
# FL SWITCH 2000

## User manual

Order No. —

INSPIRING INNOVATIONS

# User manual
# FL SWITCH 2000

2017-05-24

Designation: UM EN FL SWITCH 2000

Revision: 01

Order No.: —

This user manual is valid for:

| Designation | Order No. | Designation | Order No. |
|---|---|---|---|
| FL SWITCH 2005 | 2702323 | FL SWITCH 2206-2FX SM | 2702331 |
| FL SWITCH 2008 | 2702324 | FL SWITCH 2206-2FX ST | 2702332 |
| FL SWITCH 2105 | 2702665 | FL SWITCH 2206-2FX SM ST | 2702333 |
| FL SWITCH 2108 | 2702666 | FL SWITCH 2204-2TC-2SFX | 2702334 |
| FL SWITCH 2205 | 2702326 | FL SWITCH 2206-2SFX | 2702969 |
| FL SWITCH 2208 | 2702327 | FL SWITCH 2308 | 2702652 |
| FL SWITCH 2207-FX | 2702328 | FL SWITCH 2304-2GC-2SFP | 2702653 |
| FL SWITCH 2207-FX SM | 2702329 | FL SWITCH 2306-2SFP | 2702970 |
| FL SWITCH 2206-2FX | 2702330 | | |

# Please observe the following notes

### User group of this manual

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

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

### Explanation of symbols used and signal words

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

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

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

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

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

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

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

### How to contact us

**Internet**

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

### General terms and conditions of use for technical documentation

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

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

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



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

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

### Caution: Installation only by qualified personnel

Installation, startup and maintenance of the product may only be performed by qualified specialist staff who have been authorized for this by the system operator. An electrician is a person who, because of their training, experience and instruction, and knowledge of relevant standards, can assess any required operations and recognize any possible dangers.

Specialist staff must read and understand this documentation and comply with instructions.

Observe the national regulations in force for the operation, functional testing, repairs and maintenance of electronic devices.

# Table of contents

# 1 Factoryline SWITCH 2000 range

## 1.1 Properties and versions

The Managed Switches in the 2000 version are Ethernet Switches which are suitable for industrial use. They are available in the following versions:

– With five 10/100 Mbps RJ45 ports (FL SWITCH 2005)
– With eight 10/100 Mbps RJ45 ports (FL SWITCH 2008)

The Managed Switches in the 2100 version are Gigabit Ethernet Switches which are suitable for industrial use. They are available in the following versions:

– With five 10/100/1000 Mbps RJ45 ports (FL SWITCH 2105)
– With eight 10/100/1000 Mbps RJ45 ports (FL SWITCH 2108)

The Managed Switches in the 2200 version are Ethernet Switches which are suitable for industrial use. They are available in the following versions:

– With five 10/100 Mbps RJ45 ports (FL SWITCH 2205)
– With eight 10/100 Mbps RJ45 ports (FL SWITCH 2208)
– With seven 10/100 Mbps RJ45 ports and one FO port in SC format for multimode (FL SWITCH 2207-FX)
– With seven 10/100 Mbps RJ45 ports and one FO port in SC format for single mode (FL SWITCH 2207-FX-SM)
– With six 10/100 Mbps RJ45 ports and two FO ports in SC format for multimode (FL SWITCH 2206-2FX)
– With six 10/100 Mbps RJ45 ports and two FO ports in SC format for single mode (FL SWITCH 2206-2FX SM)
– With six 10/100 Mbps RJ45 ports and two FO ports in ST format for multimode (FL SWITCH 2206-2FX ST)
– With six 10/100 Mbps RJ45 ports and two FO ports in ST format for single mode (FL SWITCH 2206-2FX SM ST)
– With four 10/100 Mbps RJ45 ports, two Fast Ethernet combo ports, and two SFX ports (FL SWITCH 2204-2TC-2SFX)
– With six 10/100 Mbps RJ45 ports and two SFX ports (FL SWITCH 2206-2SFX)

The Managed Switches in the 2300 version are Gigabit Ethernet Switches which are suitable for industrial use. They are available in the following versions:

– With eight 10/100/1000 Mbps RJ45 ports (FL SWITCH 2308)
– With four 10/100/1000 Mbps RJ45 ports, two Gigabit combo ports, and two SFP ports (FL SWITCH 2304-2GC-2SFP)
– With six 10/100/1000 Mbps RJ45 ports and two SFP ports (FL SWITCH 2306-2SFP)

### 1.1.1 Dimensions of the FL SWITCH 2000

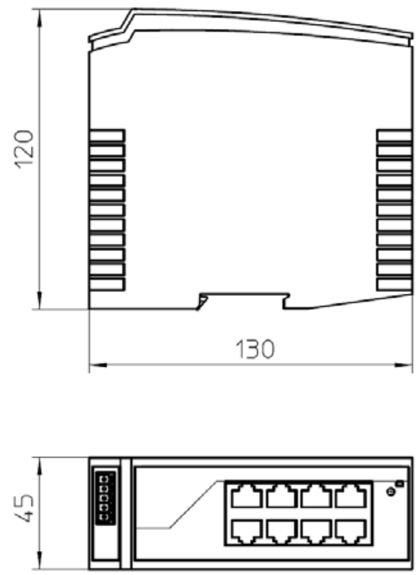



Figure 1-1 Dimensions of the FL SWITCH 2000

### 1.1.2 Elements of the devices

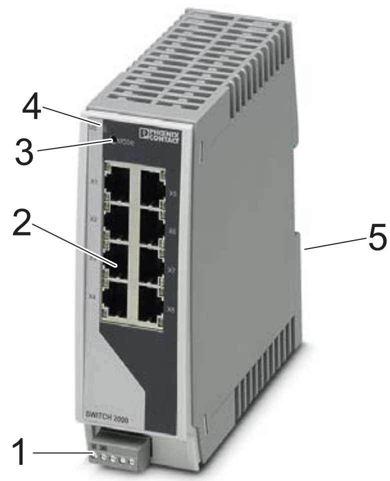



Figure 1-2 Elements of the devices

Table 1-1

| Number | Meaning |
|---|---|
| 1 | Connection for the supply voltage |
| 2 | RJ45 ports |
| 3 | Mode switch |
| 4 | Diagnostic and status indicators |
| 5 | Slot for optional SD card |

### 1.1.3 Description of the combo ports

Combo ports enable a high degree of flexibility when setting up networks. They consist of a corresponding RJ45 port (e.g., X3.1) and a corresponding SFP port (e.g., X3.2). Only one port of the pair can be used at a time. Each combo port can therefore be used as a copper or fiberglass port. Inserting an SFP module disables the corresponding RJ45 port. If a combo port is used as a fiberglass port, the Link LED of the corresponding RJ45 port lights up orange when there is an active connection.

The following FL SWITCH 2000 versions have combo ports:

– FL SWITCH 2204-2TC-2SFX (2 Fast-Ethernet combo ports for 100 Mbps SFP modules, ports 3 and 7)
– FL SWITCH 2304-2GC-2SFP (2 Gigabit combo ports for 100 Mbps and 1000 Mbps SFP modules, ports 3 and 7)

### 1.1.4 Status and diagnostic indicators

Please note that the meaning of the LEDs differs in Smart mode (see “Using Smart mode” on page 17).

| Des. | Color | Status | Meaning |
|---|---|---|---|
| **US1** | Green | On | Supply voltage 1 within the tolerance range |
| | | Off | Supply voltage 1 too low |
| **US2** (for 2200/2300 version only) | Green | On | Supply voltage 2 within the tolerance range |
| | | Off | Supply voltage 2 too low |
| **FAIL** (for 2200/2300 version only) | Red | On | Digital alarm output floated, i.e., an error is present |
| | | Off | Digital alarm output connected to ground potential (ground), i.e., an error is not present |
| **LNK/ACT** (at port top) | Green | On | Link active |
| | | Flashing | Data transmission |
| | | Off | Link not active |
| **SPD** (at port bottom) | Green/ orange | On | Green: 100 Mbps<br>Orange (for 2100/2300 version only): 1000 Mbps |
| | | Off | 10 Mbps if Link LED is active |

# 2 Mounting and installation

## 2.1 Mounting and removing the devices

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

**Mounting:**

- Place the module onto the DIN rail from above (A1). The upper holding keyway of the module must be hooked onto the top edge of the DIN rail. Push the module from the front towards the mounting surface (A2).

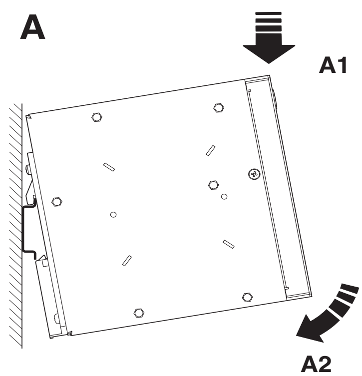



Figure 2-1 Snapping the device onto the DIN rail

- Once the module has been snapped on properly, check that it is fixed securely on the DIN rail.

**Removal:**

- Pull down the positive latch using a suitable tool (e.g., screwdriver). The positive latch remains snapped out. Then swivel the bottom of the device away from the DIN rail slightly (B1). Next, lift the device upwards away from the DIN rail (B2).

