters are entered.
User Name:	Configure the user name. Once the user account is created, you will not be able to change the user name.
User Role:	Assign a role to the selected account that defines the user rights. The following roles can be selected: – Read-only: The user has read access to the device and therefore access to the web pages in the information and diagnostics areas. Furthermore, the user has permission to change their own access password. – Expert: An expert user account has extensive read and write access to the device and can therefore modify a good portion of the configuration parameters. However, this excludes “User Management”. – Admin: An admin user has unrestricted read and write access to the device.
User Password / Retype Password:	Here, you can configure the password for the selected user account. For a new user account, this password is also used for initial access to the device.

A user can only be created if a valid password is entered. The password must be between eight and 64 characters long.

User account locking:	This function can be used to lock out a user for a certain period of time if they have repeatedly attempted to log in using the wrong password. It is not possible to access the device during this time, even if the correct access data is entered.
Login Attempts Limit:	When the “User account locking” function is activated: Here, configure the number of failed login attempts after which the user account is locked.
Access Lock Time:	When the “User account locking” function is activated: Here, set the time (in minutes) for which a user account is locked if the “Login Attempts Limit” is exceeded.
Current Access Lock Time:	Admin users can use this status to determine whether and for how long the selected user account has now been locked.
Unlock button:	Admin users can click on the “Unlock” button to unlock a locked account before the full “Access Lock Time” has elapsed.

4.2.3.2 System

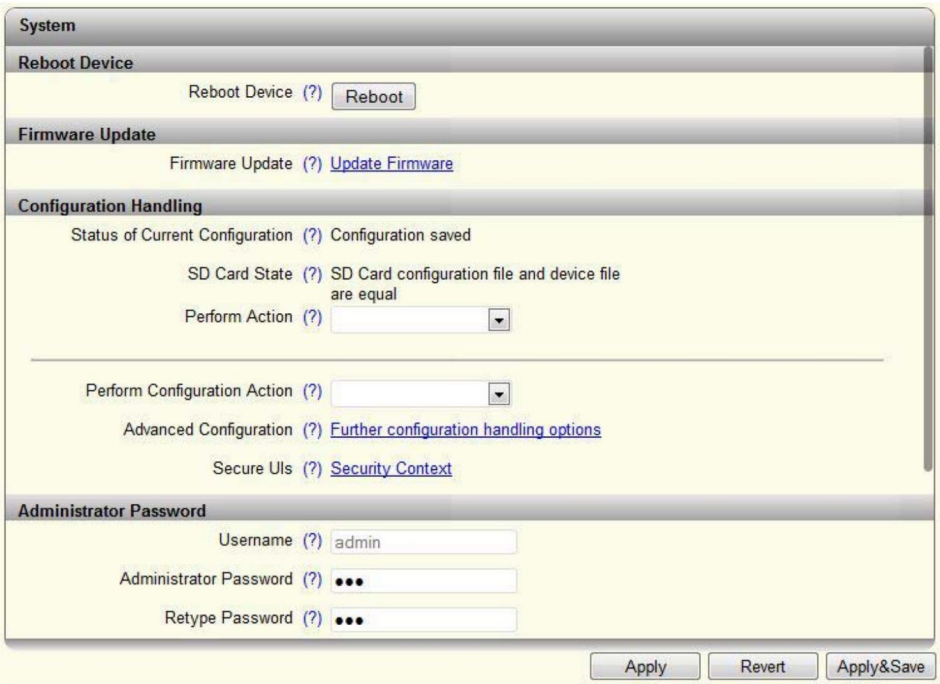


Figure 4-12 “System” web page

System – Reboot Device

Reboot Device

Clicking on the “Reboot” button restarts the device. All unsaved parameters will be lost.

The connection to the device is interrupted for the boot phase.

System – Firmware Update

Firmware Update

Clicking on the “Update Firmware” link opens a pop-up in which the parameters for the firmware update must be entered.

Pop-up: Update Firmware

Update via HTTP: Select “HTTP” as the method.

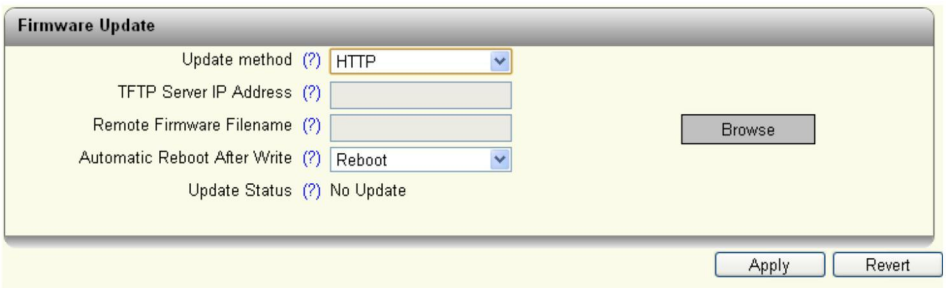


Figure 4-13 “Firmware update via HTTP” pop-up

Browse:	Clicking on the “Browse” button allows you to select the desired file on your PC.
Automatic Reboot After Write:	Here, specify whether a reboot should be performed after the firmware update.

If you perform a firmware update without rebooting immediately, “Update Status” displays the message “Firmware Update successful”, which informs you that the firmware has been transferred to the device and will be activated on the next reboot.

The firmware update starts as soon as you click on “Apply”.

Update via TFTP: Select “TFTP” as the method.

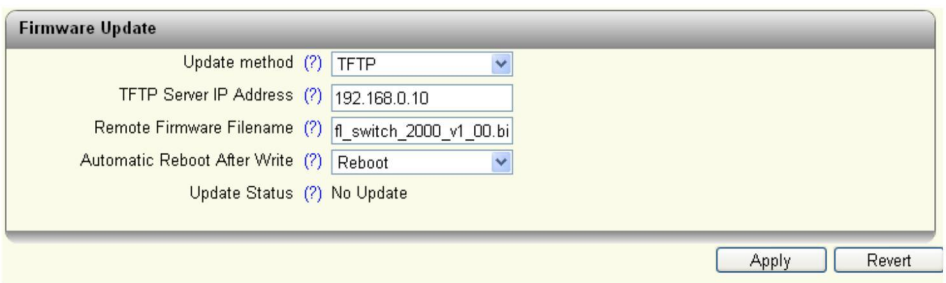


Figure 4-14 “Firmware update via TFTP” pop-up

TFTP server IP address:	Here, you can set the IP address of the computer on which the TFTP server is active.
Remote Firmware Filename:	Here, you can set the name of the firmware file that is to be transferred to the device.
Automatic Reboot After Write:	Here, specify whether a reboot should be performed after the firmware update.

The firmware update starts as soon as you click on “Apply”.

System – Configuration Handling

Configuration Handling

Status of Current Configuration:	Shows the status of the active configuration.
SD Card State:	Indicates whether or not an SD card is inserted.
Perform Action:	The selected action is performed by clicking in the drop-down list: – Compare: Compares the configuration file on the SD card with the one on the device. – Clear: Deletes the configuration file on the SD card.
Perform Configuration Action:	The selected action is performed by clicking in the drop-down list: – Factory Default: Resets the device configuration to the delivery state. – Save Configuration: Saves the active device configuration to the SD card. – Reload Configuration: Loads the configuration file from the SD card and applies it. The device is then restarted.
Advanced Configuration:	Clicking on the “Further configuration handling options” link opens a “File Transfer” window (see page 32). There you need to enter the parameters for transferring a configuration file from the device to the PC (download) or from the PC to the device (upload).
Secure UIs:	Clicking on the “Security Context” link opens the “Security Context” pop-up (see page 34).

Pop-up: Advanced Configuration

Transfer Method:	Select the transmission protocol you would like to use to transfer the file.
File Type:	Select the file type you would like to transfer. – You can either transfer a configuration file, a security context or a snapshot file.
Configuration Name:	Enter the name under which you want to save the configuration on the PC. Any change to the configuration name only takes effect when you click on the “Apply&Save” button.

File Transfer via HTTP

Select “HTTP” as the transfer method.

Transfer of configuration file or security context

Figure 4-15 “Advanced Configuration” – transferring the configuration file via HTTP

Update Status:	Shows the current transfer status.
Start Transfer:	Click on the “Write to device” button to select the file on your PC that is to be transferred to the switch.
HTTP Read:	Click on the “config.cfg” link to download the active configuration directly to your PC.

Transfer of snapshot files

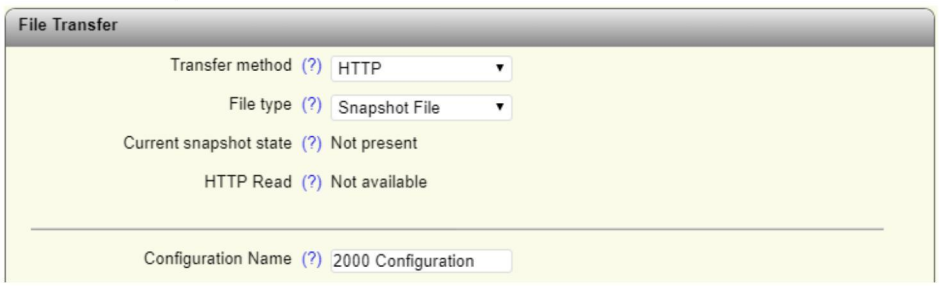


Figure 4-16 “Advanced Configuration” – transferring the snapshot file via HTTP

HTTP Read:	Click on the “snapshot.tar.gz” link to download the current snapshot file directly to your PC.

File Transfer via TFTP

Select “TFTP” as the transfer method.

Transfer of configuration file or security context

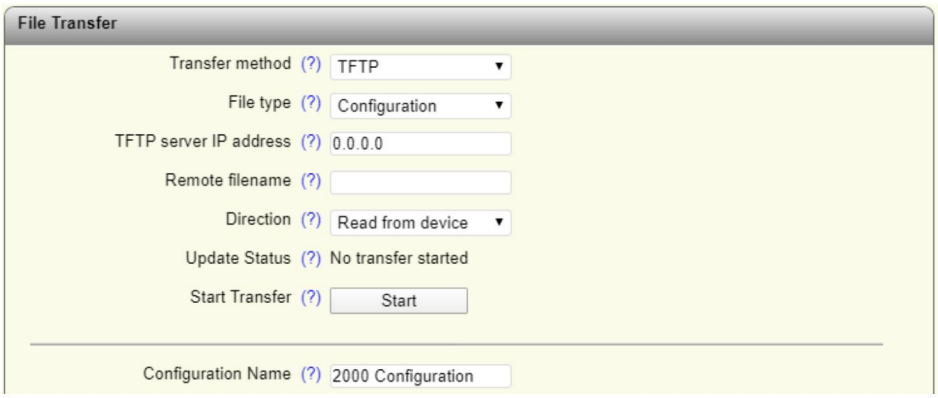


Figure 4-17 “Advanced Configuration” – transferring the configuration file via TFTP

TFTP server IP address:	Enter the IP address via which the TFTP server can be reached.
Remote filename:	Enter the name of the file that you would like to transfer.
Direction:	Select whether the file should be uploaded to or downloaded from the device.
Update Status:	Shows the current transfer status.
Start Transfer:	Click on the “Start” button to start the transfer of the file.

Transfer of snapshot files

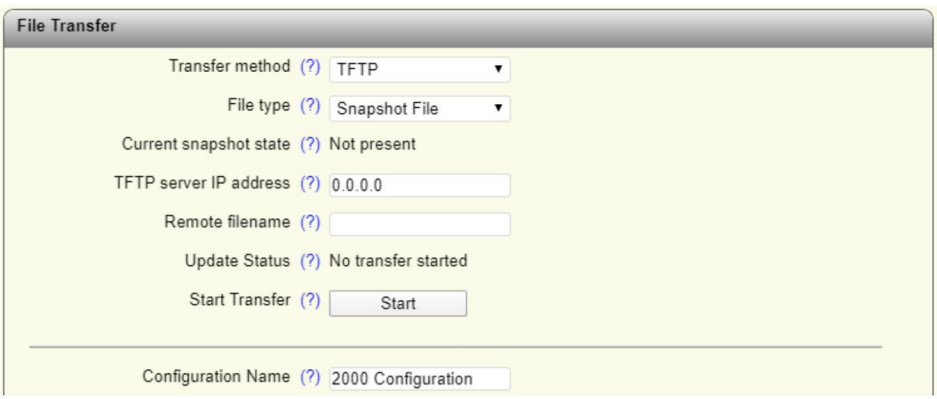


Figure 4-18 “Advanced Configuration” – transferring the snapshot file via TFTP

TFTP server IP address:	Enter the IP address via which the TFTP server can be reached.
Remote filename:	Enter the name of the file that you would like to transfer.
Update Status:	Shows the current transfer status.
Start Transfer:	Click on the “Start” button to start the transfer of the file.

Pop-up: Security Context

Figure 4-19 “Security Context” pop-up

Create new context:	Clicking on the “Generate” button creates all the necessary keys and certificates for operation with HTTPS and SSH.
Current state:	Shows the status of the current availability of the security context.
Root CA:	Clicking on the “cacert.cer” link loads the Root CA certificate for installation in the browser.
Advanced Configuration:	Clicking on the “File transfer” link opens the “Advanced Configuration” pop-up (see Section “Pop-up: Advanced Configuration” on page 32).

System – Administrator Password

Administrator Password

Here, you can change the administrator password.

Figure 4-20 “Administrator Password” configuration area

Administrator Password / Retype Password:	The new password must be between eight and 64 characters long. The new password will be enabled after logging out. In the delivery state, the password is “private” (please note that it is case-sensitive). For security reasons, the input fields do not display your password; “*******” is displayed instead.
Individual SNMPv3 Password:	Clicking the button opens two further input fields where you can configure a separate SNMPv3 password. The minimum password length is eight characters.

For further information on using SNMPv3 with a separate password, refer to section “SNMP – Simple Network Management Protocol”.

System – Device Identification

Device Identification

In this area, you can configure device information, which is then displayed on the “Device Status” page.

Figure 4-21 “Administrator Password” configuration area

Device Name:	Here, you can configure the device name. In the factory default configuration, the device name corresponds to the device host name.
Device Description:	In this text field, you can enter a device description.
Physical Location:	Here, you can provide the location of the device, such as the building in which it is installed.
Device Contact:	Here, you can enter a contact address.

4.2.3.3 Quick Setup

You can configure the basic settings in the Quick Setup area.

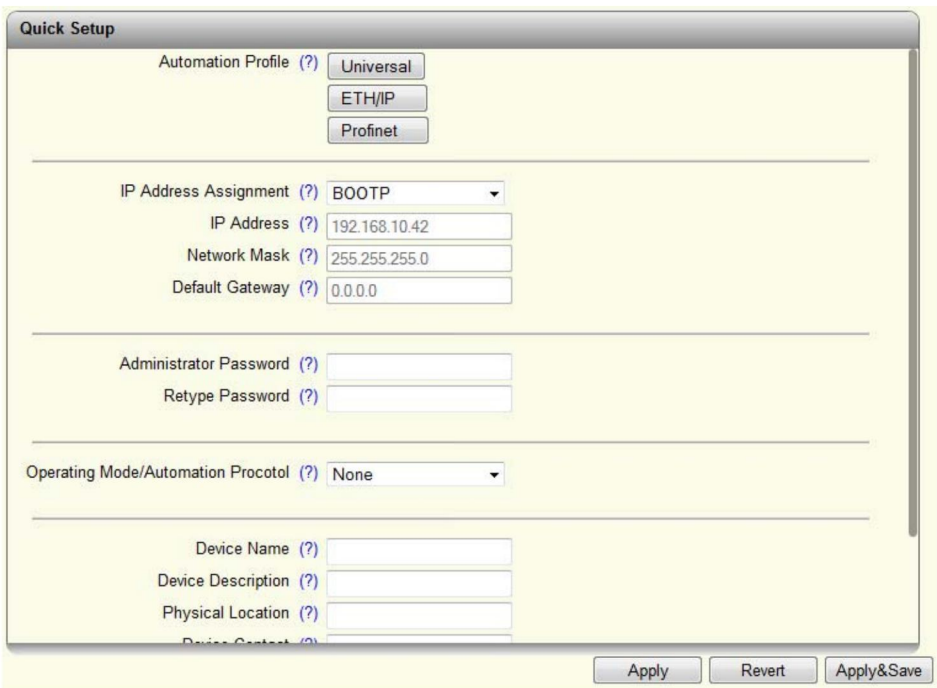


Figure 4-22 “Quick Setup” web page

Automation Profile:	Select a profile that is optimized for the desired operating mode. – Universal: In Universal mode, the automation protocols (PN device) are deactivated and BootP is activated for IP address assignment. – ETH/IP: In EtherNet/IP mode, IGMP snooping, IGMP querier (version 2), the “EtherNet/IP” Quality of Service profile, and address conflict detection (ACD) are activated. – PROFINET: In PROFINET mode, LLDP is activated. On the 22xx/23xx/24xx/25xx versions, the PROFINET device, DCP for IP address assignment, and the “PROFINET” Quality of Service profile are also activated.

Activating an automation profile from web-based management only changes the functions relevant to this mode.

In contrast to the setting via the Smart mode button (see “Using Smart mode” on page 9), any other configurations stored on the device are retained and are not deleted.

IP Address Assignment:	Select the type of IP address assignment. – STATIC: Static IP address – BOOTP: Assignment via the Bootstrap protocol – DHCP: Assignment via a DHCP server – DCP: Assignment via the PROFINET engineering tool or controller (22xx/23xx/24xx/25xx versions only)
IP Address:	Set the desired IP address.
Network Mask:	Set the desired subnet mask here.
Default Gateway	Set the desired default gateway here.
Administrator Password:	Here, you can change the administrator password.
Operating Mode/Automation Protocol:	Here, you can set the operating mode of the device.
Device Name	Here, you can enter the device name of the switch.
Device Description:	Here, you can enter a description for the device.
Physical Location:	Here, you can enter a location for the device.
Device Contact:	Here, you can enter the name of a contact person for the device.
LLDP Mode:	Here, you can enable or disable LLDP. – Disable: LLDP is deactivated – Enable: LLDP is activated – Send only: Received LLDP BPDUs are ignored – Receive only: No LLDP BPDUs are sent

The “LLDP Topology” link opens the corresponding page. This can also be accessed via the menu item of the same name (see “LLDP – Link Layer Discovery Protocol” on page 79).

The port-based LLDP configuration can be found on the “Service” page (see “Service” on page 39).

4.2.3.4 Network

The basic network settings are made here.

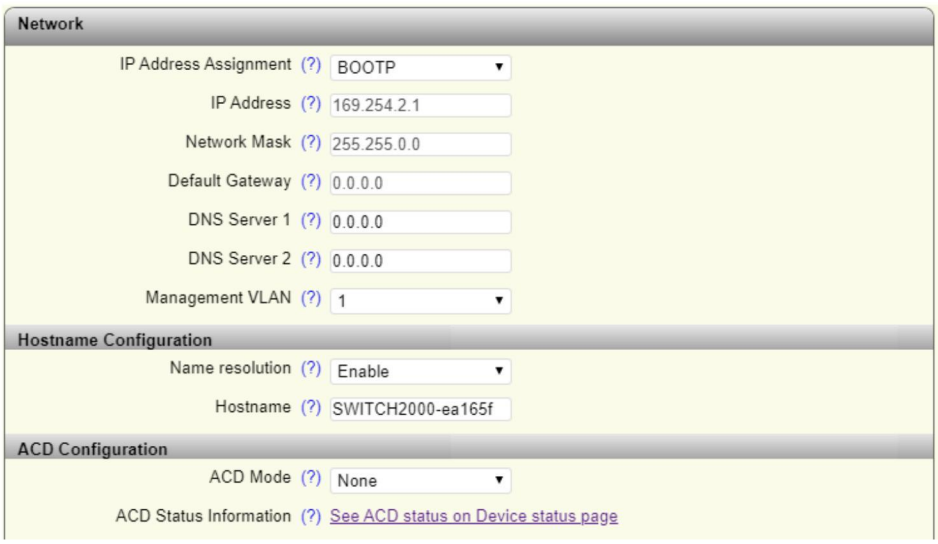


Figure 4-23 “Network” web page

IP Address Assignment: Select the type of IP address assignment.
- STATIC: Static IP address
- BOOTP: Assignment via the Bootstrap protocol
- DHCP: Assignment via a DHCP server
- DCP: Assignment via the PROFINET engineering tool or controller (22xx/23xx/24xx/25xx versions only)

- If you have chosen “STATIC”, now make the following settings:
  - IP Address: Set the desired IP address.
  - Network Mask: Set the desired subnet mask.
  - Default Gateway: Set the desired default gateway.