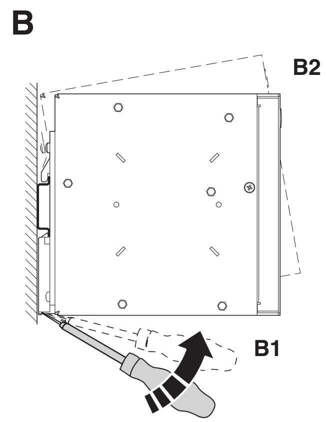



Figure 2-2 Removing the device

## 2.2 Installing the devices

### 2.2.1 Connecting the supply voltage

The device is operated using a 24 V DC voltage, which is applied via COMBICON. For devices in the 2200/2300 version, the voltage can also be supplied redundantly (see Figure 2-4).

> For devices in the 2200/2300 version: if redundant power supply monitoring is active (default setting), an error is indicated if only one voltage is applied. A bridge between US1 and US2 prevents this error message. It is possible to deactivate monitoring in web-based management or via SNMP.

**Operation with one power supply**

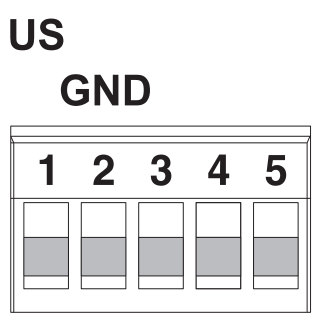



Figure 2-3 Operating the device with one power supply (example)

**Redundant operation with two power supplies**

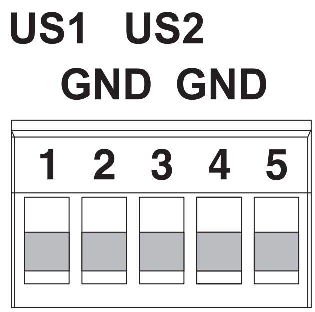



Figure 2-4 Redundant operation with two power supplies (example)

Please note that load distribution does not take place. The power supply unit with the higher voltage will supply the device on its own.

### 2.2.1.1 Connecting a relay to the digital alarm output

The digital alarm output is an open drain output. In normal mode, the output is connected to ground potential. If an error/alarm is present, the output is floated.

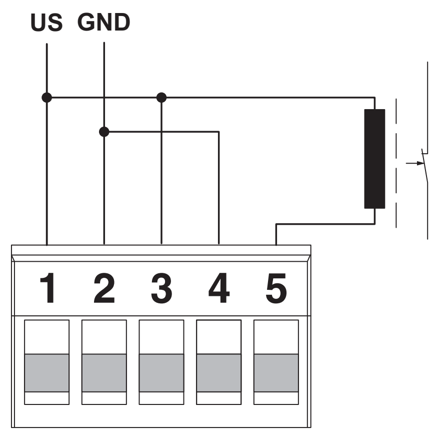



Figure 2-5 Connecting a relay to the digital alarm output

Please note that the relay must be suitable for the operating voltage. Use the RIF-0-RPT-24DC/21 (Order No. 2903370), for example.

### 2.2.2 Grounding ⏚

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

All Factoryline devices must be grounded so that any possible interference is shielded from the data telegram and discharged to ground potential. A conductor of at least 2.5 mm$^2$ must be used for grounding. Mount the module on a grounded DIN rail. The module is functional grounded by snapping it onto the DIN rail.

### 2.2.3 Assignment of the RJ45 Ethernet connectors

Please note that for operation with 1000 Mbps (Gigabit), cables with four twisted pairs (eight wires), which meet the requirements of CAT5e as a minimum, must be used.

Please note that only devices in the 2100/2300 version support Gigabit.

Table 2-1 Pin assignment of RJ45 connectors

| Pin number | 10Base-T/10 Mbps | 100Base-T/100 Mbps | 1000Base-T/1000 Mbps |
|---|---|---|---|
| 1 | TD+ (transmit) | TD+ (transmit) | BI_DA+ (bidirectional) |
| 2 | TD- (transmit) | TD- (transmit) | BI_DA- (bidirectional) |
| 3 | RD+ (receive) | RD+ (receive) | BI_DB+ (bidirectional) |
| 4 | - | - | BI_DC+ (bidirectional) |
| 5 | - | - | BI_DC- (bidirectional) |
| 6 | RD- (receive) | RD- (receive) | BI_DB- (bidirectional) |
| 7 | - | - | BI_DD+ (bidirectional) |
| 8 | - | - | BI_DD- (bidirectional) |

### 2.2.4 Use of SFP slots (principle)

The SFP slots are used by SFP modules (FO fiberglass modules in SFP format). By selecting the SFP modules, the user can specify whether the switch has multimode or single-mode FO ports, for example.

The SFP modules are available separately as accessories, see “Technical data and ordering data” on page 75.

#### 2.2.4.1 Elements of the SFP modules

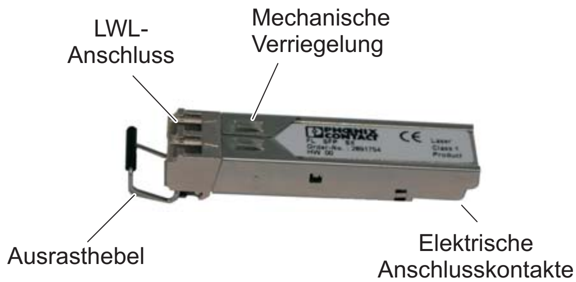



Figure 2-6 Elements of the SFP modules

#### 2.2.4.2 Mounting the SFP modules

**Inserting the SFP modules**

- Insert the SFP modules in the relevant slots on the switch.
- Ensure correct mechanical alignment of the SFP modules.

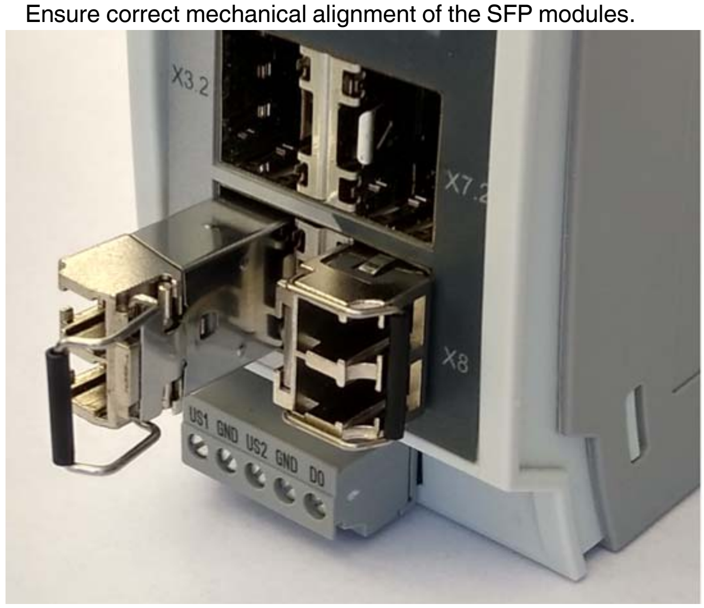



Figure 2-7 Inserting the SFP modules (example)

**Removing the SFP modules**

- Remove the FO connector before removing the SFP module.
- Turn the release latch to the side and pull out the SFP module.

## 2.2.5 Using the SD card

The switch is provided with a Phoenix Contact SD card, thereby enabling quick configuration. The slot for the SD card is located on the back of the device.

Figure 2-8 Position of the SD card slot

**Automatically reading the configuration on the SD card**

To automatically read the configuration on the SD card, make sure that the card is inserted when the switch is started. As soon as the boot process has been completed (indicated by the LEDs on the port going out), the configuration is applied in the internal switch memory and is active during operation. The SD card can then be removed. The configuration also remains active when the switch is restarted, provided an SD card is not inserted in the device.

# 3 Startup and function

## 3.1 Delivery state/factory settings

By default upon delivery or after the system is reset to the factory settings, the following functions and properties are available:

- The user name is: “admin”
- The password is: “private”
- All IP parameters are deleted. The switch has no valid IP address.
- 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 (as of firmware Version 2.01)
- The digital alarm output is an open drain output. In the event of redundant power supply, the output is connected to ground potential. If there is no redundant power supply, the output is floated.
- BootP for assigning IP parameters is activated
- The MAC address table does not contain any entries
- LLDP is activated
- DHCP server is deactivated

## 3.2 Using Smart mode

Smart mode enables the user to change the operating mode of the switch, without having access to one of the management interfaces.

The following setting options can be selected via Smart mode:

- Resetting the IP configuration
- Operating in EtherNet/IP mode
- Operating with a static IP address
- Operating in Unmanaged mode
- Reset to the factory settings

The Mode button is used to call/exit Smart mode and to select the desired setting. The four mode LEDs indicate the mode that is currently selected and that will apply when exiting Smart mode.

### 3.2.1 Calling Smart mode

- Following the switch boot phase, 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 X1 and X2 will flash. The active state is indicated alternately by the flashing of all four LEDs.
- When Smart mode is started, the switch is initially in the “Exit without changes” state.

### 3.2.2 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 18).

### 3.2.3 Possible operating modes in Smart mode

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

Table 3-1 Operating modes in Smart mode

| Mode | LED at port 1 top | LED at port 1 bottom | LED at port 2 top | LED at port 2 bottom |
|---|---|---|---|---|
| Exit Smart mode without changes | **On** | Off | Off | Off |
| Reset to the factory settings | Off | **On** | Off | Off |
| Set EtherNet/IP mode | Off | Off | **On** | Off |
| Operating with a default IP address | Off | **On** | **On** | Off |
| Reset the IP configuration | **On** | **On** | **On** | Off |
| Operating in Unmanaged mode | Off | **On** | Off | **On** |

### 3.2.4 Exiting Smart mode

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

### 3.2.5 Operating with a 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 “Operating with a static IP address” Smart mode as described in “Using Smart mode” on page 17.

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 “Operating with a default IP address” Smart mode as described in “Using Smart mode” on page 17.
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.

### 3.2.6 Operating in Unmanaged mode

For operation in Unmanaged mode, the switch can also be used without an IP address. The switch adopts the static IP address 0.0.0.0. The subnet mask and gateway are also configured to 0.0.0.0. In this way, 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 avoidance (RSTP, FRD, LTS)
– Functions for hardening the network (broadcast/multicast limiter)
– Functions for reducing the network load (IGMP snooping)

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.

## 3.3 Assigning IP parameters via BootP

BootP is activated by default.

For IP address assignment, the device uses the BootP protocol. 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 “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 it receives a valid IP address, the device stops sending BootP requests.

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

### 3.3.1 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 Tools → Options, select the BOOTP/DHCP SERVER menu item
- Configure the network interface on your PC to which the device is connected and select “BootP” mode. You can also adjust the subnet mask and configure a default gateway.
- Click “OK” to confirm the parameterization

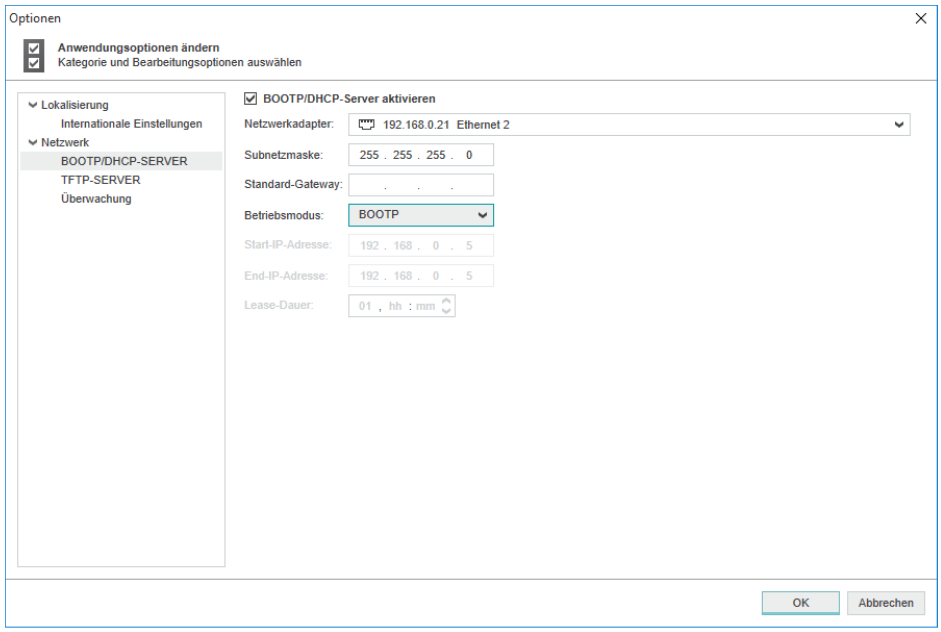



Figure 3-1 Settings for the BootP server

### 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

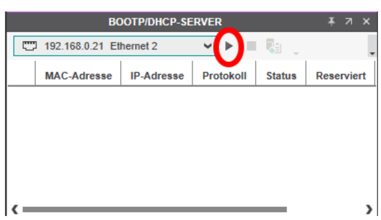



Figure 3-2 BootP server

### 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 an 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”.
- Now 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.

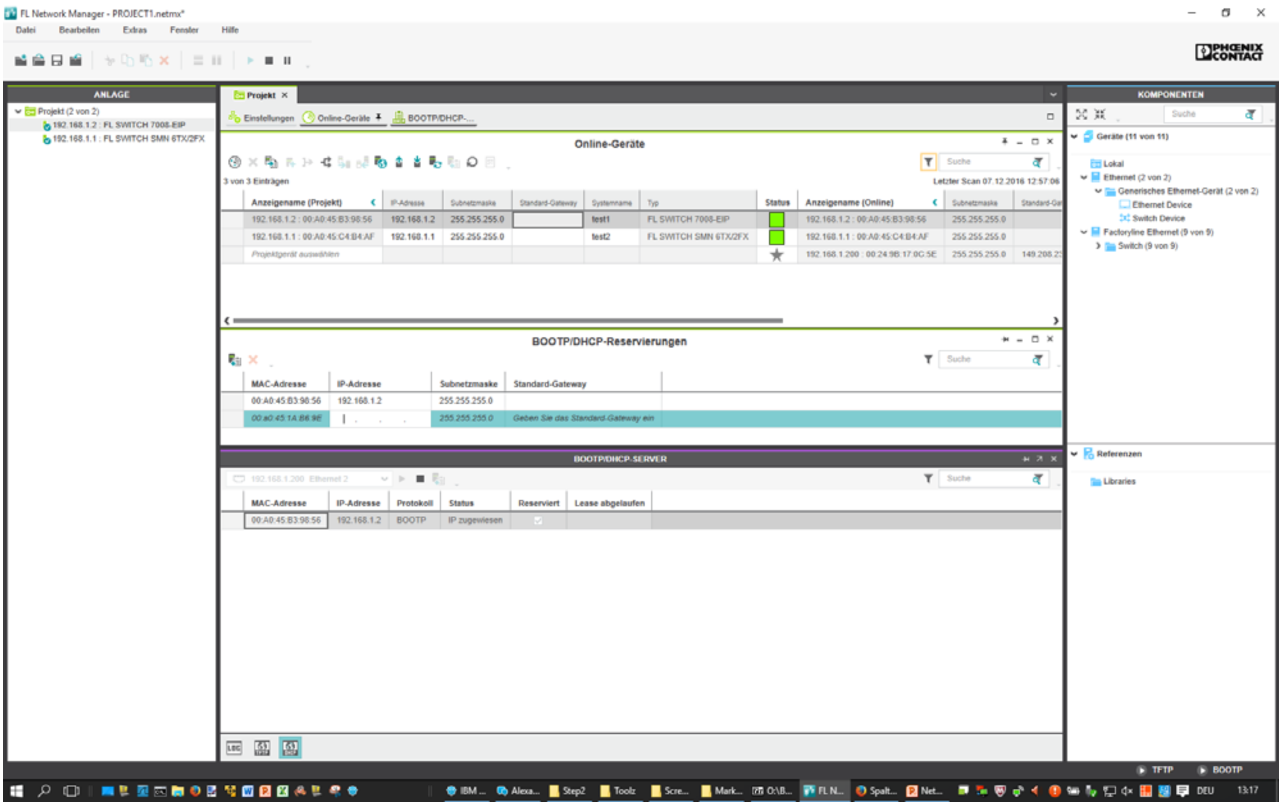


Figure 3-3 FL Network Manager with BootP/DHCP reservation list displayed

> If required, the IP parameters set here can be changed in web-based management (see “Requirements for the use of WBM” on page 27).

## 3.3.2 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 executing the program

- On the Internet, select the link phoenixcontact.net/catalog.
- Follow further instructions in order 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 product-related downloads.

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

### Step 2: “IP Assignment Tool”

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

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

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

- Click on the “Next” button.

### Step 3: “IP Address Request Listener”

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

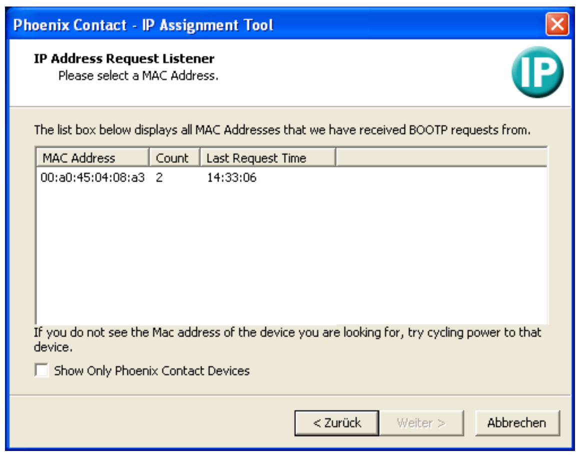



Figure 3-4 “IP Address Request Listener” window

| |
|---|
| The MAC address of the 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 which opens:

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

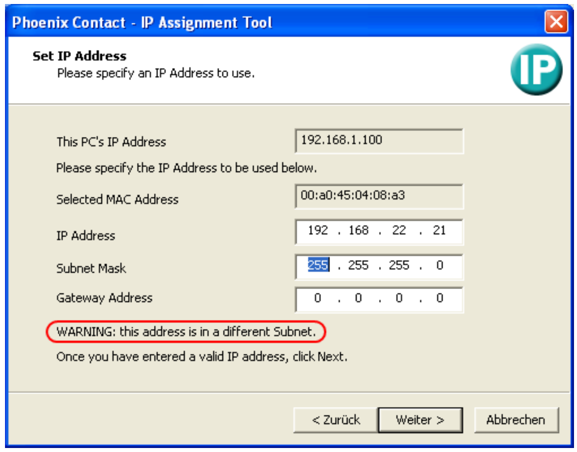



Figure 3-5 “Set IP Address” window with incorrect settings

- 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 transmit the set IP parameters to the device.