DNS Server 1: Here, you can enter the IP address of the primary DNS server.

DNS Server 2: Here, you can enter the IP address of the secondary DNS server.

Management VLAN: Here, set the VLAN in which the web-based management can be accessed (default: “1”).

Hostname Configuration

Name resolution: Here, you can enable and disable DNS name resolution via mDNS and LLMNR. When the function is activated, you can also access the device via the host name (e.g., http://switch2000-ea165f.local/).

Hostname: Configure the DNS host name of the device here.

- The host name must be between two and 63 characters long. Alphanumeric characters and dashes are permitted. A host name must not start with a dash.
- In the factory default configuration, this host name is made up of the product family name and part of the device MAC address (e.g., SWITCH2000-ea165f).

After deactivating DNS name resolution, it may take some time until the device can be accessed via the host name due to the DNS cache.

ACD Configuration

ACD Mode: Here, you can enable and disable the “Address Conflict Detection” function.

ACD Status Information: Clicking on the link opens the “Device Status” page.

Figure 4-24 ACD status information on the “Device Status” page

4.2.3.5 Service

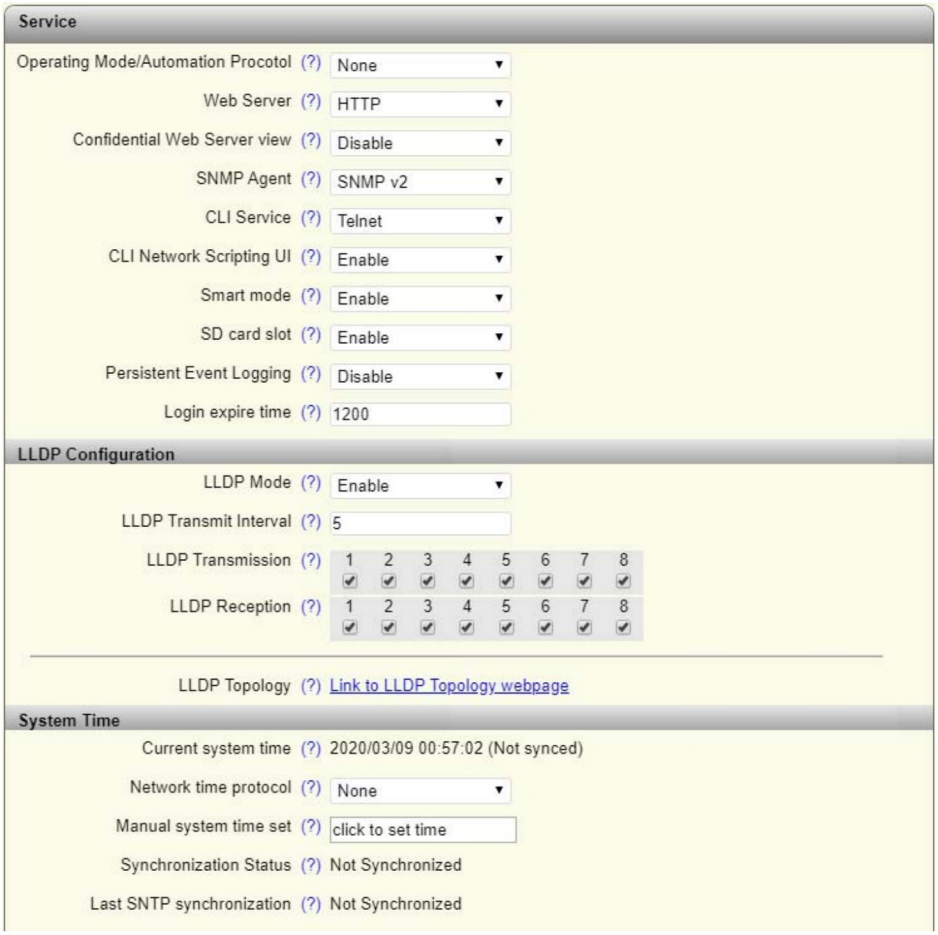


Figure 4-25 “Service” web page

Operating Mode/Automation Protocol: Here, you can set the operating mode of the device.

Web Server: Here, you can enable and disable the web server function and also select the mode (HTTP/HTTPS).

If you deactivate the web server, web-based management can no longer be accessed.

Confidential Web Server View: If this view is activated, no web pages in web-based management can be accessed without logging in first – this also applies to the web pages in the information area.

SNMP Agent: Here, you can enable and disable the SNMP server function and also select the mode (SNMP v2, SNMP v3).

CLI Service:	–	Disable:	The entry of CLI commands is deactivated.
	–	Telnet:	The entry of CLI commands via Telnet is activated.
	–	SSH:	The entry of CLI commands via Secure Shell (SSH) is activated.
CLI Network Scripting UI:	–	Disable:	The transmission of CLI commands via the network is deactivated.
	–	Enable:	The transmission of CLI commands via the network is activated.

For further information on using the CLI, refer to the “UM EN FL CLI” user manual available at phoenixcontact.net/products.

Smart mode: Here, you can enable and disable the Smart mode button.

SD card slot: Here, you can enable and disable the SD card slot.

NOTE: If the Smart mode button and SD card slot are deactivated and access is no longer possible via the Ethernet ports (e.g., due to incorrect configuration or forgotten access data), it is no longer possible to reset the device. The device must then be sent in to be reset by the manufacturer – this is subject to a fee.

When the SD card slot is disabled, it is also no longer possible to access MRP manager licenses (MRM).

Persistent Event Logging: Here, you can enable and disable the persistent storage of events. Persistent storage means that events are not deleted when the device is restarted.

Login expire time: Here, you can configure the duration until automatic logout (30 ... 3600 seconds, default: 1200 seconds).

Entering 0 deactivates automatic logout.

Service – LLDP Configuration

LLDP Configuration

LLDP Mode:	– Disable: LLDP is disabled – Enable: LLDP is enabled – Send only: Only LLDP BPDUs are sent. – Receive only: Only LLDP BPDUs are received.
LLDP Transmit Interval:	Here, set the interval at which LLDP telegrams are to be sent. The value must be between 5 and 32,786 seconds (default: 5 s).
LLDP Transmission:	Here, you can enable and disable the forwarding of LLDP telegrams for specific ports.
LLDP Reception:	Here, you can enable and disable the ignoring of LLDP telegrams for specific ports.
LLDP Topology:	Clicking on the “Link to LLDP Topology webpage” link opens the web page for “LLDP diagnostics in web-based management” on page 81.

For further information on “LLDP”, refer to section “LLDP – Link Layer Discovery Protocol” on page 79.

Service – System Time

System Time

Current system time:	Displays the current system time. “Not synced” means that the system time has either been configured manually or it is not synchronized with an (S)NTP server.
Network time protocol:	Activates synchronization via a web server.
Manual time set:	Manual setting of the system time if no SNTP server is available.

The switch does not have a battery-backed real-time clock. If the **time is entered manually**, the time may deviate after the device is started.

Primary SNTP server:	IP address or DNS name of the primary SNTP server.
Primary server description:	Description of the primary SNTP server.
Secondary SNTP server:	IP address or DNS name of the secondary SNTP server.
Secondary server description:	Description of the secondary SNTP server
UTC offset:	Selection of the time zone. The system time always refers to Greenwich Mean Time (winter). The local time is based on the system time and the UTC offset. The time difference for summer and winter time must be taken into account, if required.
Synchronization Status:	Displays the current status of synchronization with the SNTP server.
Last SNTP synchronization:	Displays the time of the last synchronization.

4.2.3.6 PROFINET Configuration

The “PROFINET Configuration” page is only displayed when PROFINET mode is active.

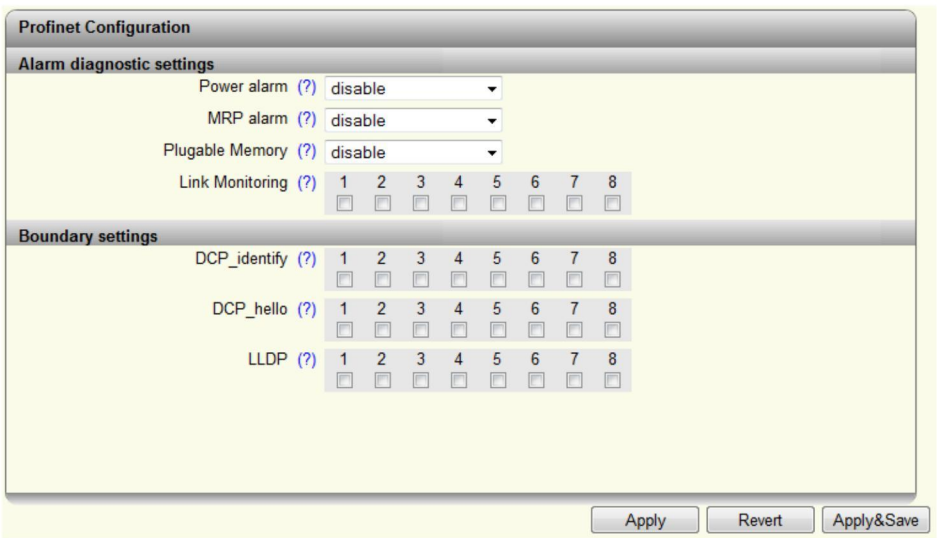


Figure 4-26 “PROFINET Configuration” web page

Alarm diagnostic settings

Power alarm:	Here, you can enable and disable the PROFINET alarm generated in the event of no power supply.
MRP alarm:	Here, you can enable and disable the PROFINET alarm for MRP ring errors.
Pluggable Memory:	Here, you can enable and disable the PROFINET alarm generated in the event of no configuration memory (SD card).
Link Monitoring:	Here, you can enable and disable the PROFINET alarm for link monitoring (link down behavior).

Boundary settings

DCP_identify:	Here, you can set the forwarding of DCP identify packets for specific ports.
DCP_hello:	Here, you can set the forwarding of hello packets for specific ports.
LLDP:	Here, you can set the forwarding of LLDP packets for specific ports.

4.2.3.7 Port Configuration

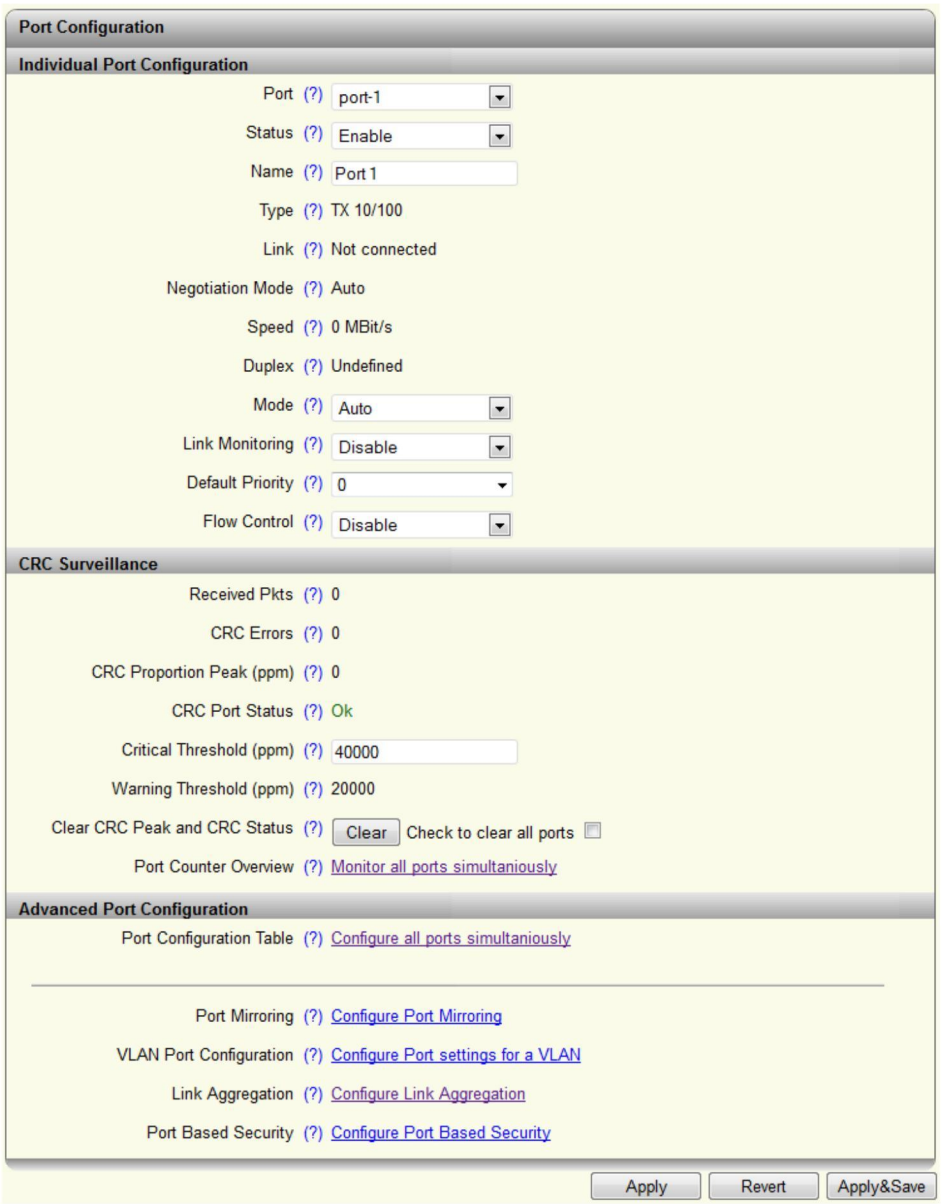


Figure 4-27 “Port Configuration” web page

Port Configuration – Individual Port Configuration

Individual Port Configuration

Port:	Select the port that you want to configure individually.
Status:	The port can be activated/deactivated here.
Name:	You can assign a name to the port.
Type:	Describes the physical properties of the port.

Link:	Shows the current link status of the port.
Negotiation Mode:	Shows the current auto negotiation status.
Speed:	Displays the current transmission speed at which the port is operating.
Duplex:	Displays the transmission mode of the port.
Mode:	The port can be set to a fixed speed and transmission mode here, and fast startup can also be set.

When using fast startup, RSTP must be deactivated in order to establish a fast link.

Link Monitoring:	Here, specify whether the link behavior is to be monitored at the selected port.
Default Priority:	Here, set the priority for incoming data packets to this port.

The “Jumbo Frames” function is only available for 21xx/23xx/25xx Gigabit versions.

Jumbo Frames:	Here, you can enable/disable the support of jumbo frames (>1518 bytes). The MTU size is set to 9600 bytes following activation.
MTU:	Here, you can set the maximum transmission unit (MTU). Packet sizes between 1522 bytes and 9600 bytes are accepted.
Flow Control:	Flow control for the selected port can be enabled and disabled here.

Port Configuration – CRC Surveillance

CRC Surveillance

Received Pkts:	Shows the number of packets received at the selected port since the last reboot or counter reset.
CRC Errors:	Shows the number of CRC errors at the selected port since the last reboot or counter reset.
CRC Proportion Peak (ppm):	Shows the highest proportion of CRC errors that occurred in a 30-second interval, relative to the total number of packets received in this interval since the last reboot or counter reset.
CRC Port Status:	Shows the status of the current port.
Critical Threshold (ppm):	Here, you can enter the threshold value at which the CRC Port Status switches to Critical (1000 ppm - 1,000,000 ppm are acceptable).
Warning Threshold (ppm):	Shows the threshold value in ppm at which the CRC Port Status switches to Warning (50% of Critical Threshold).
Clear CRC Peak and CRC Status:	Clicking the “Clear” button resets the CRC Peak and CRC Status.
Port Counter Overview:	Clicking on the “Monitor all ports simultaneously” link takes you to the “Port Counter” web page.

Port Configuration – Advanced Port Configuration

Advanced Port Configuration

Port Configuration Table:

Clicking on the “Configure all ports simultaneously” link takes you to the “Port Configuration Table” page.

There, you can set the status, mode, link monitoring, jumbo frames, and flow control for all ports.

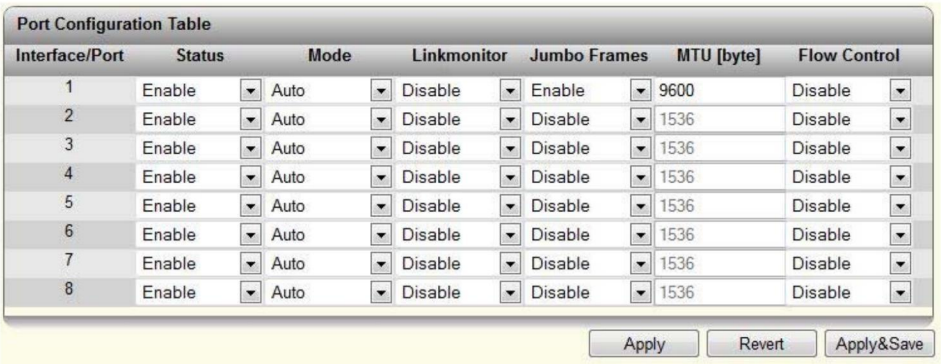


Figure 4-28 “Port Configuration Table” web page

Port Mirroring: Clicking on the “Configure Port Mirroring” button takes you to the port mirroring configuration (see “Port Mirroring” on page 64).

VLAN Port Configuration: Clicking on the “Configure Port Settings for a VLAN” button takes you to the “VLAN Port Configuration” page (see “VLAN Configuration” on page 85).

Link Aggregation: Clicking on the “Configure Link Aggregation” button takes you to the “Link Aggregation” page (see “LACP – Link Aggregation Control Protocol” on page 73).

Port Based Security: Clicking on the “Configure Port Based Security” button takes you to the “Port Based Security” page (see “Security” on page 51).

4.2.3.8 VLAN Configuration

For further information on “VLAN”, refer to section Section “Virtual Local Area Network – VLAN” on page 85.

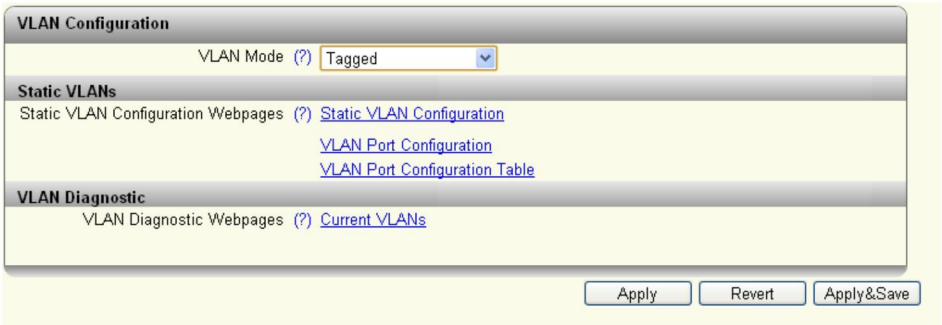


Figure 4-29 “VLAN Configuration” web page

4.2.3.9 Multicast Filtering

For further information on “Multicast”, refer to section “Multicast Filtering” on page 83.