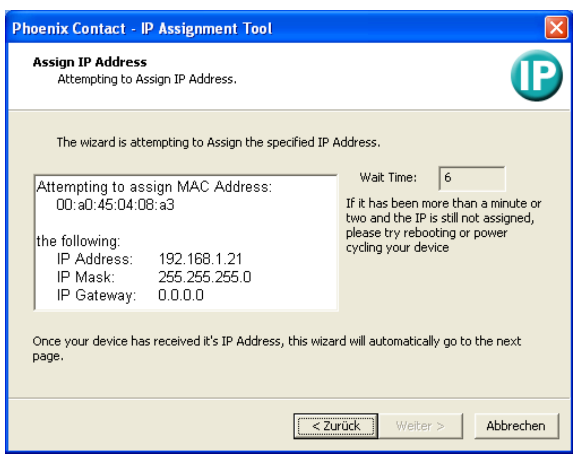



Figure 3-6 “Assign IP Address” window

Following successful transmission, the next window opens.

### Step 6: completing IP address assignment

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

To assign IP parameters for additional devices:

- Click on the “Back” button.

To exit IP address assignment:

- Click on the “Finish” button.

If required, the IP parameters set here can be changed in web-based management (see Section “Network” on page 39).

# 4 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.

## 4.1 Store and forward

All data telegrams received by the switch are stored and checked for validity. Invalid or faulty data packets (> 1536 bytes or CRC errors) and fragments (< 64 bytes) are rejected. Valid data telegrams are forwarded by the switch.

## 4.2 Multi-address function

The switch learns all the source addresses for each port. Only packets with:
– Unknown source addresses
– A source address for this port or
– A multicast/broadcast address

in the destination address field are forwarded via the relevant port. The switch can learn up to 8192 addresses. This is important if more than one end device is connected to one or more ports. Several independent subnetworks can be connected to one switch.

### 4.2.1 Learning addresses

The switch independently learns the addresses for end devices, which are connected via this port, by evaluating the source addresses in the data telegrams. When the switch receives a data telegram, it forwards this data telegram to only that 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 from its address table address entries that exceed a specific age (default: 40 seconds, adjustable from 10 to 825 seconds, aging time).

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

A list of detected MAC addresses can be found in the MAC address table. 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 available setting range is 10 - 825 seconds. For static configuration, an aging time of 300 seconds is recommended.

### 4.2.2 Prioritization

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

**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.
- Packets with VLAN/prioritization tag are forwarded according to the queues listed above.
- All remaining data is assigned to the low-priority queue.

#### 4.2.2.1 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 in various processing queues, depending on the priority information contained in the CoS tag. The switch supports four internal processing queues.

#### 4.2.2.2 Quality of Service (QoS)

Quality of Service affects the forwarding and handling of data streams and results in individual data streams being given differential treatment (usually preferential). QoS can be used, e.g., to guarantee a transmission bandwidth for individual data streams. The switch uses QoS in connection with prioritization.

# 5 Configuration and diagnostics in web-based management

The user-friendly web-based management (WBM) interface can be used to manage the switch from anywhere in the network using a standard browser (e.g., Internet Explorer 11). The configuration and diagnostic functions are clearly displayed on 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, set parameters, and the operating state can be viewed.

| |
|---|
| Modifications to the device can only be made by entering the valid password. By default upon delivery, the user name is “admin” and the password is “private”. |

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

## 5.1 Requirements for the use of WBM

As the web server operates using the Hyper Text Transfer Protocol, a standard browser can be used. Access is via the URL “http://IP address of the device”. Example: “http://172.16.29.112”. If the web server is set to the secure HTTPS protocol in WBM, access is via the URL “http**s**://IP address of the device”. For full operation of the web pages, the browser must support JavaScript 1.2 and Cascading Style Sheets Level 1. We recommend the use of Microsoft Internet Explorer 11.

| |
|---|
| WBM can only be called using a valid IP address. By default upon delivery, the switch has no valid IP address (see “Assigning IP parameters via BootP” on page 19). |

| |
|---|
| Device login is only possible if cookies are allowed 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. |

In order to make changes, you must log into the device. To do so, click on the “Login” button.

By default upon delivery, the user name is “admin” and the password is “private”.


Figure 5-1 Login window

## 5.2 Functions/information in WBM

WBM is split into the following areas:

– Information: general device information
– Configuration: device configuration
– Diagnostics: device-specific diagnostics


Figure 5-2 Start page for web-based management (example)

## 5.2.1 Information area of WBM

### 5.2.1.1 Help & Documentation

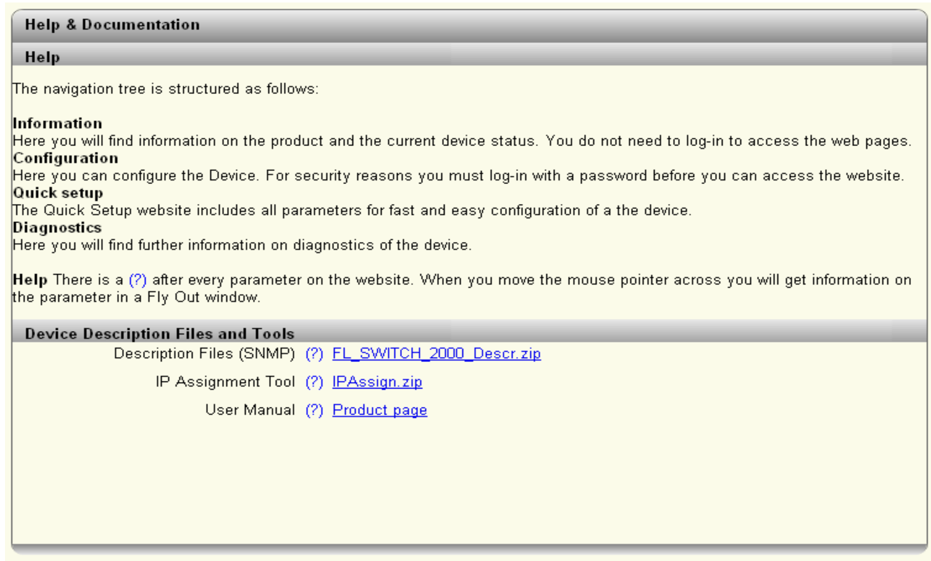


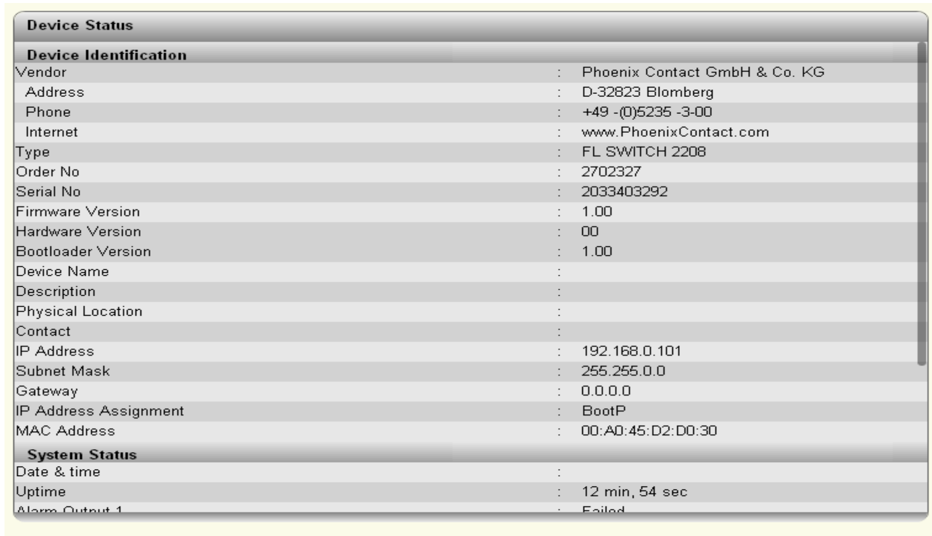

Figure 5-3 “Help & Documentation” web page

Here you will find useful information about using web-based management. On this page, the following files and software, which are supplied with the device, can be downloaded directly from the device:

– Description Files (SNMP)
– IP Assignment Tool (see “Assigning the IP address using FL NETWORK MANAGER Basic” on page 19)

### 5.2.1.2 Device Status

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



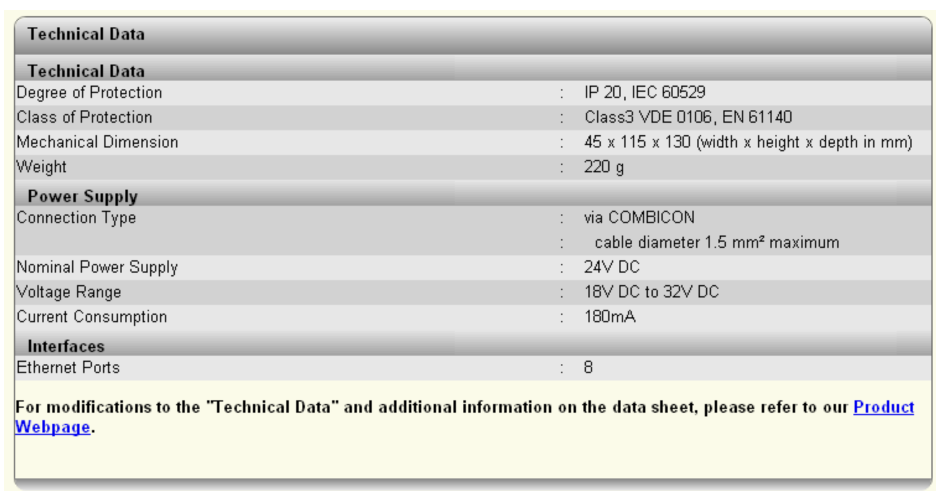
**Device Status**

| | | |
|---|---|---|
| **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 2208 |
| Order No | : | 2702327 |
| Serial No | : | 2033403292 |
| Firmware Version | : | 1.00 |
| Hardware Version | : | 00 |
| Bootloader Version | : | 1.00 |
| Device Name | : | |
| Description | : | |
| Physical Location | : | |
| Contact | : | |
| IP Address | : | 192.168.0.101 |
| Subnet Mask | : | 255.255.0.0 |
| Gateway | : | 0.0.0.0 |
| IP Address Assignment | : | BootP |
| MAC Address | : | 00:A0:45:D2:D0:30 |
| **System Status** | | |
| Date & time | : | |
| Uptime | : | 12 min, 54 sec |
| Alarm Output 1 | : | Failed |

Figure 5-4 “Device Status” web page

### 5.2.1.3 Technical Data

Here you will find the technical data for your device, such as specifications for the power supply.



**Technical Data**

| | | |
|---|---|---|
| **Technical Data** | | |
| Degree of Protection | : | IP 20, IEC 60529 |
| Class of Protection | : | Class3 VDE 0106, EN 61140 |
| Mechanical Dimension | : | 45 x 115 x 130 (width x height x depth in mm) |
| Weight | : | 220 g |
| **Power Supply** | | |
| Connection Type | : | via COMBICON |
| | : | cable diameter 1.5 mm² maximum |
| Nominal Power Supply | : | 24V DC |
| Voltage Range | : | 18V DC to 32V DC |
| Current Consumption | : | 180mA |
| **Interfaces** | | |
| Ethernet Ports | : | 8 |

**For modifications to the "Technical Data" and additional information on the data sheet, please refer to our Product Webpage.**

Figure 5-5 “Technical Data” web page

### 5.2.1.4 Local Diagnostics

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

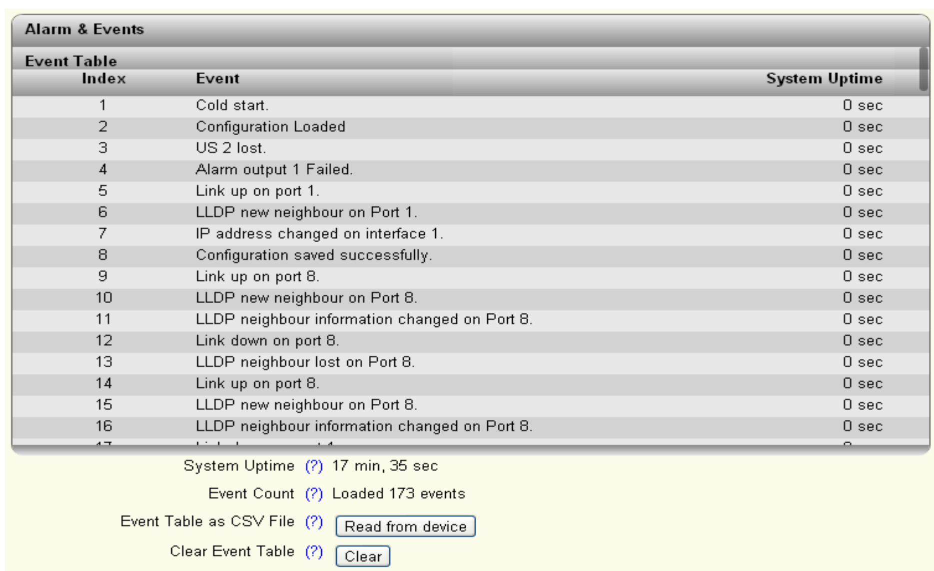
Local Diagnostics

| | | |
|---|---|---|
| **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 10/100 Mbit/s (LED off/green) |

Figure 5-6 “Local Diagnostics” web page

### 5.2.1.5 Alarm & Events

You will find a list of alarms and events on this page. The entries in the “Event Table” are also retained after power up. The “Event Table” can be downloaded from the device in CSV format.



Alarm & Events

Event Table

| Index | Event | System Uptime |
|---|---|---|
| 1 | Cold start. | 0 sec |
| 2 | Configuration Loaded | 0 sec |
| 3 | US 2 lost. | 0 sec |
| 4 | Alarm output 1 Failed. | 0 sec |
| 5 | Link up on port 1. | 0 sec |
| 6 | LLDP new neighbour on Port 1. | 0 sec |
| 7 | IP address changed on interface 1. | 0 sec |
| 8 | Configuration saved successfully. | 0 sec |
| 9 | Link up on port 8. | 0 sec |
| 10 | LLDP new neighbour on Port 8. | 0 sec |
| 11 | LLDP neighbour information changed on Port 8. | 0 sec |
| 12 | Link down on port 8. | 0 sec |
| 13 | LLDP neighbour lost on Port 8. | 0 sec |
| 14 | Link up on port 8. | 0 sec |
| 15 | LLDP new neighbour on Port 8. | 0 sec |
| 16 | LLDP neighbour information changed on Port 8. | 0 sec |

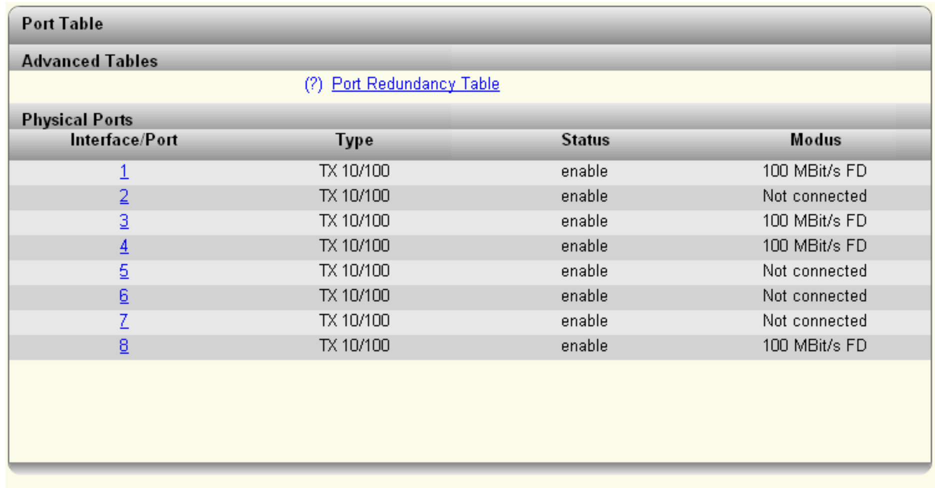
| | | |
|---|---|---|
| System Uptime | (?) | 17 min, 35 sec |
| Event Count | (?) | Loaded 173 events |
| Event Table as CSV File | (?) | Read from device |
| Clear Event Table | (?) | Clear |

Figure 5-7 “Alarm & Events” web page

### 5.2.1.6 Port Table

You will find a list of the current states of the individual ports on this page.