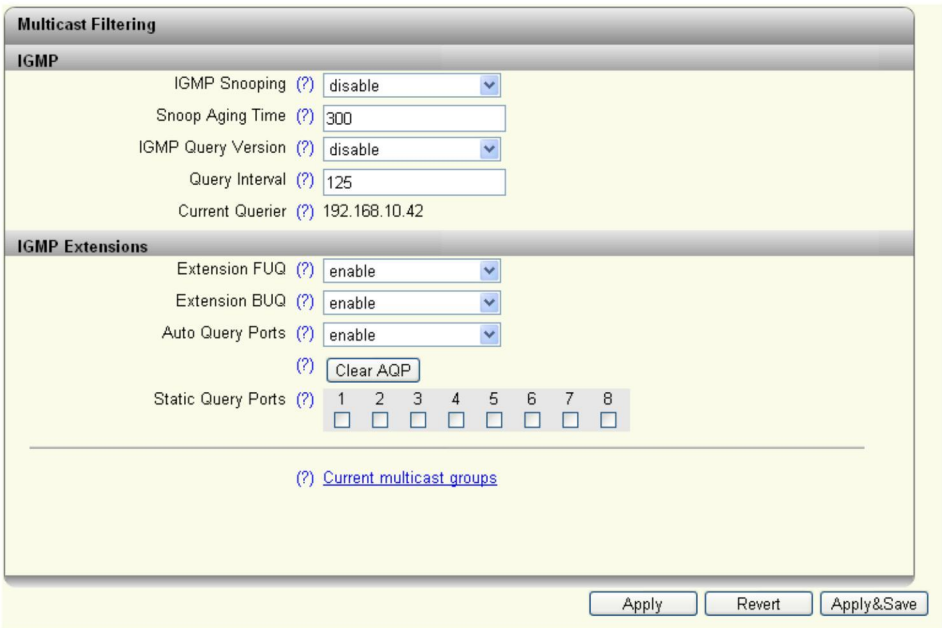


Figure 4-30 “Multicast Filtering” web page

4.2.3.10 Network Redundancy

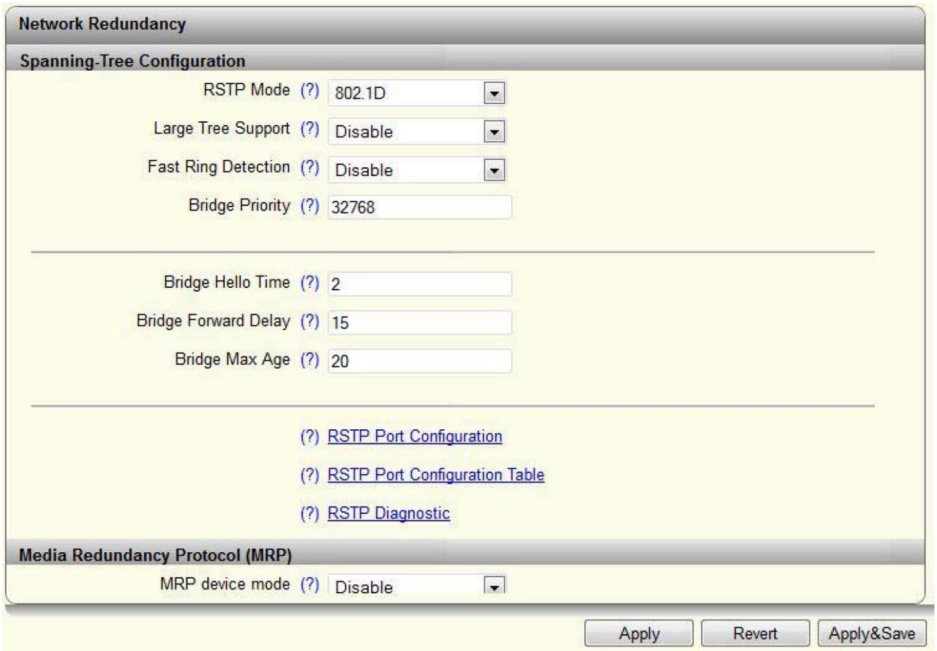


Figure 4-31 “Spanning-Tree Configuration” area

Network Redundancy

Spanning-Tree Configuration

RSTP Mode:

- Disable: The RSTP function is not activated
- 802.1D: The RSTP function is activated globally and working in accordance with standard IEEE802.1D-2004

The functions below are only available if “802.1D” is activated.

The Large Tree Support and Fast Ring Detection functions are only available on the 22xx/23xx/24xx/25xx versions.

Large Tree Support: 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.

Fast Ring Detection: This function speeds up switch-over to a redundant path in the event of an error and enables easy diagnostics. RSTP Fast Ring Detection assigns an ID to each ring. This ID is communicated to every switch in the respective ring. One switch can belong to several different rings at the same time.

Bridge Priority:	The bridge and backup root can be specified via “Bridge Priority”. Only multiples of 4096 are permitted. The value will be rounded automatically to the next multiple of 4096. When you click on “Apply&Save”, the initialization mechanism is started (default value: 32,768).
Bridge Hello Time:	Specifies the time interval within which the root bridge regularly reports to the other switches via BPDU.
Bridge Forward Delay:	The value indicates how long the switches are to wait for the port state in STP mode to change from “Discarding” to “Listening” and from “Listening” to “Learning” (2 x Forward Delay).
Bridge Max Age:	The parameter is set by the root switch and used by all switches in the ring. The parameter is sent to ensure that each switch in the network has a constant value, which is used as the basis for testing the age of the saved configuration.

Clicking on the “RSTP Port Configuration” button takes you to the “RSTP Port Configuration” pop-up (see page 49).

Clicking on the “RSTP Port Configuration Table” button takes you to the “RSTP Port Configuration Table” pop-up (see page 50).

Clicking on the “RSTP Diagnostics” button opens the “RSTP Diagnostics” page as a pop-up (see page 63).

Network Redundancy

Media Redundancy Protocol (MRP)

MRP device mode:

- Disable: The MRP function is not activated
- Client: The MRP function is activated and the switch is the client
- Manager: The MRP function is activated and the switch is the ring manager

The MRP manager function is only available on 22xx/23xx/24xx/25xx versions and can be implemented via the FL SD FLASH/MRM configuration memory.

VLAN:	If the VLAN mode is set to “Tagging”, you can select the VLAN here to which the MRP control packets should be forwarded.
Ring Port 1:	Select the first MRP ring port here
Ring Port 2:	Select the second MRP ring port here

Pop-up: RSTP Port Configuration

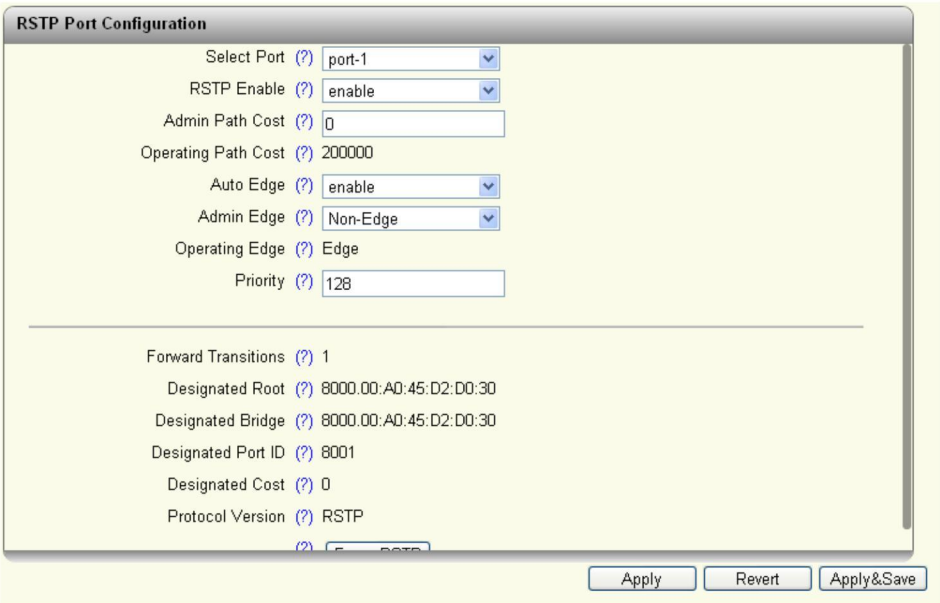


Figure 4-32 “RSTP Port Configuration” web page

Select Port:	Here, select the port for which you want to change the RSTP settings.
RSTP Enable:	– Enable: RSTP is activated for the port – Disable: RSTP is deactivated for the port
Admin Path Cost:	Displays the path costs set for this port. A path cost equal to “0” activates cost calculation according to the transmission speed (10 Mbps = 2,000,000; 100 Mbps = 200,000).
Operating Path Cost:	Displays the path costs used for this port.
Auto Edge:	Here, you can specify whether to automatically switch from non-edge port to edge port after a link up.
Admin Edge:	Here, you can specify whether this port is to be operated as an edge port (default setting), if possible.
Operating Edge:	Shows whether this port is operated as an edge port or a non-edge port.
Priority:	Shows the priority set for this port (default value: 128).
Forward Transitions:	Indicates the number of times the port has switched from the “Discarding” state to the “Forwarding” state.
Designated Root:	Shows the root bridge for this spanning tree.
Designated Bridge:	Indicates the switch from which the port receives the best BPDUs.
Designated Port ID:	Indicates the 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:	Shows the path costs of this segment to the root switch.
Protocol Version:	Shows the protocol version.
Force RSTP:	Clicking on the “Force RSTP” button activates RSTP for the port as long as it has been operated in STP mode beforehand.

Pop-up: RSTP Port Configuration Table

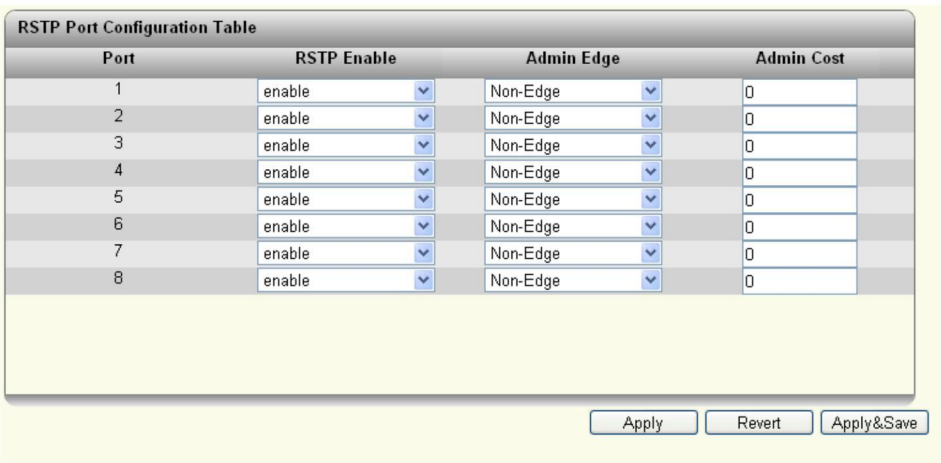


Figure 4-33 “RSTP Port Configuration Table” web page

Port:	Shows the ports for which RSTP is available.
RSTP Enable:	Here, you can activate or deactivate RSTP for each port individually.
Admin Edge:	Here, you can specify whether this port is to be operated as an edge port (default setting), if possible.
Admin Cost:	Displays the path costs set for this port. A path cost equal to “0” activates cost calculation according to the transmission speed (10 Mbps = 2,000,000; 100 Mbps = 200,000).

Link Aggregation

Clicking on the link takes you to the configuration page for link aggregation.

4.2.3.11 Security

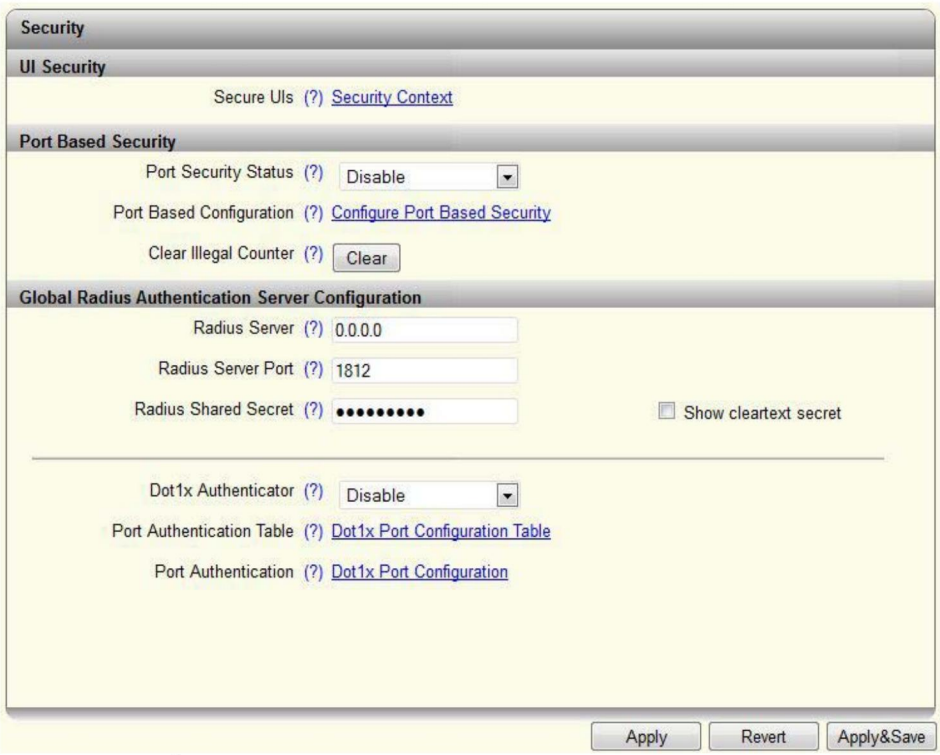


Figure 4-34 “Security” web page

UI Security

Secure UIs:	Clicking on the “Security Context” link opens the pop-up of the same name (see “Pop-up: Security Context” on page 34).

Port Based Security

Port Security Status:	Here, you can globally enable and disable port-based security.
Port Based Configuration:	Clicking on the “Configure Port Based Security” link takes you to the configuration page for port-based security (see ““Port Based Security” web page” on page 52).
Clear Illegal Counter:	Clicking on the “Clear” button sets the illegal access counter for all of the ports to zero.

Security

Global Radius Authentication Server Configuration

Radius Server IP Address:	Here, you can set the IP address of the RADIUS authentication server.
Radius Server Port:	Here, you can set the UDP port of the RADIUS server (default: 1812).
Radius Shared Secret:	Here, you can set the shared secret required for encrypted communication with the RADIUS authentication server. The shared secret must not exceed 128 characters.
Dot1x Authenticator:	Here, you can specify whether the device should be an 802.1x authenticator or not.

One end device can be authenticated via 802.1x per port.

Port Authentication Table:	Clicking on the “Dot1x Port Configuration Table” link takes you to the table-based configuration page for RADIUS authentication (see ““Dot1x Port Configuration Table” web page” on page 54).
Port Authentication:	Clicking on the “Dot1x Port Configuration” link takes you to the port-based configuration page for RADIUS authentication (see ““Dot1x Port Configuration” web page” on page 55).

“Port Based Security” web page

All of the configurations on the “Port Based Security” web page only take effect if the “Port Security Status” function is activated on the “Security” web page (see section “Security” on page 51).

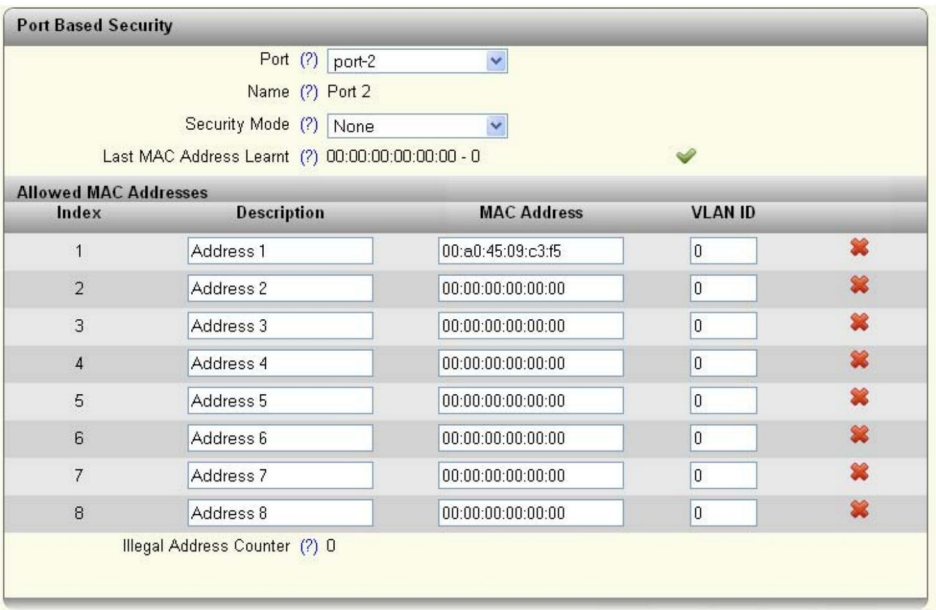


Figure 4-35 “Port Based Security” web page

Port:	Select the port for which the security settings should be made.
Name:	Displays the name of the selected port.
Security Mode:	Here, set what happens if a MAC address that is not permitted is detected by the device. – None: No security settings for this port. – Trap: If a MAC address that is not permitted is detected at the port, a trap is sent to the defined SNMP trap server (see section “Trap Manager” on page 65). The packets are not blocked. – Block: If a MAC address that is not permitted is detected at the port, all packets are blocked at the port and a trap is sent to the defined SNMP trap server (see section “Trap Manager” on page 65). The packets at this port remain blocked until a permitted MAC address is detected.
Last MAC Address Learnt:	Displays the MAC address of the last connected device. By clicking on the green checkmark, this MAC address can be added to the list of permitted MAC addresses.
Illegal Address Counter:	Displays the number of times a port has been accessed illegally. Each initial access by a MAC address is counted. Repeated access by known MAC addresses are counted twice if a different MAC address has accessed the port in the meantime.

“Port Based Security” web page

Allowed MAC Addresses

Up to 50 MAC addresses are permitted per port. Each MAC address can only be permitted at one port. MAC addresses that are permitted at one port also cannot be dynamically learned at other ports.

The web-based management or network cannot be accessed via a MAC address that is permitted at another port.

Index:	Displays the index of the permitted MAC addresses.
Description:	Here, you can provide a description for a permitted MAC address.
MAC Address:	Enter a MAC address for which you want to allow access. Alternatively, you can select the green checkmark to the right of the “Last MAC Address Learned” field to use the last MAC address that was learned.
VLAN ID:	Enter the VLAN where the device with the permitted MAC address is located.

Clicking on the red “X” to the right of this column deletes the permitted MAC address for this port.

“Dot1x Port Configuration Table” web page

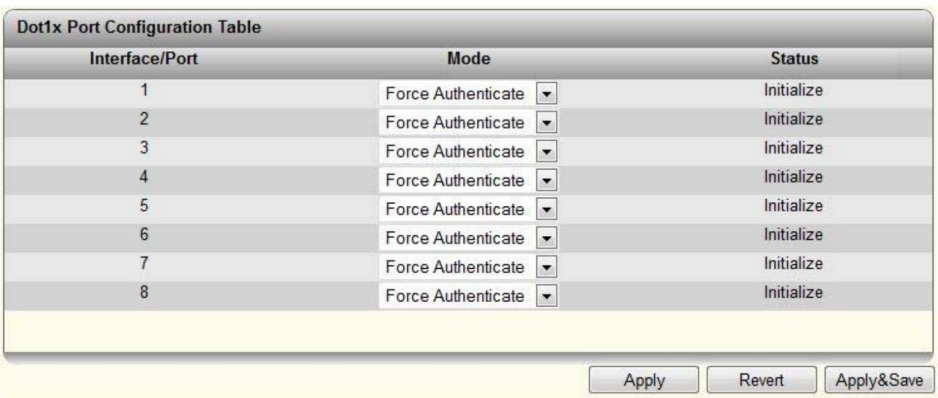


Figure 4-36 “Dot1x Port Configuration Table” web page

Interface/Port:	Displays the port number.
Mode:	Here, you can set the authentication mode for the port. – Auto: Devices connected to the port are authenticated via 802.1x. 802.1x (Dot1x Authenticator) must be activated for this. – Force Authenticate: All of the devices connected to the port are authenticated. – Force Unauthenticate: None of the devices connected to the port are authenticated.
Status:	Displays the authentication status of the port

“Dot1x Port Configuration” web page

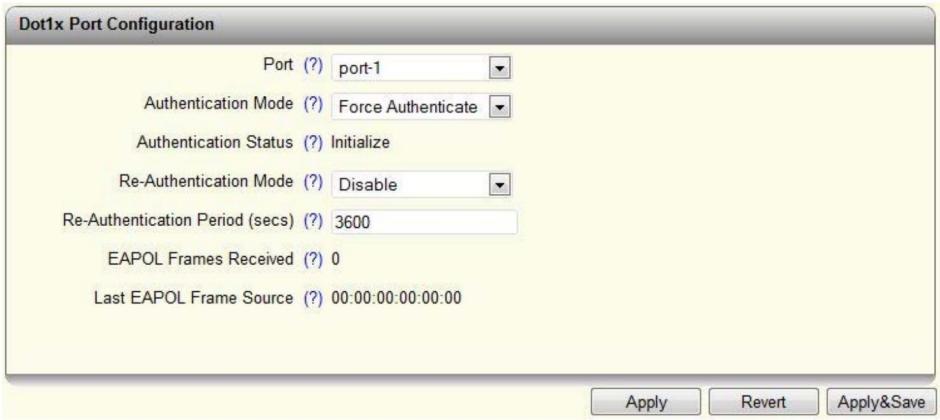


Figure 4-37 “Dot1x Port Configuration” web page

Port:	Here, select the port for which you wish to carry out RADIUS configuration.
Authentication Mode:	Here, you can set the authentication mode for the port. – Auto: Devices connected to the port are authenticated via 802.1x. 802.1x (Dot1x Authenticator) must be activated for this. – Force Authenticate: All of the devices connected to the port are authenticated. – Force Unauthenticate: None of the devices connected to the port are authenticated.
Authentication Status:	Displays the authentication status of the port
Re-Authentication Mode:	Here, you can specify whether a client should be re-authenticated at a regular interval.
Re-Authentication Period (secs):	Here, you can set the interval at which a client should be re-authenticated (1 ... 65,535 seconds).
EAPOL Frames Received:	Displays the received EAPOL packets.
Last EAPOL Frame Source:	Displays the last MAC address from which an EAPOL packet was received at the port.

4.2.3.12 DHCP Service

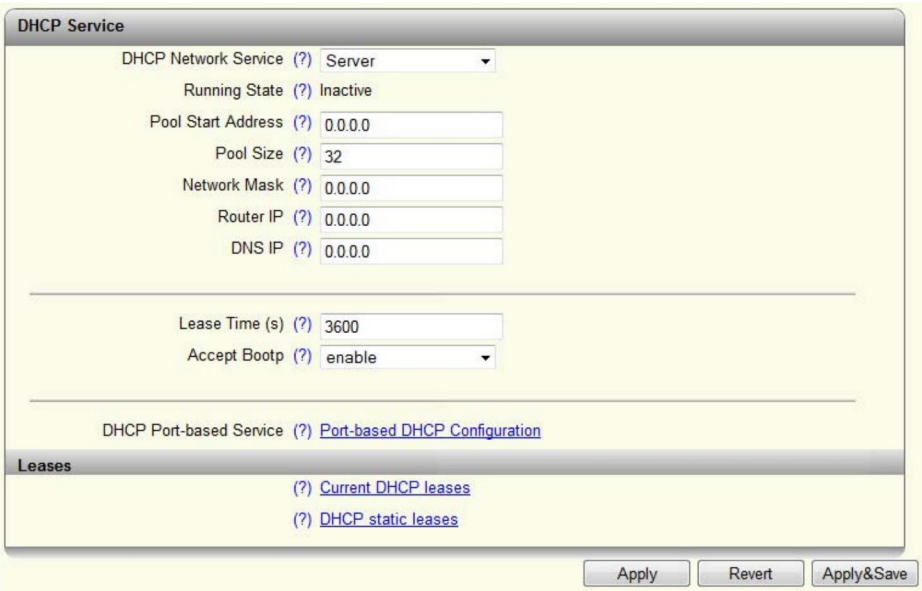


Figure 4-38 “DHCP Service” web page

DHCP network services are only available on the 22xx/23xx/24xx/25xx versions.

DHCP Network Service: Here, select the DHCP service you wish to use.

- None: No DHCP service will be used on the switch.
- Relay Agent: The DHCP relay agent (DHCP option 82) is enabled.
- Server: The switch will be used as the DHCP server.

The following fields are only available after selecting “Relay Agent” as the DHCP network service.

Option 82: Here, select the address that should be used as the remote ID.

- IP: Uses the IP address of the switch as the remote ID.
- MAC: Uses the MAC address of the switch as the remote ID.

Server IP Address: Here, set the IP address of the DHCP server in your network.

Port Mode: Here, select the ports for which the DHCP relay agent should be activated.

The following fields are only available after selecting “Server” as the DHCP network service. The “Server” DHCP network service can only be activated if the IP Address Assignment mode is set to “STATIC”.

Running State:	Shows the current status of the DHCP server. The status is “Inactive” if some setting options are incorrect.
Pool Start Address:	Here, set the first IP address of the DHCP server address pool.
Pool Size:	Here, set the number of IP addresses in the DHCP server address pool. Please note that the number of IP addresses must match the configured subnet.
Network Mask:	Here, set the subnet mask that is assigned to the DHCP clients.
Router IP:	Here, set the router/default gateway IP address that is assigned to the DHCP clients.
DNS IP:	Here, set the DNS IP address that is assigned to the DHCP clients.
Lease Time (s):	Here, you can set the time that the DHCP server leases an IP address to a client before it has to report to the server again. The value must be between 300 and 2,592,000 seconds; “0” is interpreted as an infinite time (default: 3600).
Accept Bootp:	Here, you can specify whether the switch acting as the DHCP server accepts BootP requests. If this function is activated, an IP address with an infinite lease time is assigned to the requesting DHCP clients.
DHCP Port-based Service:	Clicking on the “Port-based DHCP Configuration” link opens the “Port-based DHCP Configuration” pop-up (see “Pop-up: Port-based DHCP Configuration” on page 58).

Leases

Clicking on the “Current DHCP leases” link opens the “Current DHCP leases” pop-up where the IP addresses that are currently assigned are displayed (see “Pop-up: Current DHCP Leases” on page 58).

Clicking on the “DHCP static leases” link opens the “DHCP Static Leases” pop-up for configuring static IP address assignments (see “Pop-up: DHCP Static Leases” on page 59).

Pop-up: Port-based DHCP Configuration

You can configure the port-based DHCP server function in this pop-up.

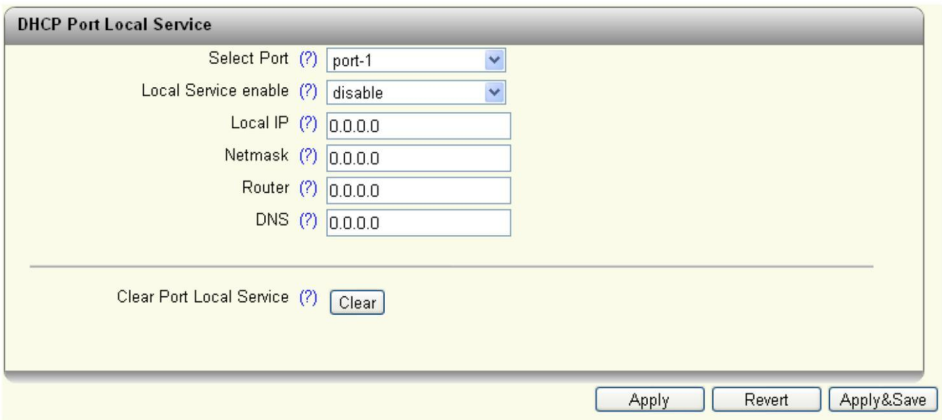


Figure 4-39 “DHCP Port Local Service” pop-up

Select Port:	Here, select the port for which you wish to carry out port-based DHCP server configuration.
Local Service enable:	Here, activate the port-based DHCP server function for the selected port.
Local IP:	Here, enter the IP address that is assigned to the client at the selected port.
Netmask:	Here, enter the subnet mask that is assigned to the client at the selected port.
Router:	Here, enter the gateway address that is assigned to the client at the selected port.
DNS:	Here, enter the DNS address that is assigned to the client at the selected port.

Pop-up: Current DHCP Leases

This pop-up displays the IP addresses that are currently assigned.

Leased IP:	Displays the assigned IP addresses.
Client ID:	Displays the MAC address of the client to which the IP address is assigned.
System Uptime:	Displays the time that has elapsed since the IP address was assigned to the client.
Local Port:	Displays the port to which the client is connected.
State:	Displays the status of the client.
Lease count:	Displays the number of assigned IP addresses.
Release:	Clicking on the “Release” button releases unused entries again.

Pop-up: DHCP Static Leases

This pop-up displays the configured static IP assignments. In addition, you can create new static IP assignments by assigning a fixed IP address to MAC addresses.

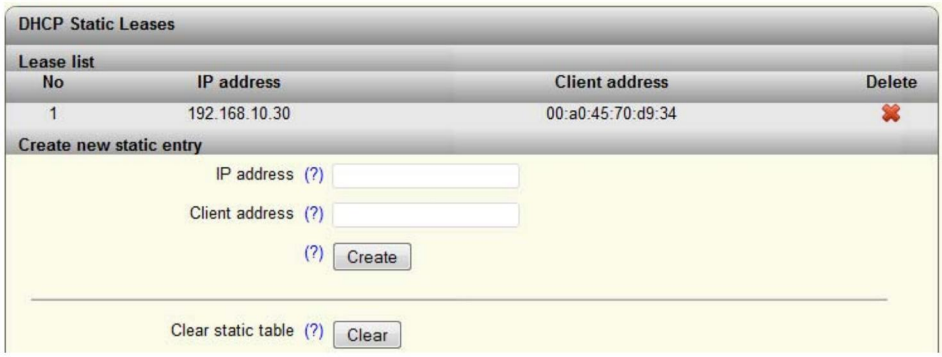


Figure 4-40 “DHCP Static Leases” pop-up

Lease list

IP address:	Displays the static IP address that is assigned.
Client address:	Displays the MAC address of the client.
Delete:	Clicking on the red “X” in the “Delete” column deletes the entry.

Create new static entry

IP address:	Here, enter the static IP address that you wish to assign.
Client address:	Here, enter the MAC address to which you wish to assign a static IP address.
Create:	Click on the “Create” button to perform the static assignment.
Clear static table:	Click on the “Clear” button to delete all the static DHCP leases.

4.2.3.13 Local Events

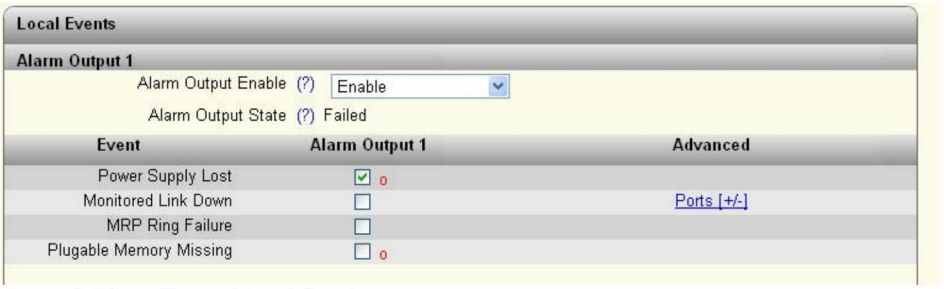


Figure 4-41 “Local Events” web page

Alarm output 1

Here, you can activate the digital alarm output (22xx/23xx versions) or signal contact and read the current status (if a red “**o**” is present, this event has occurred).

Events

Here, you can specify the conditions under which the digital alarm output or signal contact should report an error.

Power Supply lost:	An error message is generated if supply voltage US1 or US2 is lost
Monitored link down:	Under “Advanced”, select the ports to which link down behavior should be reported.
MRP Ring Failure:	An error message is generated in the event of an MRP ring error.
Pluggable Memory Missing:	An error message is generated if no memory card is present.

4.2.3.14 Quality of Service

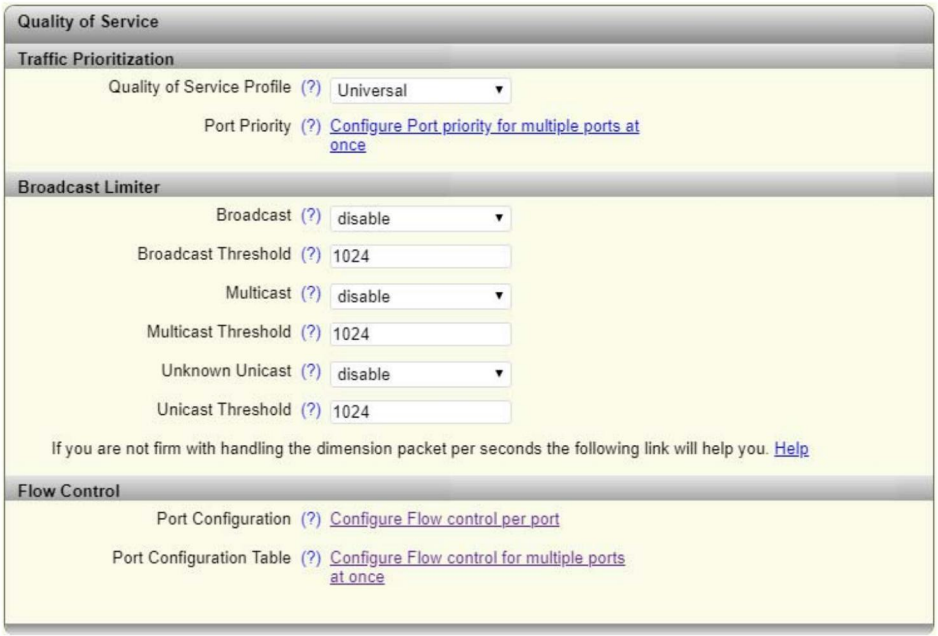


Figure 4-42 “Quality of Service” web page

Traffic Prioritization

The switches have eight priority queues into which incoming data traffic is sorted according to specific criteria. These queues are processed in descending order of priority. High-priority data traffic is therefore always forwarded first.

Quality of Service Profile:

Here, select the profile for prioritizing data traffic. The following selection options are available:

- Universal: This profile is the factory setting on standard versions. Class of Service (VLAN tag priority) is activated for data prioritization.
- PROFINET: This profile is the factory setting on PROFINET versions. Data prioritization based on Ethertype is activated in addition to Class of Service. In this profile, PROFINET data packets are always forwarded with high priority. Only control packets of redundancy protocols (RSTP and MRP) are given even higher priority.
- EtherNet/IP: In this profile, prioritization via DSCP values is activated in addition to Class of Service. This means that preferential treatment is given to EtherNet/IP data traffic. Only control packets of redundancy protocols (RSTP and MRP) are given even higher priority.

Port Priority:	Clicking on the link takes you directly to the configuration page for the default priority. Incoming data traffic on the device that does not have a priority tag is marked according to the setting and is assigned to a priority queue. To activate these settings, the VLAN mode of the device must also be set to “Tagged”.

Broadcast Limiter

Broadcast:	Here, activate or deactivate the broadcast limiter.
Broadcast Threshold:	Here, set the threshold value in frames per second for the broadcast limiter. The value entered is rounded down to the next valid value.
Multicast:	Here, you can activate or deactivate the multicast limiter.
Multicast Threshold:	Here, set the threshold value in frames per second for the multicast limiter. The value entered is rounded down to the next valid value.
Unknown Unicast:	Here, you can activate or deactivate the limiter for unknown unicasts. Unicasts of a MAC address that have been learned by the switch are not affected.
Unicast Threshold:	Here, set the threshold value in frames per second for the limiter of unknown unicasts. The value entered is rounded down to the next valid value.

Flow Control

Port Configuration:	Clicking on the “Configure Flow Control per port” link opens the “Port Configuration” web page, which contains the configuration options for flow control.
Port Configuration Table:	Clicking on the “Configure Flow control for multiple ports at once” link opens the “Port Configuration Table” web page where flow control can be configured for all ports.

The layer 3 functions supported by the NAT versions are described in “Layer 3 functions – routing and NAT”.

4.2.4 WBM diagnostics area

4.2.4.1 LLDP topology

For further information, please refer to section “LLDP – Link Layer Discovery Protocol” on page 79.

4.2.4.2 RSTP Diagnostic

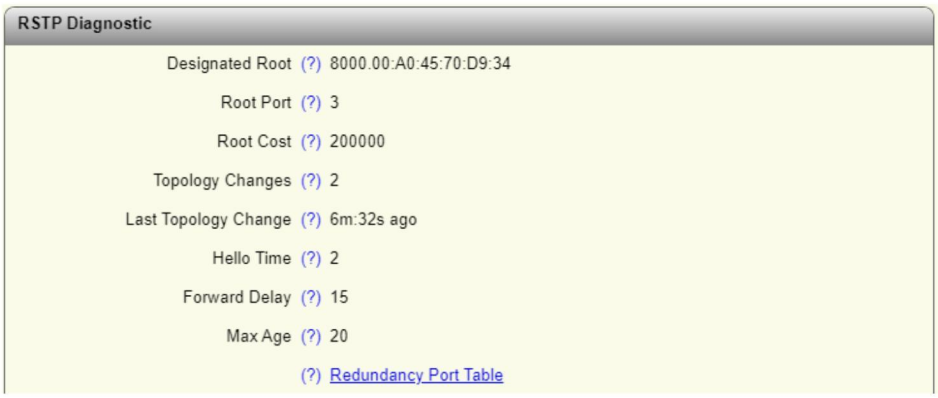


Figure 4-43 “RSTP Diagnostic” web page

Designated Root:	Shows the root bridge for this spanning tree.
Root Port:	Displays the port to which the root is connected. If the root is not directly connected, it shows the direction of the root.
Root Cost:	Displays the total path costs for the root.
Topology Changes:	Displays the number of topology changes.
Last Topology Change:	Displays when the last topology changes took place.
Hello Time:	Shows the hello time set at the root.
Forward Delay:	Shows the forward delay set at the root.
Max Age:	Shows the maximum age time set at the root.

Clicking on the “Redundancy Port Table” button opens a table containing information about the individual ports and their redundancy mechanism assignment.

4.2.4.3 MRP Diagnostic

Figure 4-44 “MRP Diagnostic” web page

Operating Mode:	Displays the current MRP device status.
MRP Manager Function:	Indicates whether an MRP manager license (MRM) is available.

The following fields are only available after selecting “Manager” as the operating mode.

Ring Status:	Displays the current status of the MRP ring.
Change Counter:	Displays the number of status changes in the MRP ring.

Clicking on the “Redundancy Port Table” button opens a table containing information about the individual ports and their redundancy mechanism assignment.

4.2.4.4 Current VLANs

For further information, please refer to Section “Pop-up: Current VLANs” on page 87.

4.2.4.5 Current Multicast Groups

For further information, please refer to Section “Multicast Filtering” on page 83.

4.2.4.6 Port Mirroring

The port mirroring function allows you to mirror the incoming and outgoing data traffic of individual ports to one port where it can be analyzed using a connected diagnostic device or tool.

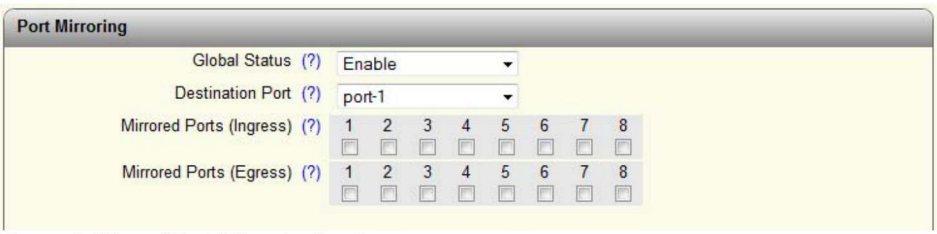


Figure 4-45 “Port Mirroring” web page

Global Status:	– Enable: Port mirroring is activated globally – Disable: Port mirroring is deactivated globally
Destination Port:	Under “Destination Port”, select the port to which the diagnostic device or tool is connected.
Mirrored Ports (Ingress):	Here, specify the ports from which the incoming data traffic should be mirrored.
Mirrored Ports (Egress):	Here, specify the ports from which the outgoing data traffic should be mirrored.

4.2.4.7 Trap Manager

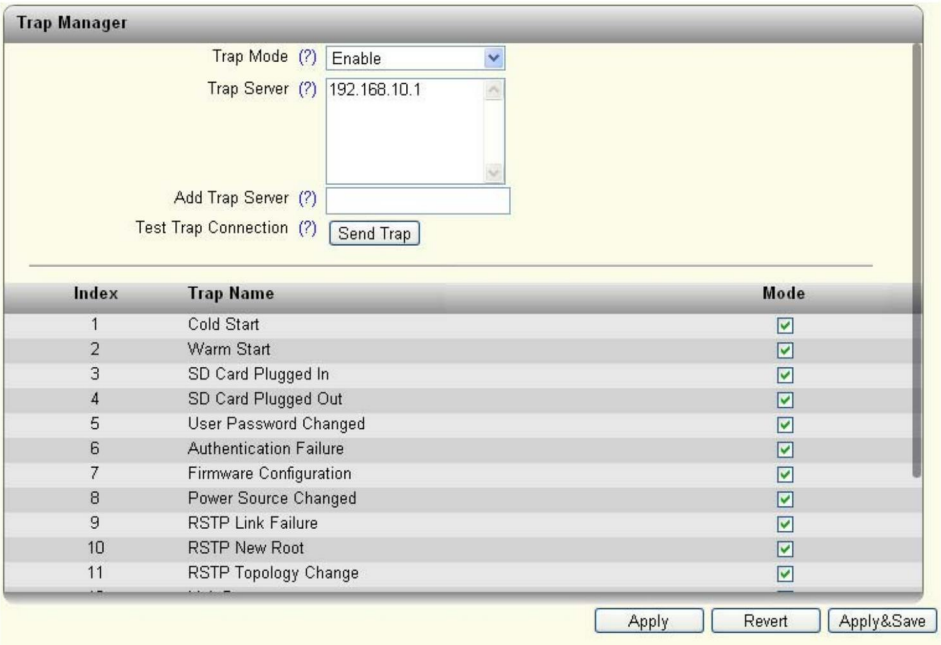


Figure 4-46 “Trap Manager” web page

Trap Mode:	– Enable: The sending of SNMP traps is enabled – Disable: The sending of SNMP traps is disabled
Trap Server:	All trap servers that are to receive SNMP traps from this device are displayed here.
Add Trap Server:	Here, enter the IP address or DNS name of a trap server and click on “Apply&Save” to create this trap server.
Test Trap Connection:	Click on the “Send Trap” button to test the connection to the trap server.