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

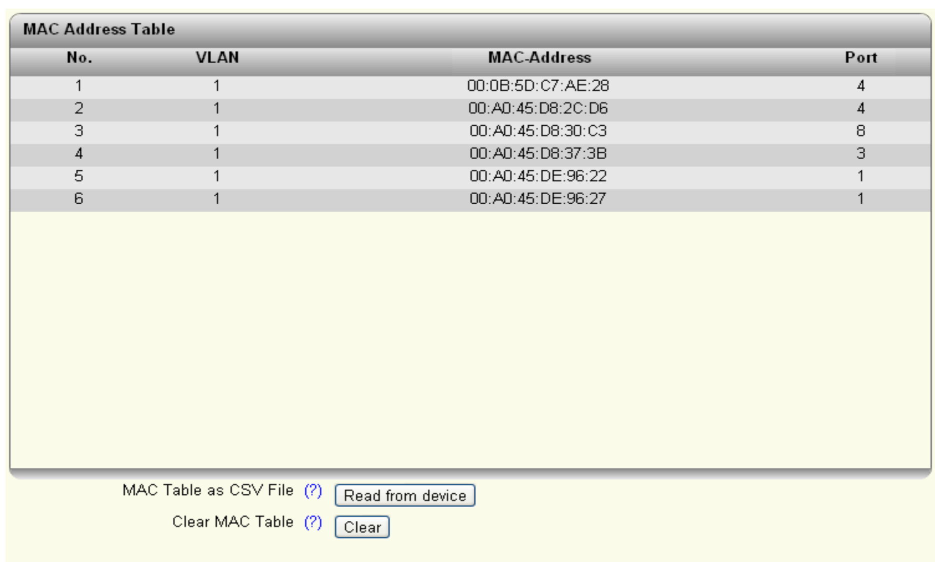



| Interface/Port | Type | Status | Modus |
|---|---|---|---|
| 1 | TX 10/100 | enable | 100 MBit/s FD |
| 2 | TX 10/100 | enable | Not connected |
| 3 | TX 10/100 | enable | 100 MBit/s FD |
| 4 | TX 10/100 | enable | 100 MBit/s FD |
| 5 | TX 10/100 | enable | Not connected |
| 6 | TX 10/100 | enable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

Figure 5-8 “Port Table” web page

### 5.2.1.7 MAC Address Table

You will find a list of the current devices in the network on this page. The list can be downloaded from the device in CSV format.




| No. | VLAN | MAC-Address | Port |
|---|---|---|---|
| 1 | 1 | 00:0B:5D:C7:AE:28 | 4 |
| 2 | 1 | 00:A0:45:D8:2C:D6 | 4 |
| 3 | 1 | 00:A0:45:D8:30:C3 | 8 |
| 4 | 1 | 00:A0:45:D8:37:3B | 3 |
| 5 | 1 | 00:A0:45:DE:96:22 | 1 |
| 6 | 1 | 00:A0:45:DE:96:27 | 1 |



Figure 5-9 “MAC Address Table” web page

## 5.2.2 Configuration area of WBM

### 5.2.2.1 System

Reset Device: clicking on the “Reset” button restarts the device. All unsaved parameters will be lost.

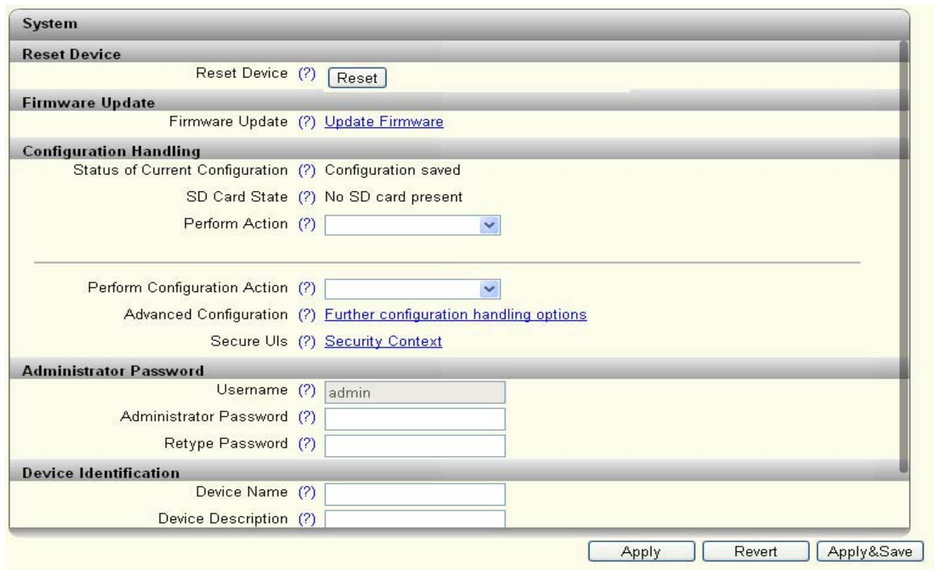



Figure 5-10 “System” web page

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

#### 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. Clicking on “Browse” allows you to select the desired file on your PC. Clicking on “Apply” starts the update.

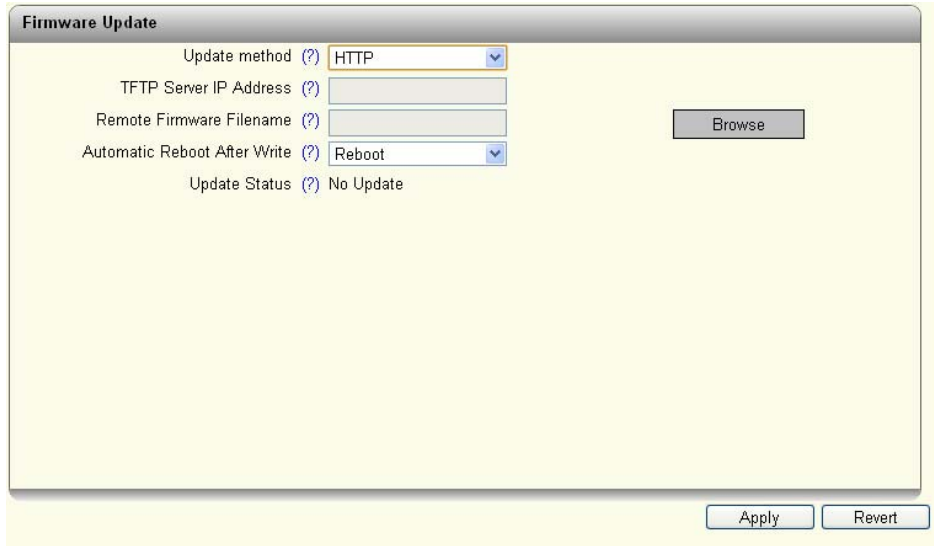



Figure 5-11 “Firmware Update via HTTP” pop-up

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

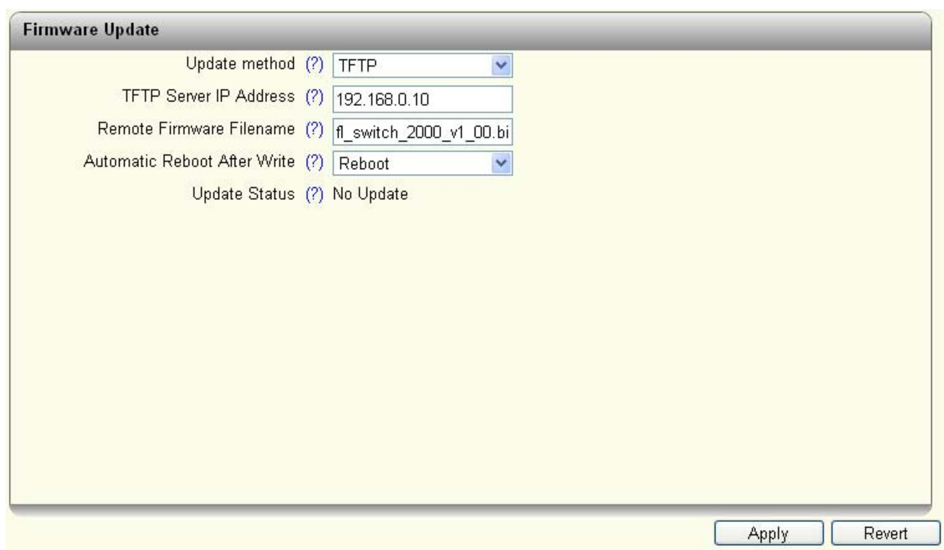



Figure 5-12 “Firmware Update via TFTP” pop-up

- TFTP server IP address:
  Here, set the IP address of the computer on which the TFTP server is active.
- Remote firmware filename:
  Here, set the name of the firmware file which is to be transferred to the device.

– Automatic reboot after upload:
  Here, set whether a reboot should be carried out after the firmware update. The firmware update starts as soon as you click on “Apply”.

**Configuration Handling**

Status of Current Configuration: indicates the status of the active configuration

SD Card State: indicates whether or not an SD card is inserted

| |
|---|
| This display can only be refreshed by reloading the web page. |

Perform Action:

– Compare: compares the configuration file on the SD card with the one on the device.
– Clear: deletes the configuration file on the SD card.

The selected action is performed by clicking in the drop-down list.

Perform Configuration Action:

– 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.

The selected action is performed by clicking in the drop-down list.

Advanced Configuration: clicking on the “Further configuration handling options” link opens a window in which the parameters for transferring a configuration file from the device to the PC (download) or from the PC to the device (upload) must be entered.

Secure UIs: clicking on the “Security Context” link opens the “Security Context” pop-up (see page 37).

**Pop-up: Advanced Configuration**

File Type: select the file type here.

Direction: here you should select whether the configuration is to be uploaded to or downloaded from the device.