The table lists the SNMP traps that the device can send. Here, you can select the actions for which SNMP traps should be sent.

4.2.4.8 Port Counter

This page provides an overview of the port statistics for the device.

Four views provide an overview of the general, sent and received packets, errors, and collisions on the individual ports.

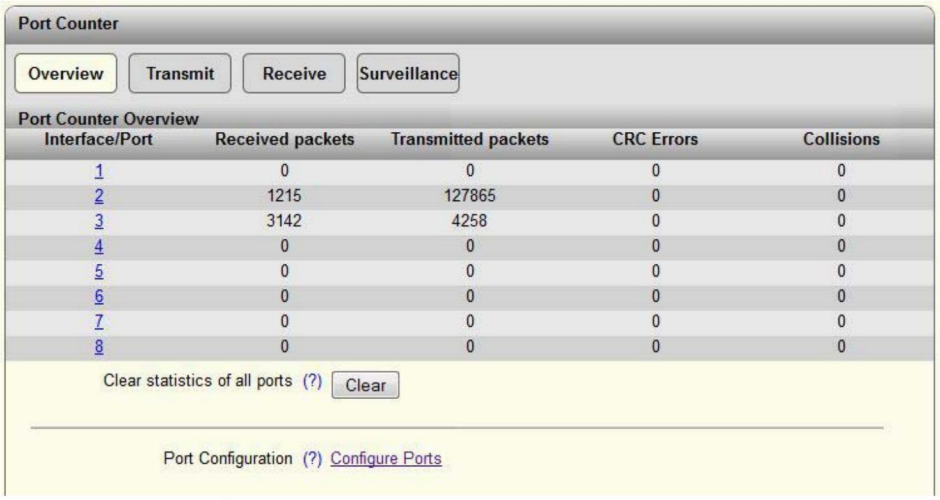


Figure 4-47 “Port Counter” web page

Interface/Port	Clicking on one of the port numbers in the “Interface/Port” column takes you to the port details pages. Here, you can view detailed statistics about the sent and received data packets for every port. In addition, the current and maximum port utilization is displayed as a percentage.
Clear statistics of all ports:	Clicking on the “Clear” button resets all of the port counters in the Overview, Transmit, and Receive views to zero. In Surveillance view, click the button to reset the CRC Proportion Peak and CRC Status of all ports.
Port Configuration:	Clicking on the “Configure Ports” link opens the “Port Configuration” page (see page 43).

Port details page

Figure 4-48 “Port Details” web page

Port Counter Overview: Clicking on the “Monitor all ports simultaneously” link takes you back to the “Port Counter” overview page.

Clear Port Statistics: Clicking on the “Clear” button resets all of the counters for the currently displayed port to zero.

4.2.4.9 Port Utilization

Here you will find an overview of the percentage port utilization for this device. For a detailed overview, click on the graph of an individual port.

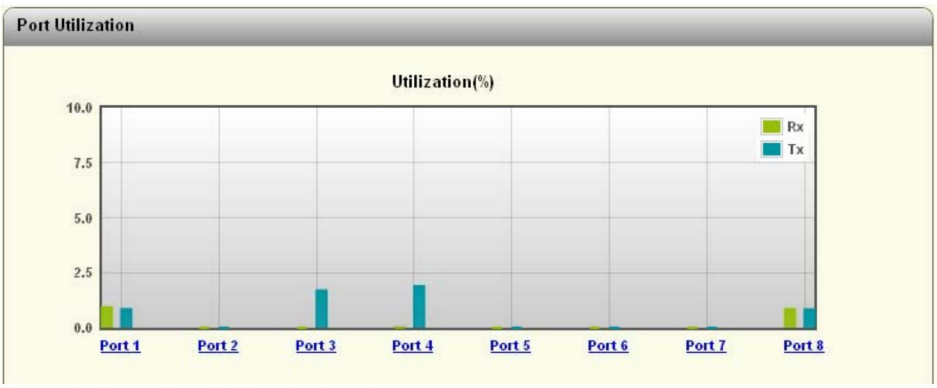


Figure 4-49 “Port Utilization” web page

4.2.4.10 Snapshot

You can use the snapshot function to capture and download all parameters relevant to the runtime (e.g., configuration, events, etc.) and provide them to a service technician.

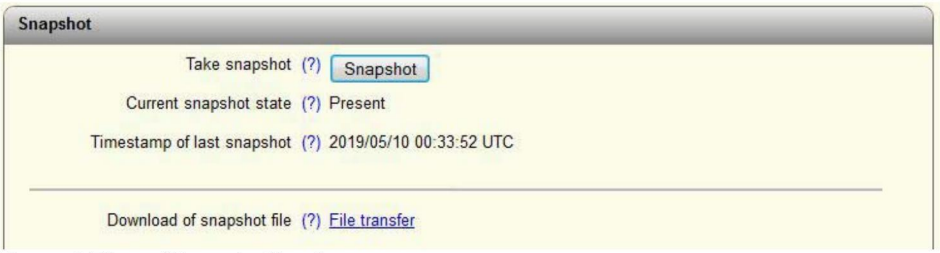


Figure 4-50 “Snapshot” web page

Take snapshot:	Click the “Snapshot” button to take a snapshot.
Current snapshot state:	Indicates whether the snapshot is available, is currently being generated or does not exist.
Timestamp of last snapshot:	Displays the time at which the last snapshot was generated.
Download of snapshot file:	Clicking on the “File transfer” link opens the window for manual file download.

4.2.4.11 Syslog

The Syslog function enables messages or events to be transmitted to one or more servers via UDP. In the event that two Syslog servers have been configured, the switch sends all messages/events to both servers.

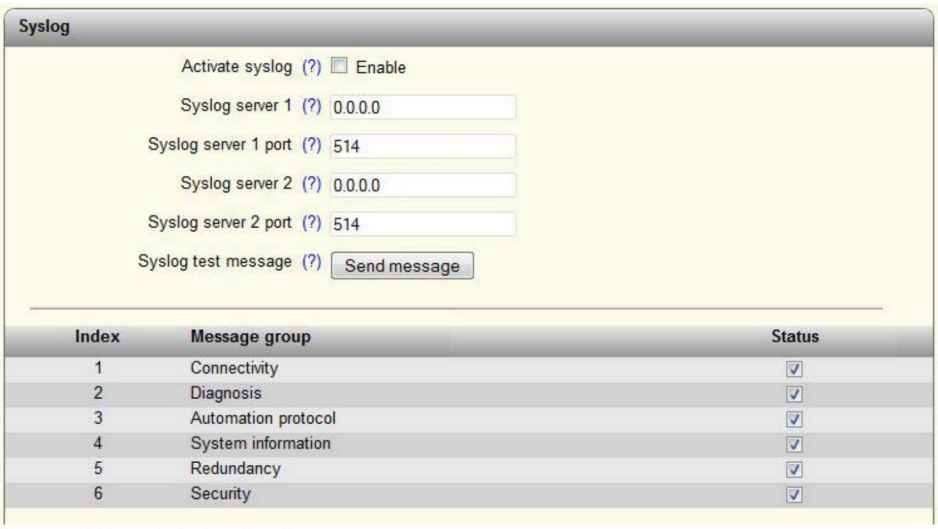


Figure 4-51 “Syslog” web page

Activate syslog:	Activate or deactivate the Syslog function here.
Syslog server 1:	Set the IP address or DNS name of the first Syslog server here.
Syslog server 1 port:	Set the UDP port of the first Syslog server here (default: 514).
Syslog server 2:	Set the IP address or DNS name of the second Syslog server here.
Syslog server 2 port:	Set the UDP port of the second Syslog server here (default: 514).
Syslog test message:	Click on the “Send message” button to test the connection to the Syslog server. With Syslog, message reception is not confirmed by the server. Therefore the connection status can only be checked on the server, and **not** in the web-based management of the switch.
Status:	Use the check boxes in the “Status” column to select the categories whose events are to be sent to the Syslog server. The table below provides an overview of the specific events in the respective categories.

Table 4-1 Syslog

Connectivity	IP conflict detected
	TFTP connection failed
	ACDconflict detected IP
	LLDP new neighbor on port
	LLDP neighbor information changed on port
	Link monitor alarm raises on port
	IP address changed on interface
	Port Link up/down
	SFP module plugged on Port
	ACD device has no IP
	MTU size changed
Diagnosis	CRC status and peak on port reset
	CRC status on port changed to ok
	CRC status on port changed to critical
	CRC thresholds on port changed by user
	Alarm output failed
	CRC status on port changed to warning
Automation protocol	PROFINET diagnosis available
	IP address changed via PROFINET
	Name of the device changed via PROFINET
	PROFINET connection lost
	PROFINET module different on slot

System information	System time synchronized
	Pluggable memory removed
	Update firmware successful
	Configuration saved/loaded on/from pluggable memory
	Update failed
	Configuration difference detected
	Configuration saved/loaded successfully
	Configuration parameter changed
	Smart Mode entered
	Smart Mode button enabled/disabled
	SD card slot enabled/disabled
	Error in configuration file
	Pluggable memory cleared
	New interface created
	Power supply lost
	Name of the device changed
	Parameter has been changed by the user
	FW image not valid
	Update processing
	Write to flash memory
	Wrong update image
	IGMP Snooping mode changed
	IGMP Snooping aging time changed
	Syslog test message
	Start FW update
	Write FW image into flash
Redundancy	RSTP ring detected
	RSTP topology changed
	RSTP root changed
	RSTP ring failed
	MRP client/manager activated
	MRP ring failed
	MRP link failed at port

Security	Port access violation on Port
	Radius Authentication Server shared secret changed
	Port successfully authenticated
	Password changed
	User authentication failed
	Radius Authentication Server IP/UDP address changed
	User configuration changed
	User Login/Logout
	Unauthorized access

4.2.4.12 SFP Diagnostics

This page is only available on devices with SFP ports.

Here you will find an overview of the SFP ports.

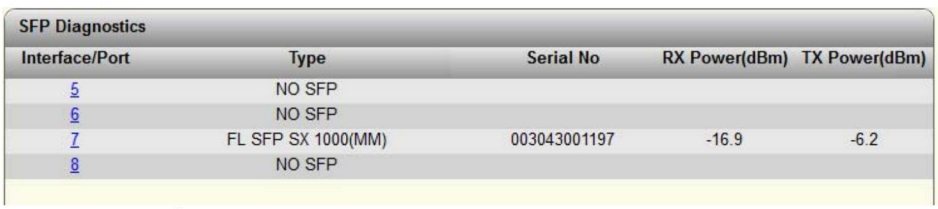


Figure 4-52 “SFP Diagnostics” web page

Interface/Port	The ports that can be used with SFP modules are displayed here. Clicking on a port number opens the port configuration for that port.
Type:	The type of SFP module used is displayed here. If no SFP module is inserted, “NO SFP” is displayed.
Serial No:	This column displays the serial number of the SFP module used.
RX Power(dBm):	This column displays the incoming power level.
TX Power (dBm):	This column displays the outgoing power level.

5 LACP – Link Aggregation Control Protocol

The Link Aggregation function enables you to bundle several physical LAN interfaces to create a logical channel referred to as a trunk. This makes it possible to transfer larger quantities of data and improve failsafe performance. If one or more physical connections of a trunk fail, the remaining connections handle the data load as far as possible.

Using a trunk does not mean that the data throughput is multiplied, as all data communication frames are always processed via a single connection only. I.e., a trunk with two connections cannot automatically transmit 2 Gbps in the case of a Gigabit switch.

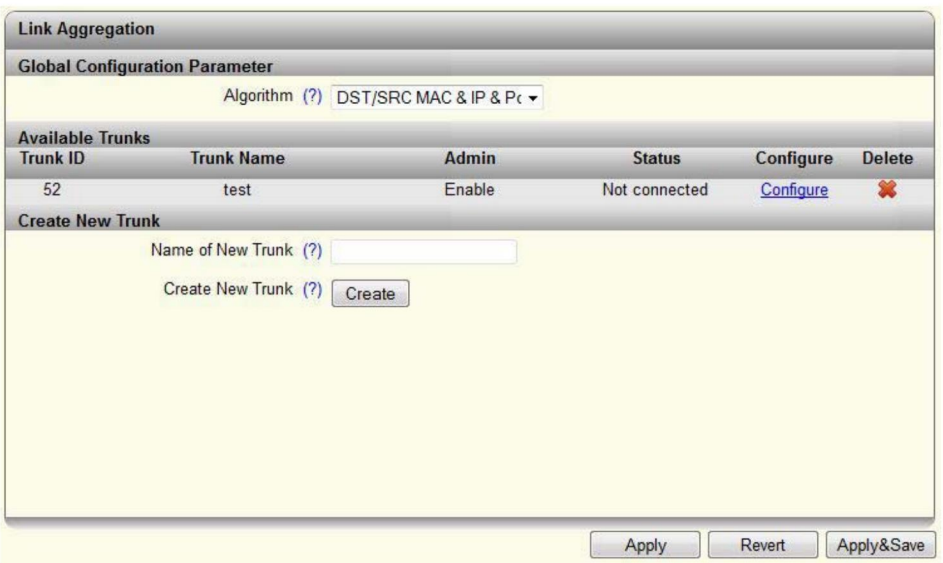


Figure 5-1 “Link Aggregation” web page

Algorithm:	Here, you can set the algorithm that is responsible for the load distribution and that decides which physical connection is used for data communication. The various algorithms use the MAC or IP addresses of the source or destination fields, or the TCP/UDP port numbers.
Name of New Trunk:	Here, you can enter a name for a new trunk.
Create New Trunk:	Click on the “Create” button to create a new empty trunk.
Configure:	Clicking on the “Configure” link in the table containing all the created trunks opens the configuration page for the respective trunk.

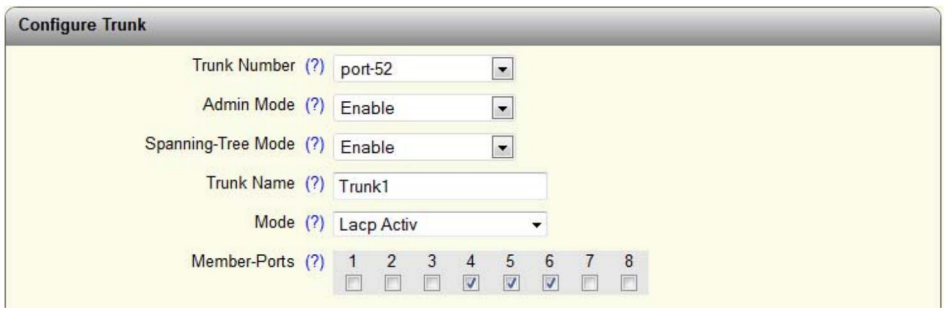


Figure 5-2 “Configure Trunk” web page

Trunk Number: Here, select the trunk to be configured by entering its ID.

Admin Mode: Here, you can enable and disable a trunk.

Spanning-Tree Mode: Here, select whether the RSTP protocol is to be enabled for this trunk.

Trunk Name: Here, you can change the name of the trunk.

Mode: Here, you can specify how ports are to be added to the trunk.

- If you select “Static”, the ports are immediately added to the trunk.
- When “LACP Active/Passive” is selected, the two members of a link aggregation first exchange information via LACPDUs:
  - With “Active”, this is regardless of whether the peer also has LACP.
  - With “Passive”, this only occurs after LACPDUs have been received by the peer.

If the switch is used as an MRP client and if a trunk port was selected for at least one ring port, increased recovery times may be required in the MRP ring if “LACP Active/Passive” is activated.

In this case, it is therefore recommended to select “Static” mode.

Member-Ports: Here, select up to four ports that are to belong to the trunk.

6 SNMP – Simple Network Management Protocol

General function

SNMP is a non-proprietary standard for network management. It defines commands for reading and writing information, and defines formats for error and status messages. SNMP is also a structured model that consists of agents, their respective MIB (Management Information Base), and a manager.

The manager is a software tool that is executed on a network management station. The agents are located inside switches, bus terminals, 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 via data that is written to the MIB by the manager. In the event of an emergency, the agents can also send messages (traps) directly to the manager.

All configuration changes that are to take effect after a device restart must be saved permanently using the “flWorkFWCtrlConfSave” object.

SNMP interface

All managed Factoryline components have an SNMP agent. The agent for this type of device manages the following MIBs (Management Information Bases):

- FL Managed Infrastructure MIB
- lldpMIB
- RFC1213 MIB
- rmon
- snmpMIB
- ifMIB
- snmpFrameworkMIB
- etherMIB
- pBridgeMIB
- qBridgeMIB
- dot1dBridge
- rstpMIB
- IP MIB

Network management stations, such as a PC with an MIB browser, can read and modify the configuration and diagnostic data of 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 respective device must be made available to the SNMP management tools.

On the one hand, these are globally valid MIBs, which are defined and described in RFCs (Requests for Comments). For example, this includes MIB2 in accordance with RFC1213, which is supported by all SNMP-capable network devices. On the other hand, manufacturers can define their own private 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 (object name and

parameters) may be assigned to an object ID and published. If this object is then no longer needed, it is labeled as expired, but it cannot be reused, e.g., 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. Although a password is required for read access in SNMP, this is set to “public”, which is usual for network devices, and cannot be changed.

In the delivery state, the password for write access is “private” and can be changed by the user.

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

Use of SNMPv3

When using SNMPv3, several points must be observed when accessing the SNMP objects. In contrast to SNMPv2, SNMPv3 is a protected protocol where the message contents and passwords are transmitted in encrypted format.

To use SNMPv3, you must first configure the switch accordingly (see “Service” on page 39). In addition, you need to switch your MIB browser to SNMPv3:

- MD5 as the algorithm for authentication
- DES as the algorithm for privacy
- User name: “admin”
- Password: Current device password of the user „admin“
  (Note: The password must be at least eight characters long. If the default password is “private”, “private_” must be used for access.).
  If the “separate SNMPv3 password” option is activated, this applies in combination with the user “admin”.

Another benefit for the user is the option of sending traps using the Simple Network Management Protocol (see “Trap Manager” on page 65).

Management Information Base (MIB)

Description 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 request by a manager or in response to a specific event, the agent transmits the collected information to the management station.

Not all devices support all object classes.

- If an unsupported object class is requested, an error message is generated.
- If an attempt is made to modify an unsupported object class, an error message is also generated.

The descriptions of the individual SNMP objects are located in the respective MIBs and can be downloaded from the Phoenix Contact e-shop. Please note that the MIB is located in the respective software package (zip file) of a firmware.

7 LLDP – Link Layer Discovery Protocol

Basic principles

LLDP

The switch supports LLDP in accordance with IEEE 802.1ab and thus 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 or sent to neighbors, as long as LLDP is activated:

- The device sends its own management and connection information to neighboring devices.
- The device receives management and connection information from neighboring devices.

Please note that a port that is blocked via RSTP does not receive any LLDP BPDUs, but is still able to send them.

LLDP general

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

Function

A network infrastructure component sends 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 peer connected to the respective port learns the corresponding port-specific neighbors from these BPDUs.

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

The switch manages a maximum of 50 items of neighbor information. Any information beyond this is ignored.

If several neighbors are displayed at one switch port, then at least **one other** switch/hub that does not support LLDP or does not have LLDP activated is installed **between** this switch and the neighbor indicated.

Table 7-1 Event table for LLDP

Event	Action of the individual LLDP agent	Response of the neighboring LLDP agent
Activate LLDP agent or device start	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	Transmit 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	-
Receipt of a BPDU from a new neighbor	Extend list of neighbors and respond with port-specific BPDU	Include sender in the list of neighbors

LLDP configuration in web-based management

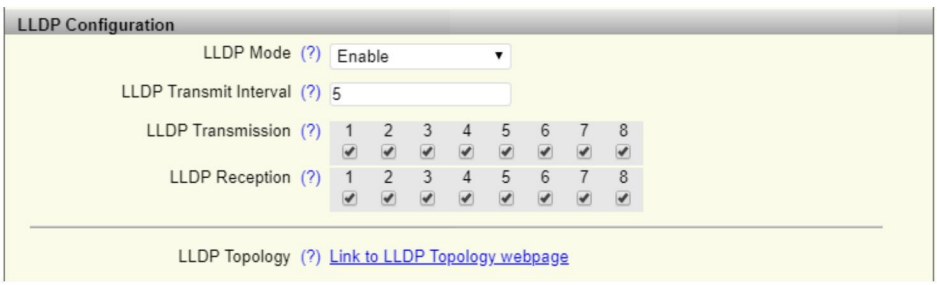


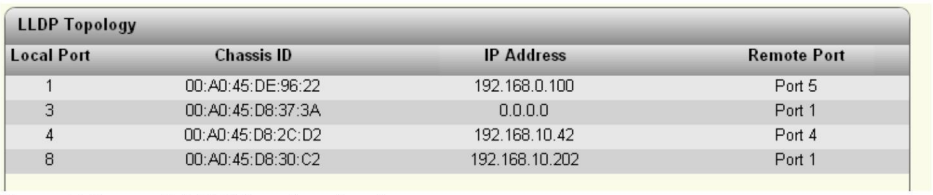
Figure 7-1 “Link Layer Discovery Protocol” web page

For 20xx/21xx version devices, LLDP can be activated or deactivated globally for all ports.

The 22xx/23xx/24xx/25xx version devices also offer a port-based configuration option for sending and receiving LLDP BPDUs.

LLDP can be configured in WBM (see “Service” on page 39).

LLDP diagnostics in web-based management



LLDP Topology

Local Port	Chassis ID	IP Address	Remote Port
1	00:A0:45:DE:96:22	192.168.0.100	Port 5
3	00:A0:45:D8:37:3A	0.0.0.0	Port 1
4	00:A0:45:D8:2C:D2	192.168.10.42	Port 4
8	00:A0:45:D8:30:C2	192.168.10.202	Port 1

Figure 7-2 “LLDP Topology” web page

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

Local Port:	Contains the port number of the local switch that is used to connect a neighbor to this switch.
Chassis ID:	MAC address of the connected neighboring device.
IP Address:	Management IP address for the neighbor.
Remote Port:	Port number of the neighboring switch that is used to connect the neighbor to the local switch.

8 Multicast Filtering

Multicast Configuration **Multicast Filtering**

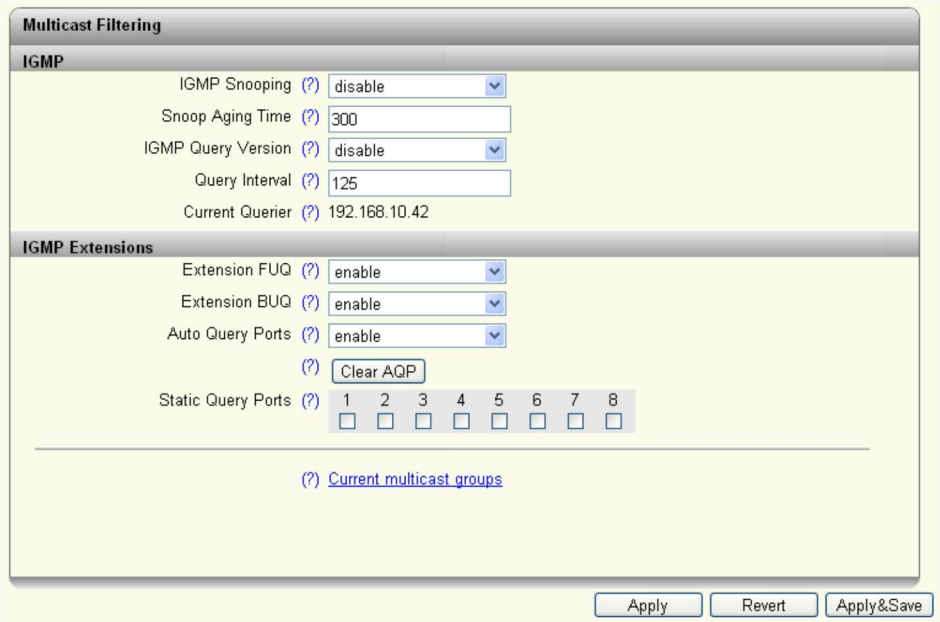


Figure 8-1 “Multicast Filtering” web page

IGMP Snooping:
- disable: The “IGMP Snooping” function is disabled.
- enable: The “IGMP Snooping” function is enabled.

Snoop Aging Time: Here, you can set the snoop aging time.

The snoop aging time is the time period during which membership reports are expected from the querier. If no membership reports are received during this time, the associated ports are deleted from the multicast groups.

The value must be between 30 and 3600 (default: 300).

IGMP Query Version: Here, you can set the IGMP query version which the switch should use to send the queries.

The switches support IGMP query versions v1 and v2. For EtherNet/IP applications, it is recommended that you activate version v2.

Query Interval: Here, you can set the interval at which the switch should send the queries.

Current Querier: Displays the IP address of the current querier in the network.

The IGMP querier function can only be used if the device has an IP address. Use of multicast filtering in Unmanaged mode is therefore limited to IGMP snooping.

Extensions FUQ (Forward Unknown to Querier):	Here, specify whether a multicast group should be created for unknown multicast packets, which forwards the packets in the direction of the querier.
Extension BUQ (Block Unknown at Querier):	Here, specify whether unknown multicast packets should be blocked at the querier.
Auto Query Ports:	Here, specify whether automatic selection of additional query ports is activated. Ports are automatically integrated in every multicast group. In the case of redundancy switch-over, the multicast packets are not blocked because the ports required are already members of the multicast group.
Clear AQP:	Button for deleting the ports that are automatically assigned to the groups.
Static Query Ports:	Select the ports that are static query ports.

Clicking on the “Current multicast groups” link opens the “Current Multicast Groups” web page as a pop-up.

The device can manage up to 50 dynamic multicast groups.

Current Multicast Groups

VLAN ID	Multicast Address	Port Member
1	01:00:5e:00:01:81	56
1	01:00:5e:40:0e:c1	56
1	01:00:5e:40:0f:00	56
1	01:00:5e:7f:ff:fa	6, 56

Figure 8-2 “Current Multicast Groups” web page

9 Virtual Local Area Network – VLAN

VLAN Configuration

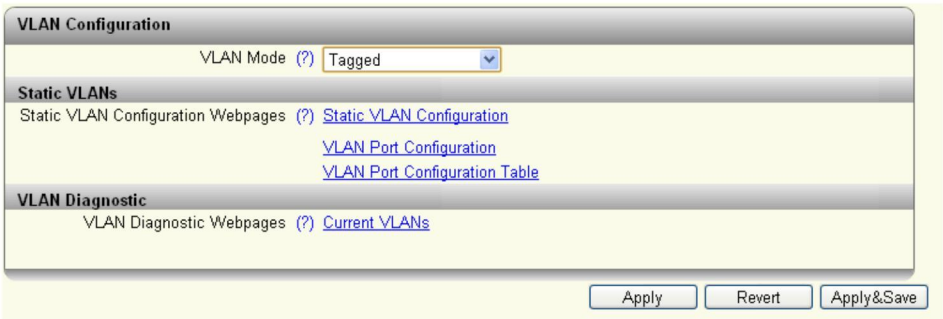


Figure 9-1 “VLAN Configuration” web page

VLAN Mode:

- Transparent: In “Transparent” mode, the switch processes the incoming data packets as described in the “Frame switching” section. Neither the structure nor the contents of the data packets are changed. The information about VLAN assignment from a tag that may be contained in the data packet is ignored.
- Tagged: In “Tagged” mode, the switch forwards the data packets based on the VLAN assignment.

Static VLANs

Static VLAN Configuration Webpages:

Clicking on the “Static VLAN Configuration” link takes you to the “Static VLAN Configuration” web page (see page 86). Up to eight (20xx/21xx version) or up to 32 (22xx/23xx/24xx/25xx version) static VLANs can be set up here.

Clicking on the “VLAN Port Configuration” link takes you to the “VLAN Port configuration” web page (see page 87).

Clicking on the “VLAN Port Configuration Table” link takes you to the VLAN port table (see page 87).

VLAN Diagnostic

VLAN Diagnostic Webpages:

Clicking on the “Current VLANs” link opens the “Current VLANs” web page as a pop-up (see page 87).

Pop-up: Static VLAN Configuration

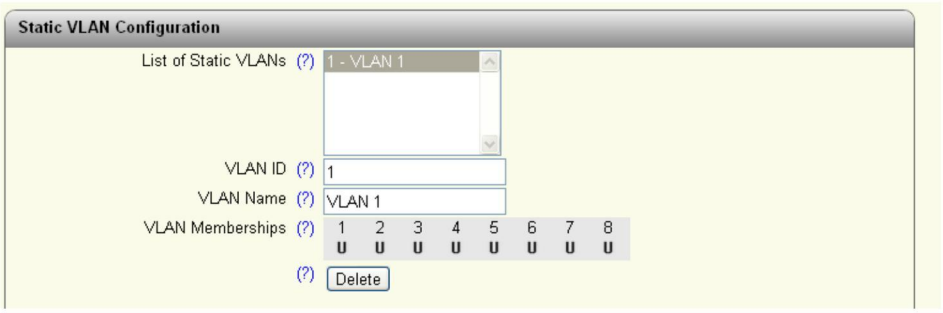


Figure 9-2 “Static VLAN Configuration” web page

List of Static VLANs:	All VLANs created up to this point are displayed here.
VLAN ID:	Set the VLAN ID you wish to assign to the new VLAN. The value must be between 2 and 4094.
VLAN Name:	Specify the VLAN name you wish to create.
VLAN Memberships:	Specify which ports are to be located in the VLAN. – T: Tagged port – U: Untagged port – -: Not a member of the VLAN

Use the “Delete” button to delete the VLAN selected in the list.

VLAN 1 cannot be deleted.

Pop-up: VLAN Port configuration

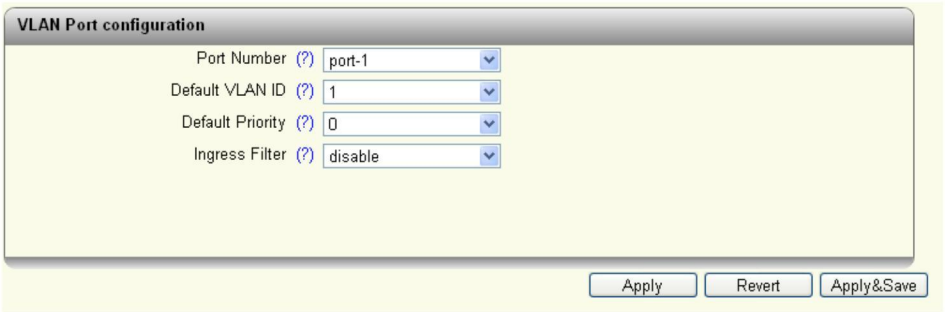


Figure 9-3 “VLAN Port configuration” web page

Port Number:	Select the port for which you want to change the VLAN settings.
Default VLAN ID:	Select the VLAN ID that is to be assigned to the port.
Default Priority:	Set the VLAN priority for the selected port.
Ingress Filter:	Specify whether the ingress filter should be activated.

Pop-up: VLAN Port Configuration Table

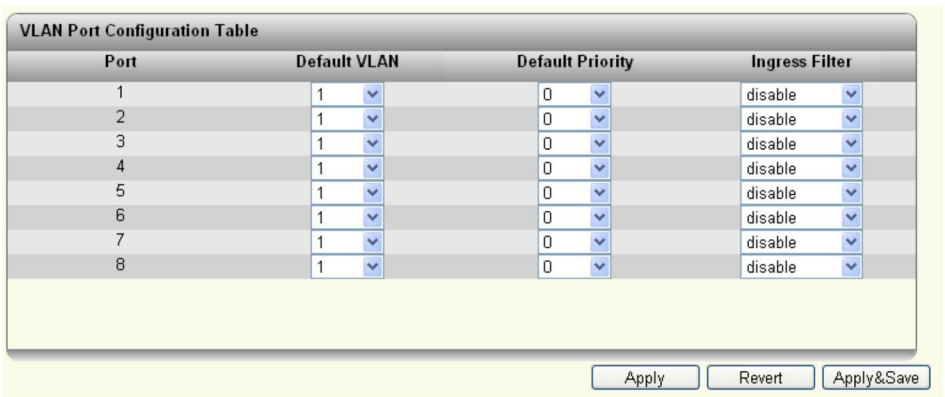


Figure 9-4 “VLAN Port Configuration Table” web page

Pop-up: Current VLANs

This page lists the current VLANs and displays the ports for each VLAN, which are either “Tagged” or “Untagged”.

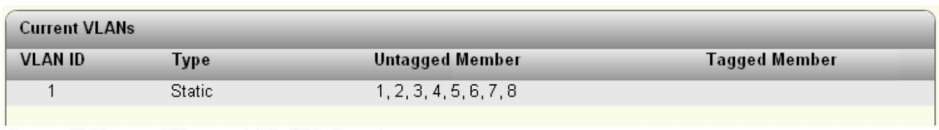


Figure 9-5 “Current VLANs” web page

10 Operation as a PROFINET device

In PC Worx version 5.00.26 or later, the switch is supported as a PROFINET device. The PROFINET controller can therefore support the startup of the switch within a PROFINET application. This includes the assignment of the IP parameters, comparison of the target/actual configuration, and archiving of the alarms sent by the switch. In the event that a device is replaced, the controller recognizes the replacement device and starts it up automatically. As a PROFINET device, the switch provides, e.g., the link states for the control program as process data items.

10.1 Preparing the switch for PROFINET operating mode

In the delivery state, the standard versions of the FL SWITCH 22xx/23xx/24xx/25xx and FL NAT 22xx/23xx are in “Universal mode” and must be set to “PROFINET mode” once.

Two mechanisms are available for switching the mode:

– After startup and IP address assignment, the operating mode/automation profile can be changed on the “Quick Setup” page in web-based management (see “Quick Setup” on page 35).
– By using Smart mode (see “Using Smart mode” on page 9).

When “PROFINET mode” is activated, the following presets are applied for operation:

– The Link Layer Discovery Protocol (LLDP) is enabled with the following configuration specifications for PROFINET components:
  a) The Discovery and Configuration Protocol (DCP) is activated as the mechanism for assigning IP parameters.
  b) The MRP protocol is not activated.

Additionally, the configuration is stored automatically and the device is restarted when changing to “PROFINET mode”.

The switch then starts up in “PROFINET mode” for the first time, and waits for a name and PROFINET IP address to be assigned (see “Device naming” on page 97 and “Operating in the PROFINET environment” on page 97).

If the switch is set from “PROFINET mode” back to “Universal mode”, the following settings are made:

– LLDP remains active with the delivery state values.
– IP address assignment is set to BootP.
– The station name for the switch does not change. If no station name has been specified, the device type is entered.

It is recommended that you save the new configuration after changing the operating mode. Please note that some configuration changes only take effect after a restart.

10.2 Switch as a PROFINET device

10.2.1 Configuration in the engineering tool

10.2.1.1 Specifying the bus configuration

The switch can be operated as a PROFINET device if it is integrated under a controller in the bus configuration in the engineering tool. A GSD file and an FDCML file for integration can be downloaded at phoenixcontact.net/products.

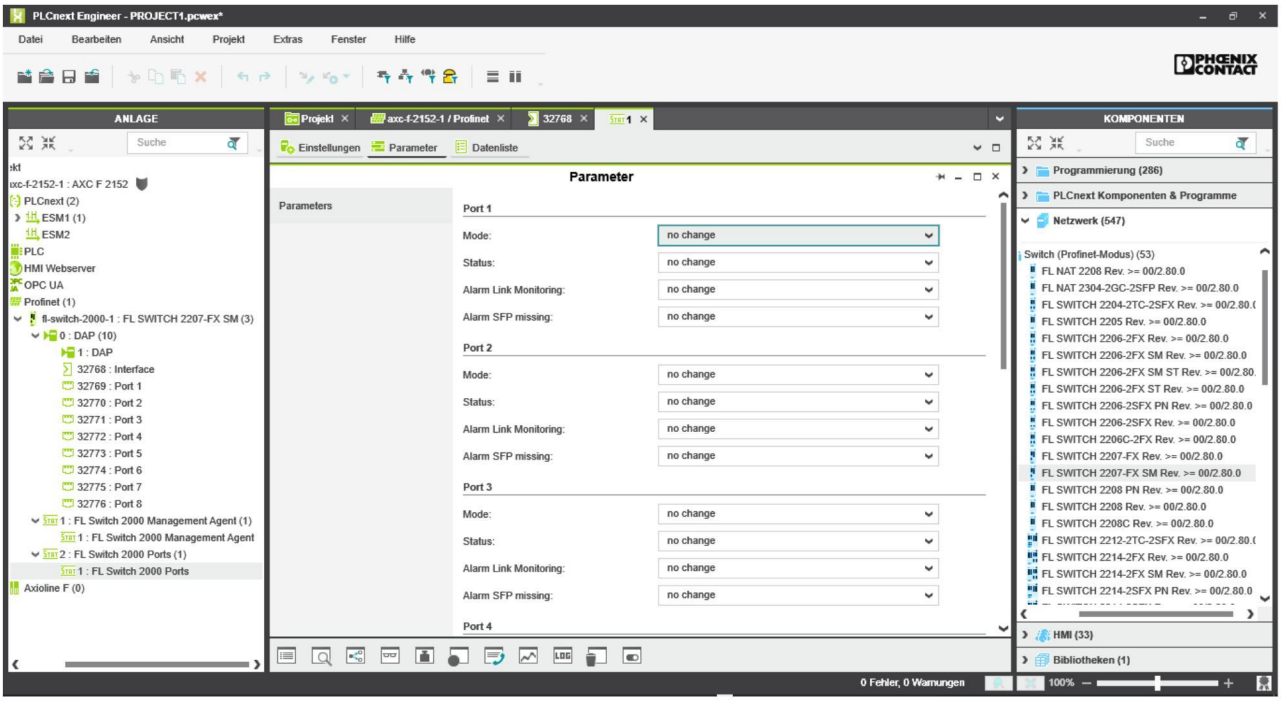


Figure 10-1 Integrating the devices in the engineering tool

If the switch is not listed in the device catalog, the device description provided by Phoenix Contact needs to be imported. The latest device description can be downloaded at phoenixcontact.net/products.

If the device description is available in the device catalog, the following options are available for bus configuration:

– Manual: The components are transferred to the bus configuration from the device catalog using drag and drop.
– Automatic: The devices are entered via the “Read PROFINET” function, which means that they can be accessed in the network via DCP (Discovery and Configuration Protocol). The devices must be supplied with voltage and “PROFINET mode” must be activated.

10.2.2 Configuring the switch as a PROFINET device

Once all the switches have been added to the bus configuration, you need to make the following settings for the individual switches via the “Detail View” tab (device details):

– Check the PROFINET device name. If necessary, change it.
– Check the IP address and subnet mask. Change both, if necessary.
– The update time for inputs should be set to “512 ms” (default).
– The update time for outputs should be set to “512 ms” (default).
– The monitoring time should be set to “2000 ms” (default).

After that, you can create and use the PROFINET variables in the control program. In addition to the “PNIO_DATA_STATE” standard variable, the switch provides the link status for each port as a process data byte.

If the “PNIO_DATA_VALID” bit for the “PNIO_DATA_STATE” variable declares the switch process data as valid, the process data item for a port can have the following values (see “Other cyclic process data” on page 99):

Value = 1: Active link

Value = 2: Link available, but the peer cannot establish the link (for FX ports only – far end fault detection)

Process data can only be accessed if the parameterized target configuration matched the actual configuration on device startup.

10.2.3 Configuration via the engineering tool

The switch can be configured via the engineering tool (PC Worx) using the universal parameter editor (UPE).

10.2.3.1 Structure of the process data

The tables below provide an overview of the information contained in the various slots.