Update status: indicates the current transfer status.

Start transfer: click on the “Start” button to start the transfer of the configuration.

Configuration name: here you should enter the name under which you want to save the configuration on the PC.

Transfer via HTTP: select “HTTP” as the transfer method. Clicking on “Browse” allows you to select the desired file on your PC. You can upload the desired file directly to the PC via your browser by selecting “HTTP Upload”.

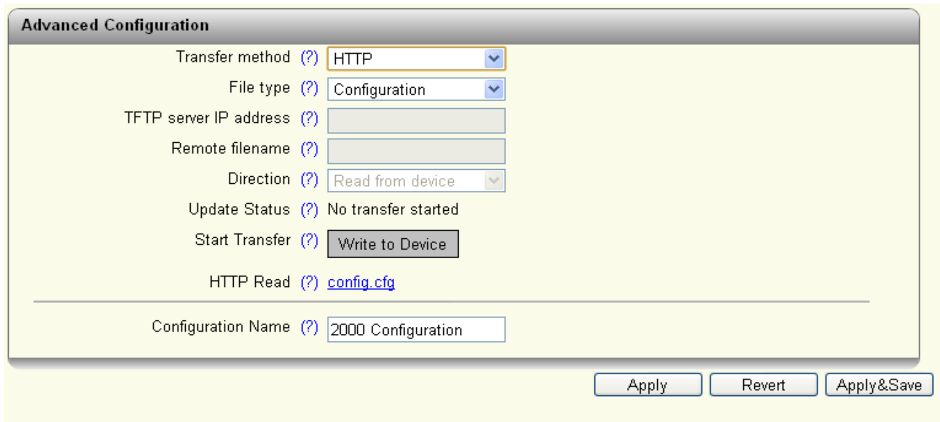



Figure 5-13 “Advanced Configuration” pop-up

Transfer via TFTP: select “TFTP” as the transfer method.

TFTP server IP address: here you should enter the IP address via which the TFTP server can be reached.

Remote filename: here you should enter the name of the file to be uploaded or downloaded.

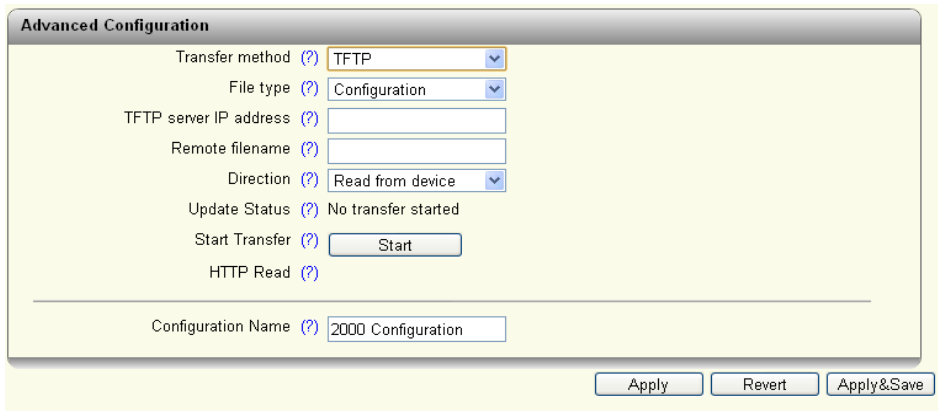



Figure 5-14 “Advanced Configuration” pop-up

### Pop-up: Security Context

Create new context: clicking on the “Generate” button creates all the necessary keys and certificates for operation with HTTPS and SSH.

Current state: displays the status of the current availability of the security context.

Root CA: clicking on the “cacert.cer” link loads the Root CA certificate for the installation in the browser.

Advanced Configuration: clicking on the “File transfer” link opens the “Advanced Configuration” pop-up (see “Pop-up: Advanced Configuration” on page 35).

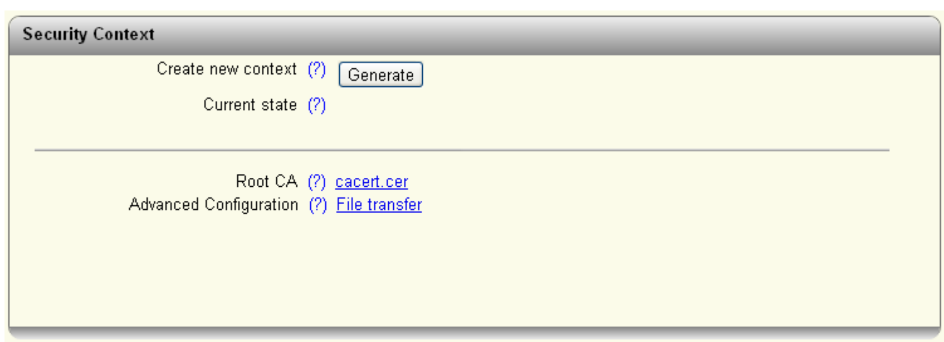



Figure 5-15 “Security Context” pop-up

### Administrator Password


Figure 5-16 “Administrator Password” configuration area

You can change the administrator password here. The new password must be between 8 and 63 characters long. The new password will be activated after logout. By default upon delivery, the password is “private” (please note that it is case-sensitive). For security reasons, the input fields do not display your password, but instead “*******” is displayed.

### Device Identification

Device information can be configured in this area, which is then displayed on the “Device Status” page.

Device Name: you can configure the device name here.

Device Description: you can enter a device description in this text field.

Physical Location: here you can provide the location of the device, such as the building in which it is installed.

Device Contact: you can enter a contact address in this field.

### 5.2.2.2 Quick Setup

The basic settings can be made in Quick Setup.

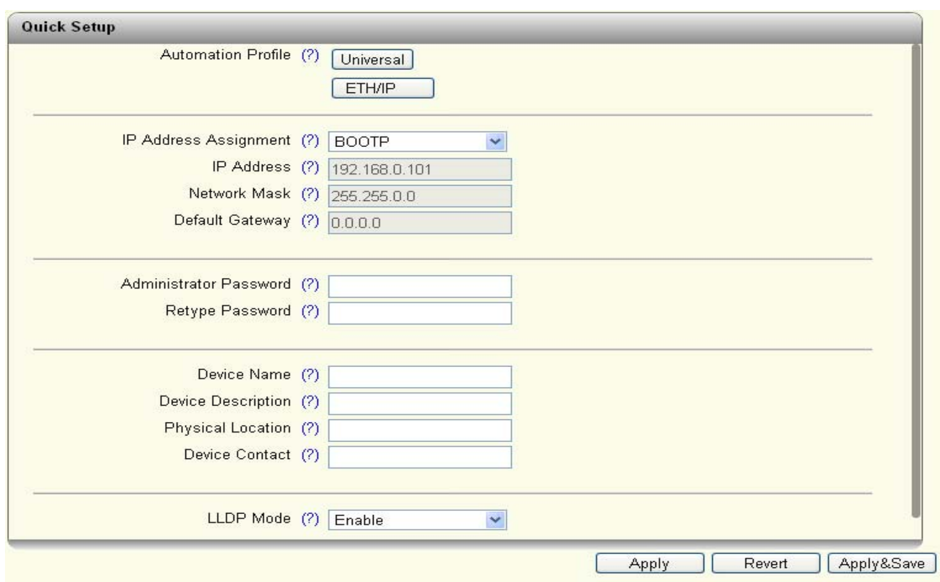



Figure 5-17 “Quick Setup” web page

Automation Profile: select a profile which is optimized for the desired operating mode.

IP Assignment: select the type of IP address assignment.

– STATIC: static IP address
– BOOTP: assignment via the Bootstrap protocol
– DHCP: assignment via a DHCP server

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: you can change the administrator password here.

Device Name: you can enter the device name of the switch here.

Device Description: you can enter a description for the device here.

Physical Location: you can enter a location for the device here.

Device Contact: you can enter the name of a contact person for the device here.

LLDP Mode: you can enable or disable LLDP here.
– 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 which can also be accessed via the menu item of the same name (see “Link Layer Discovery Protocol (LLDP)” on page 65).

Port-based LLDP configuration can be found on the “Service” page (see “Service” on page 40).

### 5.2.2.3 Network

The basic network settings are made here.

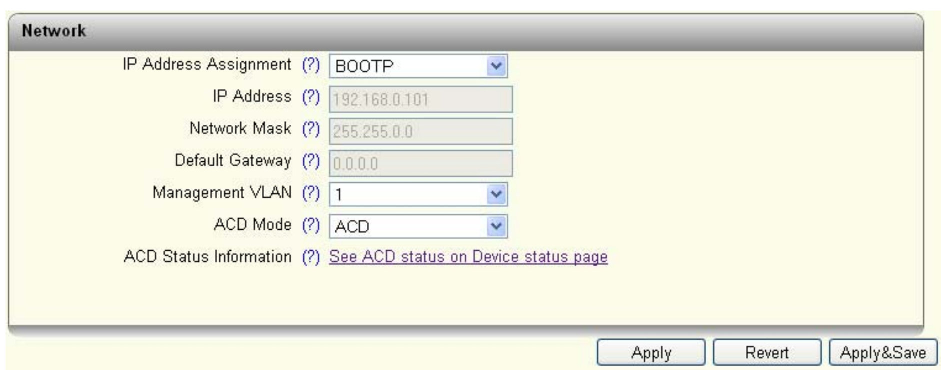



Figure 5-18 “Network” web page

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

If you have chosen “STATIC”, now make the following settings:

IP Address: set the desired IP address.