Table 10-1 Slot 1/1 inputs

Byte	PN information	Table
1,2	Control word	Table 10-10
4	Link states of ports 1 - 8	Table 10-11
5	Link states of ports 9 - 16	
6	Link states of ports 17 - 24	
7	Diagnostics	Table 10-12

Table 10-2 Slot 1/1 outputs

Byte	PN information	Table
1,2	Status word	Table 10-10

Table 10-3 Slot 2/1 inputs

Byte	PN information	Table
1	Port 1	Table 10-13
2	Port 2	
3	Port 3	
...	...	
16	Port 16	

10.2.3.2 PN records (acyclic)

Table 10-4 Record index 0x0PP (PP - port number) – Slot2 Subslot1

Byte No.	Item	Data type	Permission	Default	Valid options
0	Block version	Byte	Read-only	0	0 - indicates this data set
1	Port mode	Byte	Read/write	0	0 - no changes 1 - auto negotiation 2 - 10 Mbps HD 3 - 10 Mbps FD 4 - 100 Mbps HD 5 - 100 Mbps FD 20 - auto negotiation 10/100 only 21 - fast startup
2	Port enable status	Byte	Read/write	0	0 - no changes 1 - disable 2 - enable
3	Alarm link monitoring	Byte	Read/write	0	0 - no changes 1 - disable 2 - enable
4	Reserved				
5	Alarm SFP missing	Byte	Read/write	0	0 - no changes 1 - disable 2 - enable

Table 10-5 Record index 0x1PP (PP - port number) – Slot2 Subslot1

Byte No.	Item	Data type	Permission	Default	Valid options
0	Block version	Byte	Read-only	0	0 - indicates this data set
1	Port speed	Byte	Read-only	0	0 - not connected 1 - 10 Mbps 2 - 100 Mbps 3 - 1 Gbps port duplex
2	Port duplex	Byte	Read-only	0	0 - unknown 1 - full duplex 2 - half duplex
3	Port utilization RX	Byte	Read-only	0	In %
4	Port utilization TX	Byte	Read-only	0	In %
5	Max. utilization RX	Byte	Read-only	0	In %
6 - 9	Padding			0	
10 - 11	Fiber transceiver RX power	Int16	Read-only	0	Value in 0.1 dBm
12 - 13	Fiber transceiver TX power	Int16	Read-only	0	Value in 0.1 dBm
16	RX unicasts packet count	Uint32	Read-only	0	
20	RX broadcasts packet count	Uint32	Read-only	0	
24	RX multicasts packet count	Uint32	Read-only	0	
28	Fragment error count	Uint32	Read-only	0	
32	Undersized packet count	Uint32	Read-only	0	
36	Oversized packet count	Uint32	Read-only	0	
40	CRC error count	Uint32	Read-only	0	

Table 10-6 Record index 1 – Slot1 Subslot1

Byte No.	Item	Data type	Permission	Default	Valid options
0	Block version	Byte	Read-only	0	0 - indicates this data set
1	Alarm power supply	Byte	Read/write	0	0 - no changes 1 - disable 2 - enable
2	Alarm module remove	Byte	Read/write	0	0 - no changes 1 - disable 2 - enable
3	Alarm MRP ring failure	Byte	Read/write	0	0 - no changes 1 - disable 2 - enable

Table 10-6 Record index 1 – Slot1 Subslot1 [...]

Byte No.	Item	Data type	Permission	Default	Valid options
4	PlugMem missing	Byte	Read/write	0	0 - no changes 1 - disable 2 - enable
5 - 9	Padding				
10	RSTP mode	Byte	Read/write	0	0 - no changes 1 - RSTP 2 - RSTP/FRD 3 - RSTP/LTS 4 - RSTP/LTS/FRD
11	RSTP priority	Byte	Read/write	16	0 ... 15 - priority value as multiple of 4K 16 - no changes
12	Web server	Byte	Read/write	0	0 - no changes 1 - disable 2 - HTTP 3 - HTTPS
13	SNMP agent	Byte	Read/write	0	0 - no changes 1 - disable 2 - SNMPv2 3 - SNMPv3
14	CLI service	Byte	Read/write	0	0 - no changes 1 - disable 2 - Telnet 3 - SSH
15	CLI network scripting	Byte	Read/write	0	0 - no changes 1 - disable 2 - enable
16	Alarm output: Power supply	Byte	Read/write	0	0 - no changes 1 - disable 2 - enable
17	Alarm output: Link monitoring	Byte	Read/write	0	0 - no changes 1 - disable 2 - enable
18	Alarm output: MRP	Byte	Read/write	0	0 - no changes 1 - disable 2 - enable
19	Alarm output: Pluggable memory missing	Byte	Read/write	0	0 - no changes 1 - disable 2 - enable
20 - 31	Padding				
32 - 95	Current admin password (valid access used when setting new password)	Char array	Write	0	Empty string if not used
96 - 159	New password to configure	Byte	Read/write	0	Empty string if not used

Table 10-6 Record index 1 – Slot1 Subslot1 [...]

Byte No.	Item	Data type	Permission	Default	Valid options
160	SNTP mode	Byte	Read/write	0	0 - no changes 1 - disable 2 - unicast mode 3 - broadcast mode
161	SNTP UTC offset	Byte	Read/write	0	0 - no changes Offset values 1 - 25 representing offset from -12h to +12h
162	SNTP server IP address	Char array	Read/write	0	Empty string - no changes IP address in dotted string notation, e.g., 192.168.0.1
178	SNTP backup IP address	Char array	Read/write	0	Empty string - no changes IP address in dotted string notation, e.g., 192.168.0.1
194	DNS server IP address	Char array	Read/write	0	Same as above
210	Second DNS server IP address	Char array	Read/write	0	Same as above

Table 10-7 Record index 2 – Slot1 Subslot1

Byte No.	Item	Data type	Permission	Default	Valid options
0	Block version	Byte	Read-only	0	0 - indicates this data set
1	Pluggable memory status	Byte	Read-only	0	0 - unknown 1 - present valid 2 - present invalid 3 - not present
2	Reserved				
3	Power supply	Byte	Read-only	0	Bit mask of valid power source

Table 10-8 Record index 3 – Slot1 Subslot1

Byte No.	Item	Data type	Permission	Default	Valid options
0	Block version	Byte	Read/write	0	0 - indicates this data set
1	Clear packet statistics	Byte	Read/write	0	0 - do nothing 255 - clear statistics of all ports Any other - select port number to clear

10.2.3.3 PDEV standard records

- Port mode
  - Status of PDEV port
- Link state
  - Read/enable alarm device properties/status of PDEV port
- Neighbor
  - Read/enable alarm by setting expected neighboring device properties/status of PDEV port
- MRP role
  - Read/write device properties/status of PDEV interface
- MRP ports
  - Read/write device properties/status of PDEV interface
- MRP ring state
  - Read/enable alarm device properties/status of PDEV interface
- Fiber optic type
  - Read/write device properties/status of PDEV port
- Port statistics counter
  - Read statistics counter of PDEV port

Table 10-9 Standard record information

Item	Identifier	Elements	Step 7 dialog window
PDPortDataReal	0x802A	Getting media type, mau type, and neighborhood information from the device	Device status of PDEV port subslot (X1 py)
PDPortDataAdjust	0x802F	Setting mau type of this port (auto neg., 10/100, HD/FD)	Device properties of PDEV port subslot (X1 py)
PDPortDataCheck	0x802B	Enable alarm for data transmission impossible and remote mismatch by specifying expected mau type, link state, and neighbor	Device properties of PDEV port subslot (X1 py)
PDInterfaceMrpDataReal	0x8050	Get current MRP role (client, manager) and ring state from the device	Device status of PDEV interface (X1)
PDInterfaceMrpDataAdjust	0x8052	Set MRP role	Device properties of PDEV interface subslot (X1)
PDInterfaceMrpDataCheck	0x8051	Enable alarm for MRP mismatch	Device properties of PDEV interface subslot (X1)
PDPortMrpDataReal	0x8054	Get MRP port state	Device properties of PDEV interface subslot (X1)
PDPortMrpDataAdjust	0x8053	Set MRP ports	Device properties of PDEV interface subslot (X1)
PDPortFODataReal	0x8060	Get adjusted fiber optic type and fiber optic cable type as well as the current power budget	Device status of PDEV interface subslot (X1 py)

Table 10-9 Standard record information [...]

Item	Identifier	Elements	Step 7 dialog window
PDPortFODataAdjust	0x8062	Set fiber optic type and fiber optic cable type (will be saved together with the system configuration)	Device properties of PDEV port subslot (X1 py)
PDPortFODataCheck	0x8061	Enable alarm for fiber optic mismatch	Device properties of PDEV port subslot (X1 py)
PDPortStatistic	0x8072	Statistics counter of the port corresponding to IF MIB: ifInOctets, ifOutOctets, ifInDiscards, ifOutDiscards, ifInErrors, ifOutErrors	Not available yet

10.2.3.4 I&M record data

- I&M0
  - Vendor ID, device order ID and serial number, HW and SW revision, device status of the DAP module (slot 0) / 0xAFF0
- I&M1
  - Contains location and function description, device identification / 0xAFF1
- I&M2
  - Contains installation date, device identification / 0xAFF2
- I&M3
  - Contains description text, device identification / 0xAFF3
- I&M4
  - Contains signature, device identification / 0xAFF4

10.2.4 Device naming

In order to start up a switch in “PROFINET” operating mode, each switch must be assigned a name once, i.e., each PROFINET device is assigned a unique device name.

A device search (“Read PROFINET” function in PC Worx) is performed via the engineering tool, where all the devices that can be accessed in the network are listed. After identifying unknown devices via the specified MAC address or the “flashing” function, the device name configured in the engineering tool is saved permanently on the switch using the “Assign Name” function.

10.2.5 Operating in the PROFINET environment

A switch that has already been assigned a name starts in “PROFINET” operating mode without an IP address and waits for an IP configuration to be assigned. Once the project has been translated and downloaded to the controller, the controller implements startup and configuration.

As soon as a communication relationship has been successfully established between the switch and the controller, the switch starts its management interfaces. The switch indicates that the PROFINET connection has been established correctly by means of an entry in the event table.

10.3 PROFINET alarms

The FL SWITCH 22xx/23xx/24xx/25xx versions are able to send the following alarms (the alarms are deactivated upon device start):

- Power supply management agent
  - (Slot 1) appears when redundant power supply is lost
- MRP ring failure management agent
  - (Slot 1) appears when MRP manager detects ring failure, MRP clients do not support this alarm, PlugMem missing
- PlugMem missing
  - (Slot 1) appears when pluggable memory is missing
- Link monitoring
  - (SFP, interface or fixed) appears when link is down on that port
- SFP module missing

Standard PROFINET alarms

- Data transmission impossible
  - Appears when link is down or port mode does not match the specified values (default: disabled)
- Remote mismatch
  - Appears when neighbor information does not match the specified values (default: disabled)
- Media redundancy mismatch
  - Appears when MRP manager detects ring failures (default: disabled)
- Fiber optic mismatch
  - Appears when system reserve is reached or consumed on POF SCRJ ports (default: disabled)

10.3.1 Alarms in WBM

In “PROFINET” operating mode, the “PROFINET Alarms” web page appears in the navigation bar under “Switch Station / Diagnostics”. All the alarms supported by the PN device can be activated there. The PN devices transmit the PROFINET alarms to the controller.

The settings made for the PROFINET alarms can be saved with the configuration.

The controller can transmit a differing alarm configuration to the switch and thereby overwrite the configuration settings.

10.4 Process data communication

10.4.1 Control word/status word

The control word is a special process data item which is used to make settings that cannot be implemented using standard process data.

A command consisting of two bytes can be written to the control word of the management agent. The device responds with the same command in the status word. Byte 0 specifies the action and the new status; byte 1 specifies the port number. If a command is to apply to all the ports, value 0xFF can be sent instead of the port number. A command should only be sent once, but never in a process data communication cycle.

The following alarms and settings can be activated or deactivated via the control word:

Table 10-10 Alarms and settings

Action	Status	Byte 0	Byte 1
Alarm link monitoring	Enable	0x01	Portnum or 0xFF
	Disable	0x02	Portnum or 0xFF
Alarm power supply	Enable	0x05	0x00
	Disable	0x06	0x00
Alarm MRP ring failure	Enable	0x09	0x00
	Disable	0x0a	0x00
PlugMem missing	Enable	0x0b	0x00
	Disable	0x0c	0x00
SFP missing	Enable	0x0d	Portnum or 0xFF
	Disable	0x0e	Portnum or 0xFF
Reset packet error indicator	Reset	0x1F	0x00
Link enable status	Enable	0x20	Portnum
	Disable	0x21	Portnum

10.4.2 Other cyclic process data

- Diagnostic data
  - Link states of all ports (up to 4 bytes)

Table 10-11 Diagnostic data/link states

Bit	7	6	5	4	3	2	1	0
Port	8/16/24	7/15/23	6/14/22	5/13/21	4/12/20	3/11/19	2/10/18	1/9/17

- MRP ring failure
- Alarm contact

Table 10-12 Diagnostic data/link states

Bit	7	6	5	4	3	2	1	0
Port	MRP status 0 - no diagnostics 1 - MRP ring failure			Packet error indicator 0 - no error 1 - error counter increased				Alarm contact 1 0 - closed 1 - open

- Port information, one byte per port (ports constitute individual slot 2, subslot 1)
  - Blocking state
  - Port enable status
  - Far end fault status
  - Link status
  - SFP module available

Table 10-13 Diagnostic data/meaning

Bit	7	6	5	4	3	2	1	0
Port	Blocking mode 0 - forwarding 1 - blocking				SFP modules 0 - none 1 - available	Port enable status 0 - enabled 1 - disabled	Far end fault 0 - no fault 1 - FEFI	Link status 0 - link down 1 - link up

- Additional bit for changing an error counter. The bit should be acknowledged before it is reset to “0” in order to prevent the loss of information.

10.5 PDEV function description

The PDEV function provides an extended range of functions for switches in PROFINET mode. This includes displaying of neighbor and topology information in the engineering tool. This information is determined using the Link Layer Discovery Protocol (LLDP) and can be used, for example, to compare the target and actual network.

In addition, the PDEV function is used to display the transmitted information via the respective Ethernet ports.

The PDEV function uses two submodules:

- Interface submodule with port number 0x8X00 (X: from 0 to F)
- Port submodule with port number 0x8IXX (I: interface ID; X: port number)

These submodules are represented in the Step 7 engineering tool. PROFINET communication enables information about the port speed, duplex mode, and the link status to be read. An engineering tool reads the neighbor and topology information via SNMP, which it then displays.

11 Layer 3 functions – routing and NAT

The NAT switches of the FL NAT 2000 series provide a flexible port constellation and can thus be adapted to practically any application. Once the necessary interfaces have been created, the relevant ports can be defined, and the NAT mechanism or routing function can be configured.

In a NAT application, all of the LAN devices that should be accessible from the WAN require a gateway address.

An FL NAT 2000 switch should not simultaneously operate in NAT mode and as an MRP manager, because temporary connection interruptions can occur as a result of switch-over or topology changes. This particularly applies to applications with real-time data communication (e.g., PROFINET).

11.1 Factory default

To set the device to the factory default configuration, see “Using Smart mode” on page 9. The following NAT configuration is preset in the default state:

– Routing active
– LAN1 created (IP addressing: BootP, ports: 2 to 8)
– LAN2 created (IP addressing: DHCP, ports: 1)

11.2 Creating interfaces

New interfaces can be created in WBM under the NAT item.

No NAT mode should be set on LAN1 if possible, as this interface provides additional LAN services (e.g., PROFINET and DHCP server).

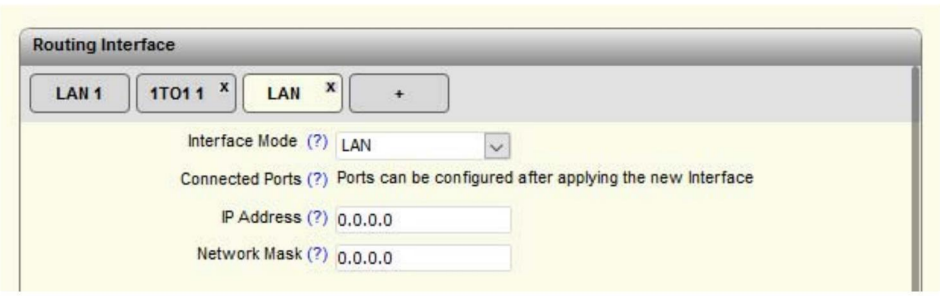


Figure 11-1 “Routing Interface / LAN” web page

Here, the “+” character is used to create a new routing interface. The interface mode describes which type of interface is being created.

The following options are available here:

Interface Mode:

- LAN:
  The LAN type represents a simple routing interface.
  It is used if the NAT switch is to be used in a simple router mode or as an interface for a LAN area that is to be translated to another network.
- 1 to 1 NAT:
  This setting creates a WAN interface that uses the 1:1 NAT mechanism to translate IP addresses from a LAN area to the WAN.
- Virtual NAT:
  This setting creates a WAN interface that uses the virtual NAT mechanism to translate IP addresses from a LAN area to the WAN.
- IP Masquerading:
  This setting creates a WAN interface that uses the IP masquerading mechanism to translate IP addresses from a LAN area to the WAN.

IP Address: The IP address of the new interface is entered here.

Network Mask: The subnet mask of the new interface is entered here.

Following confirmation of the previous parameters, the physical ports can be assigned to the created interface:

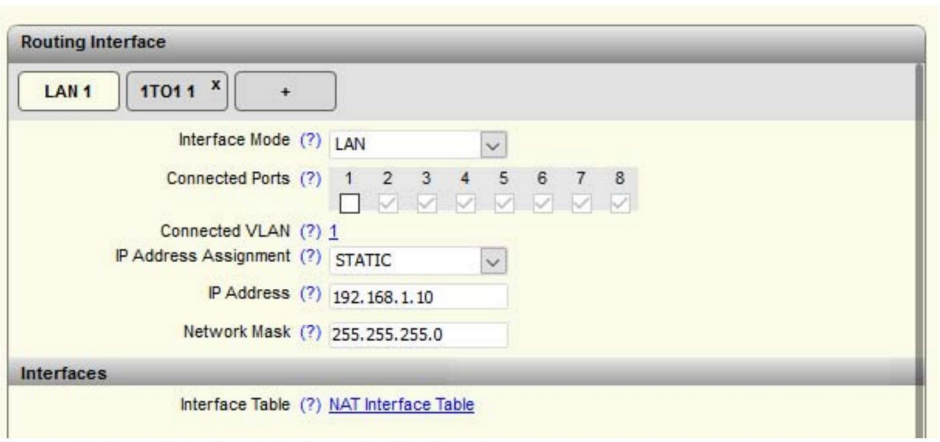
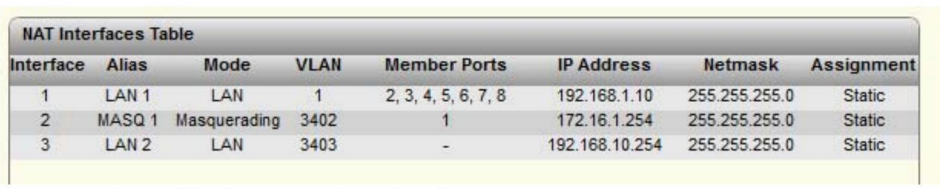


Figure 11-2 “Routing Interface / LAN 1” web page

Interface Table: Clicking on the “NAT Interface Table” link takes you to an overview table of all the configured interfaces.



NAT Interfaces Table

Interface	Alias	Mode	VLAN	Member Ports	IP Address	Netmask	Assignment
1	LAN 1	LAN	1	2, 3, 4, 5, 6, 7, 8	192.168.1.10	255.255.255.0	Static
2	MASQ 1	Masquerading	3402	1	172.16.1.254	255.255.255.0	Static
3	LAN 2	LAN	3403	-	192.168.10.254	255.255.255.0	Static

Figure 11-3 “NAT Interfaces Table” web page

11.3 Static routing

Static routing enables communication between two or more different subnets. The devices of the NAT 2000 series automatically route between the created LAN interfaces. You can create static routes via a link on the “Routing” page in the web interface:

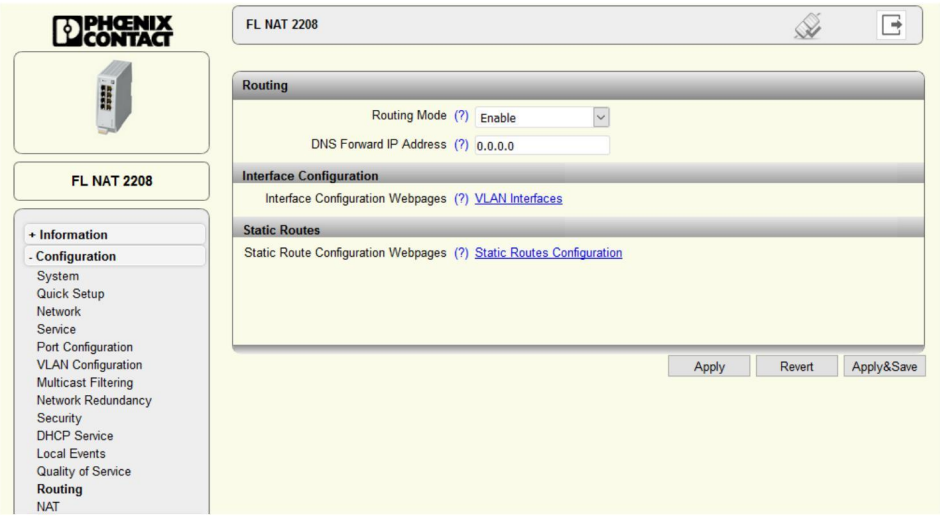


Figure 11-4 “Routing” web page

The static routes can be configured by clicking on the “Static Routes Configuration” link:

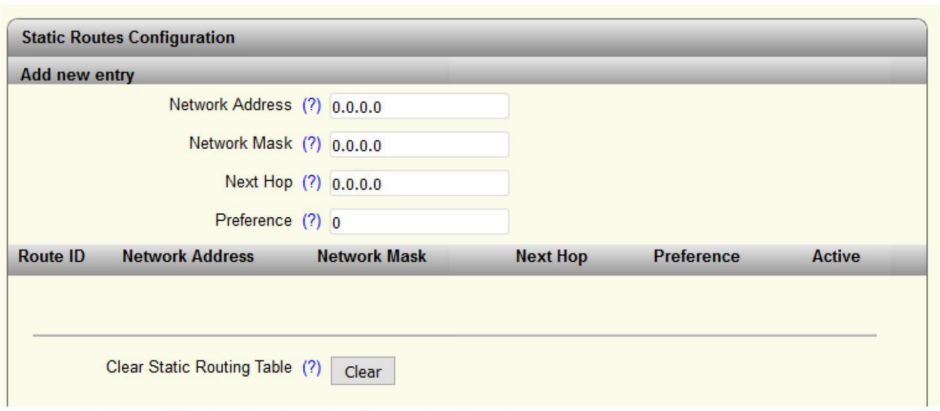


Figure 11-5 “Static Routes Configuration” web page

Network Address:	IP address of the target network to which the static route refers.
Network Mask:	Subnet mask of the target network to which the static route refers.

Next Hop:	IP address of the next router on the way to the target network.
Preference:	Specifies the priority of the static route. The lower the value, the higher the priority. The exception is “0”, which is used if no priority should be applied.
Clear Static Routing Table:	Click on the “Clear” button to delete all the static routes.

For a default route, value 0.0.0.0 must be set for the network address and network mask.

11.4 Configuration of 1:1 NAT

With 1:1 NAT, each device in the LAN is assigned an IP address from the higher-level network (WAN). The device can then be addressed from the WAN via this assigned address.

Advantages:

– No route/gateway configuration necessary in the WAN
– Communication can be established from both the LAN and WAN
– Not restricted to dedicated protocols

Disadvantage:

– An IP address must be reserved in the WAN for each device that should be accessible in the LAN

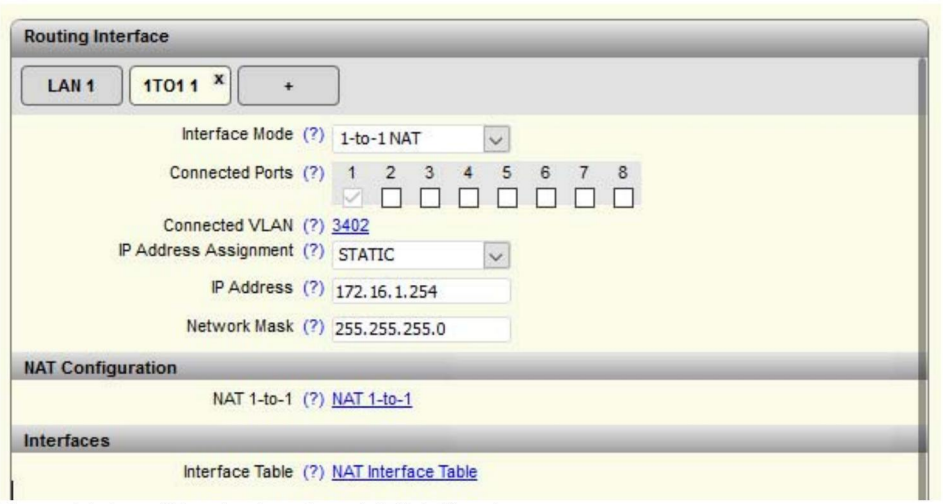


Figure 11-6 “Routing Interface / 1TO1 1” web page

Having created an interface with 1:1 NAT, you can configure the NAT rules via the “NAT 1-to-1” link:

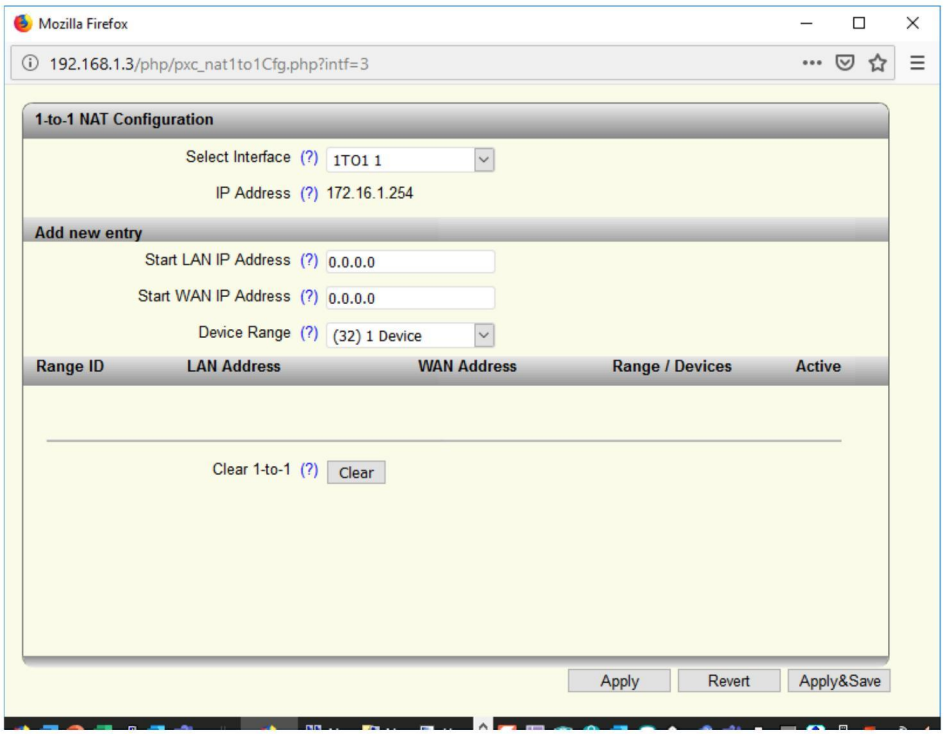


Figure 11-7 “1-to-1 NAT Configuration” web page

Select Interface	Select the correct interface from the list of all created 1:1 NAT interfaces.
Start LAN IP Address	Start IP address of the area that is to be translated.
Start WAN IP Address	Start IP address of the area that is to be translated to.
Device Range	Number of IP addresses that are to be translated.
Clear 1-to-1	Click on the “Clear” button to delete the complete table for the selected interface.

11.5 Configuration of virtual NAT

Virtual NAT

Virtual NAT combines 1:1 NAT with a virtual router level. In this router level, the address is mapped from the LAN and is then transferred to the WAN from the virtual intermediate level as with standard routing.

Advantage:

– Only one IP address is required from the WAN for the NAT interface itself

Disadvantage:

– In the WAN, the route to the (virtual) network must be indicated and the NAT WAN interface entered as the next hop or gateway address.

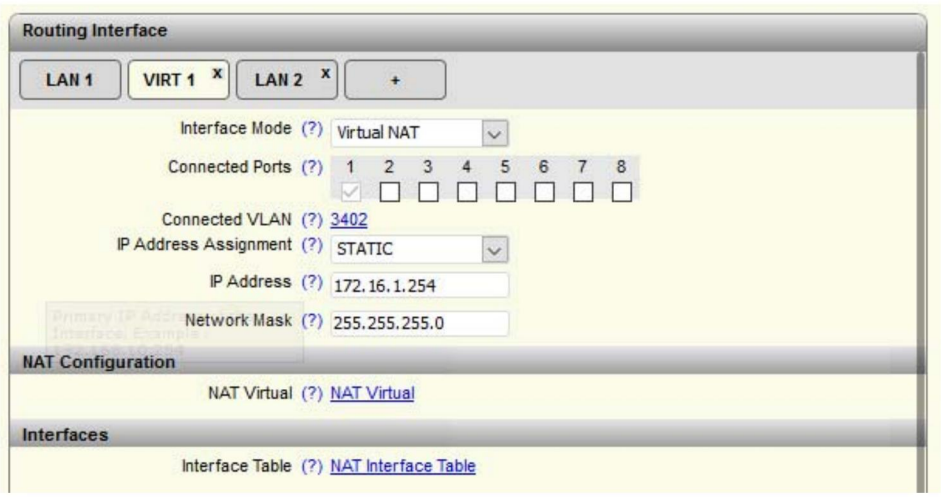


Figure 11-8 “Routing Interface / VIRT 1” web page

Having created an interface using virtual NAT, you can configure the details via the “NAT Virtual” link:

Figure 11-9 “Virtual NAT Configuration” web page

Select Interface:	Select the correct interface from the list of all created 1:1 NAT interfaces.
Virtual Network:	The IP address of the virtual network is entered here.
LAN Start IP:	Start IP address of the area that is to be translated to the virtual network.
Device Range:	Number of IP addresses that are to be translated.

11.6 Configuration of IP masquerading

The NAT device acts as a proxy, so that all of the LAN devices communicate externally using the IP address of the NAT/WAN port. Various TCP/UDP ports are used to differentiate between the different LAN devices.

Advantages:

– No additional WAN addresses are required aside from the address for the NAT device itself
– No route/gateway configuration necessary in the WAN

Disadvantage:

– WAN devices can only communicate with LAN devices via port forwarding

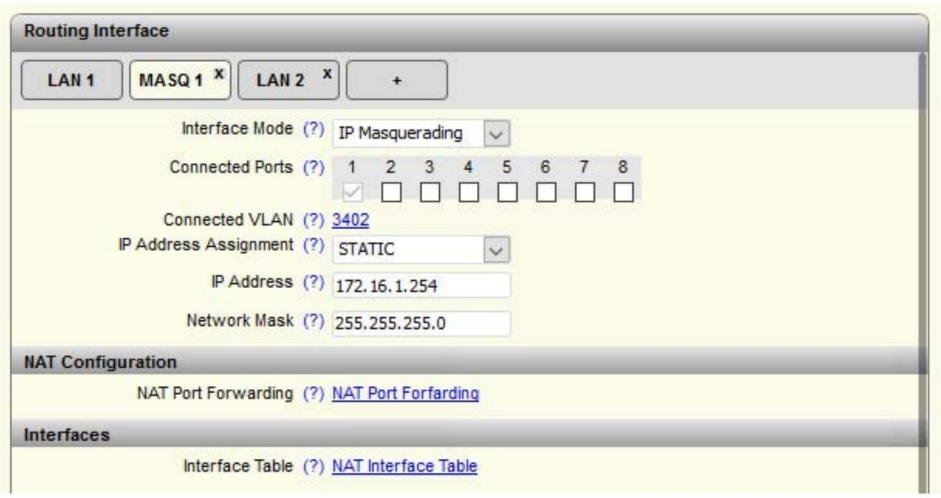


Figure 11-10 “Routing Interface / MASQ 1” web page

Having created an interface with IP masquerading, you can configure the details via the “NAT Port Forwarding” link so that port forwarding can be used. Standard IP masquerading does not require any detailed configuration and is automatically active following creation of the interface. Thus, all LAN areas are translated to this interface.

11.7 Configuration of port forwarding

Enables a specific service of a specific LAN device to be accessed from the WAN network. During this process, the WAN interface of the NAT device is addressed using a defined TCP/UDP port number so that it can be forwarded to the desired LAN device.

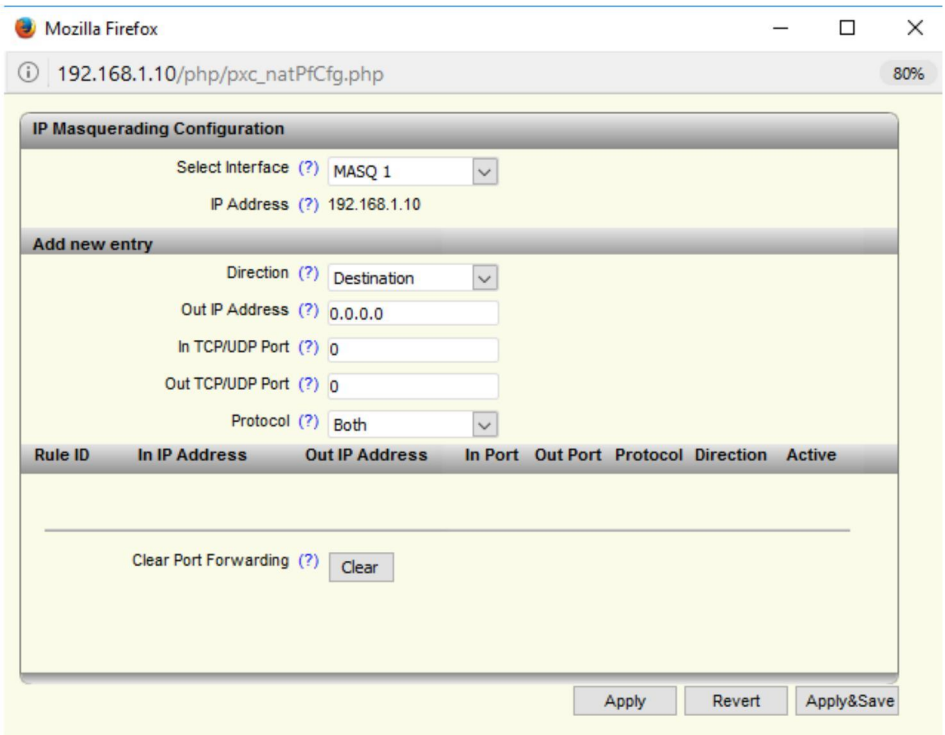


Figure 11-11 “IP Masquerading Configuration” web page

Select Interface:	Select the correct interface from the list of all created IP masquerading interfaces.
Direction	Select whether the WAN-to-LAN standard (destination) or LAN-to-WAN standard (source) should be applied. The configuration web page differs depending on the selected direction:
Clear Port Forwarding:	Click on the “Clear” button to delete the complete table for the selected interface.

Destination port forwarding:

Out IP Address:	Target address for outgoing packets.

In TCP/UDP Port:	Incoming TCP/UDP target port on the WAN side.
Out TCP/UDP Port:	Target port number with which the packet should be forwarded to the LAN (typical service port to be addressed, e.g., http (port 80)).
Protocol:	Select whether only UDP or TCP packets or both should be translated.

Source port forwarding:

Only necessary if protocols are being used that have a fixed port number as the specified source and they do not support dynamic port assignment.

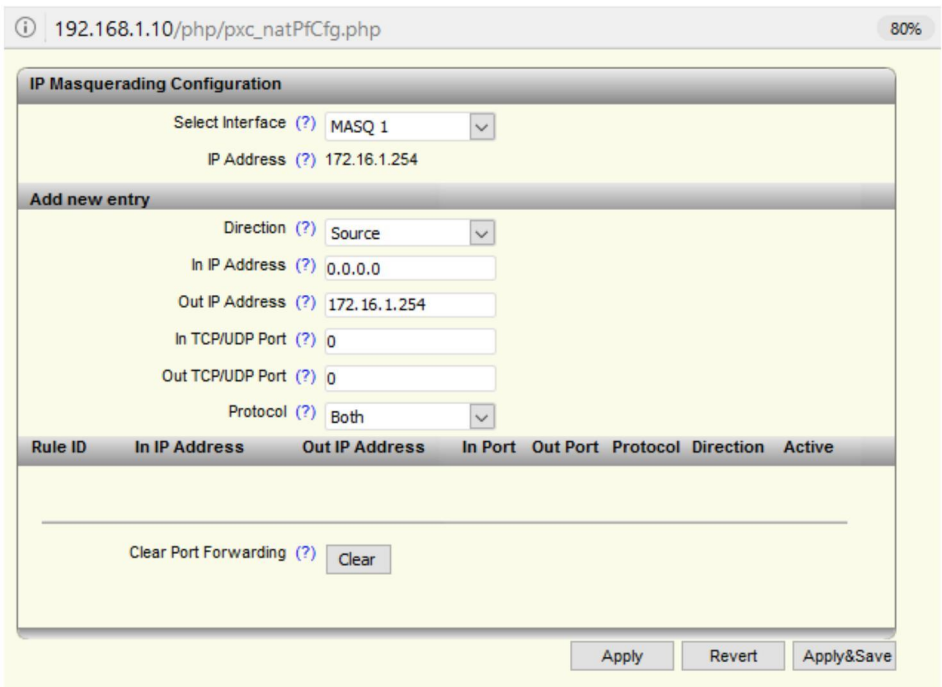


Figure 11-12 “IP Masquerading Configuration” web page

In IP Address:	LAN address of the sending device for which this standard applies.
Out IP Address:	Source IP address used for the WAN. This is usually the WAN interface address (preset).
In TCP/UDP Port:	Source port of the sending device for which this standard applies.
Out TCP/UDP Port:	Source port used for communication from the NAT router to the device in the WAN.
Protocol:	Select whether only UDP or TCP packets or both should be translated.

11.8 Application examples

To illustrate the configuration sequence, the following shows how a machine is connected to two higher-level WAN networks via 1:1 NAT. Five devices from the machine should be accessible from both higher-level networks: 192.168.10.2-192.168.10.6.

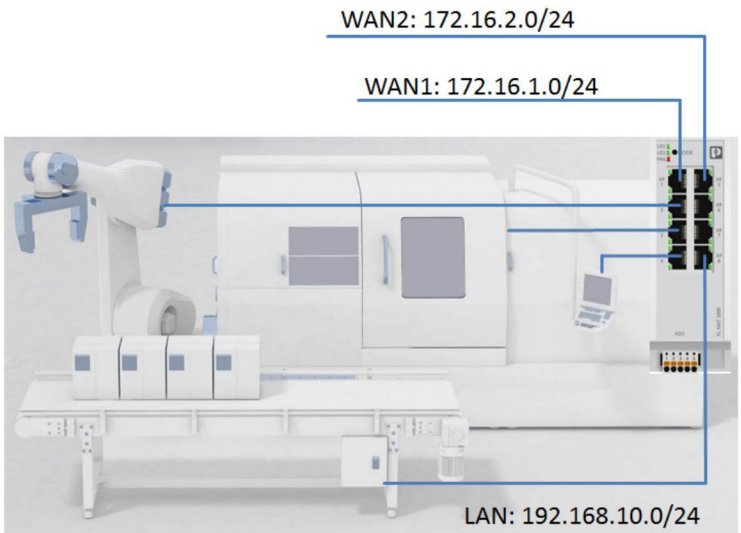


Figure 11-13 Typical connection of a machine

Step 1: Setting up the LAN interface

– Once an IP address has been assigned on the LAN side, it can be used to access the web interface via the LAN ports.
  In this example, the NAT switch on the LAN has IP address 192.168.10.254.
– The configuration options for the NAT function are available under the “NAT” menu item.
– Two LAN interfaces have already been created in default mode. LAN1 with ports 2 to 8, and LAN2 with port 1. LAN1 is configured as the internal LAN interface with ports 3 to 8. LAN port assignment is based on the WAN configuration.

Step 2: Setting up both WAN interfaces

Setting up the first WAN interface:

1. Select LAN2 and set it up as a 1:1 NAT interface via the drop-down menu
2. Set the WAN IP parameters
3. Confirm the settings with “Apply”

Setting up the second WAN interface:

1. Create another interface using the “+” button
2. Select 1:1 NAT and set the IP parameters
3. Confirm the settings with “Apply”
4. Use the check box to assign Port2 to the second WAN interface
   (The port is automatically deleted from LAN1)
5. Confirm the settings with “Apply”

Step 3: Configuring both NAT tables

– There is a link in the 1:1 NAT interfaces for configuring the 1:1 NAT tables. The configuration window is opened via this link.

  You must set the following parameters there:

  Parameters for WAN 1 (1TO1 1)

  – Start LAN IP Address: 192.168.10.8
  – Start WAN IP Address: 172.16.1.8
  – Device Range: 8 Devices

  Parameters for WAN2 (1TO1 2)

  – Start LAN IP Address: 192.168.10.8
  – Start WAN IP Address: 172.16.2.8
  – Device Range: 8 Devices

A Appendix for document lists

A 1 List of figures

Section 2

Section 4

Section 5

Section 7

Section 8

Section 9

Section 10

Section 11

A 2 List of tables

Section 2

Section 4

Section 7

Section 10

A 3 Index

Numerics

A

B

C

D

E

F

H

I

L

Please observe the following notes

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 general 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.

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:
phoenixcontact.com

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

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 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

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Phone: +49 5235 3-00
Fax: +49 5235 3-41200
E-mail: info@phoenixcontact.com
phoenixcontact.com

108998_en_01
Order No. —01

INSPIRING INNOVATIONS