Network Mask: set the desired subnet mask here.

Default Gateway: set the desired default gateway here.

Management VLAN: set the VLAN here, in which the management is to be located (default: “1”).

ACD Mode: you can enable/disable the “Address Conflict Detection” function here.

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

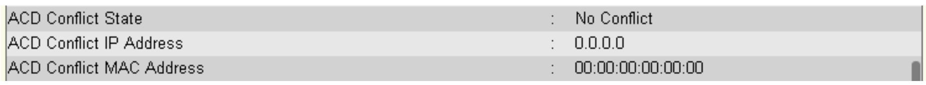



Figure 5-19 ACD status information on the “Device Status” page

#### 5.2.2.4 Service

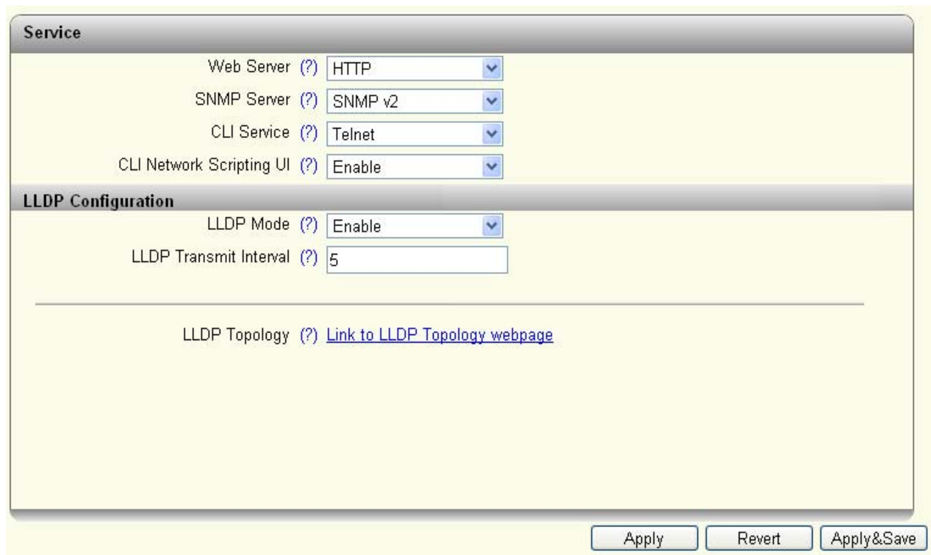



Figure 5-20 “Service” web page

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

SNMP Server: you can enable/disable the SNMP server function and the mode (SNMP v2, SNMP v3) here.

CLI Service:

- Disable: entry of CLI commands is deactivated
- Telnet: entry of CLI commands via Telnet is activated
- SSH: entry of CLI commands via Secure Shell (SSH) is activated

CLI Network Scripting UI:

- Disable: transmission of CLI commands via the network is deactivated
- Enable: transmission of CLI commands via the network is activated

> For additional information on using the CLI, refer to “Configuration and diagnostics via Command Line Interface (CLI)” on page 57.

LLDP Mode:

– Disable: LLDP is disabled
– Enable: LLDP is enabled
– Send only: only LLDP BPDUs are sent.
– Receive only: only LLDP BPDUs are received.

Port-based LLDP configuration can be found on the “Service” page (see “Service” on page 40).

LLDP Transmit Interval: here you can set the interval in which LLDP telegrams are to be sent. The value must be between 5 and 32786 seconds (default: 5 s).

LLDP Transmission: you can enable/disable port-specific forwarding of LLDP telegrams here

LLDP Reception: you can enable/disable port-specific ignoring of LLDP telegrams here

For additional information on “LLDP”, refer to “Link Layer Discovery Protocol (LLDP)” on page 65.

### 5.2.2.5 Port Configuration

#### Individual Port Configuration

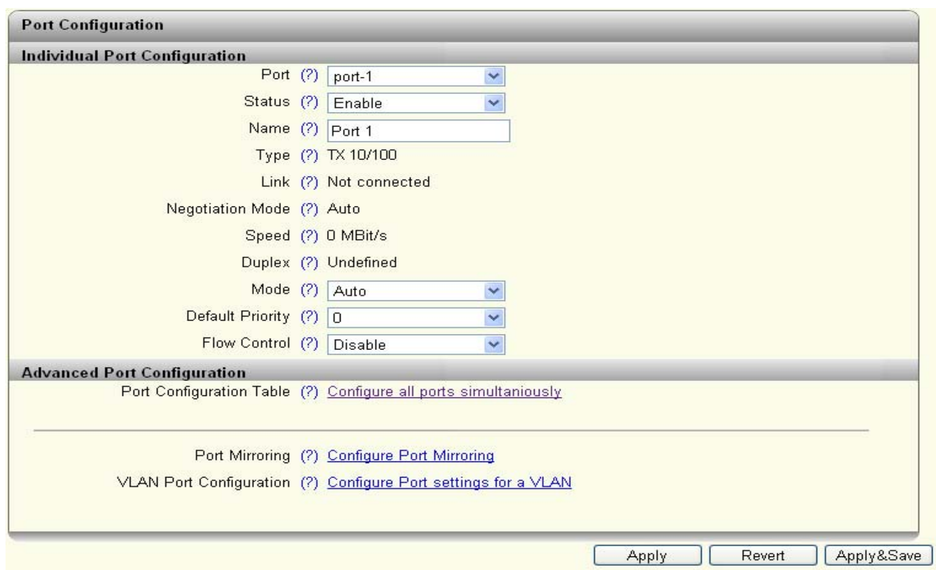



Figure 5-21 “Port Configuration” web page

Port: select the port that you want to configure individually.

Status: the port can be activated/deactivated here.

Name: you can assign the port a name.

Type: describes the physical properties of the port.

Link: displays the current link status of the port.

Negotiation Mode: indicates 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.

Link Monitoring: here you can set whether the link behavior is to be monitored at the selected port.

Default Priority: set the priority for incoming data packets at this port here.

Flow Control: flow control for the selected port can be enabled and disabled here.

### Advanced Port Configuration

Clicking on the “Configure all ports simultaneously” link takes you to the “Port Configuration Table” page. You can set the status, mode, link monitoring, and flow control for all ports here.

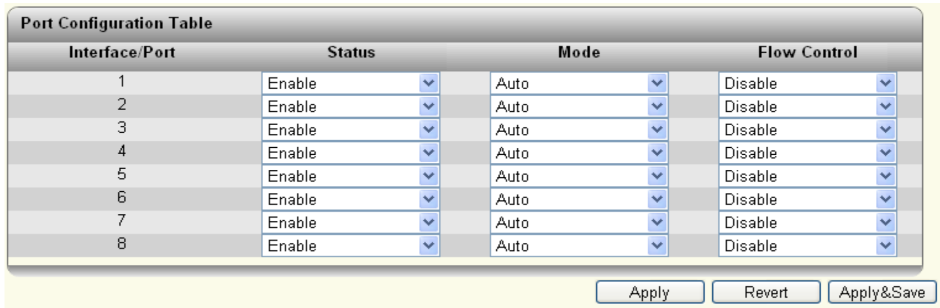



Figure 5-22 “Port Configuration Table” web page

Clicking on the “Configure Port Mirroring” button takes you to the port mirroring configuration (see “Port Mirroring” on page 53).

Clicking on the “Configure Port Settings for a VLAN” button takes you to the “VLAN Port Configuration” page (see “VLAN Configuration” on page 71).

### 5.2.2.6 VLAN Configuration

For additional information on “VLAN”, refer to “Virtual Local Area Network (VLAN)” on page 71.

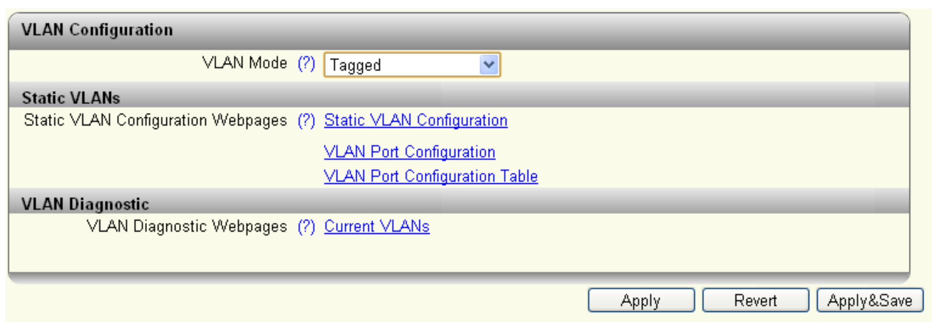



Figure 5-23 “VLAN Configuration” web page

### 5.2.2.7 Multicast Filtering

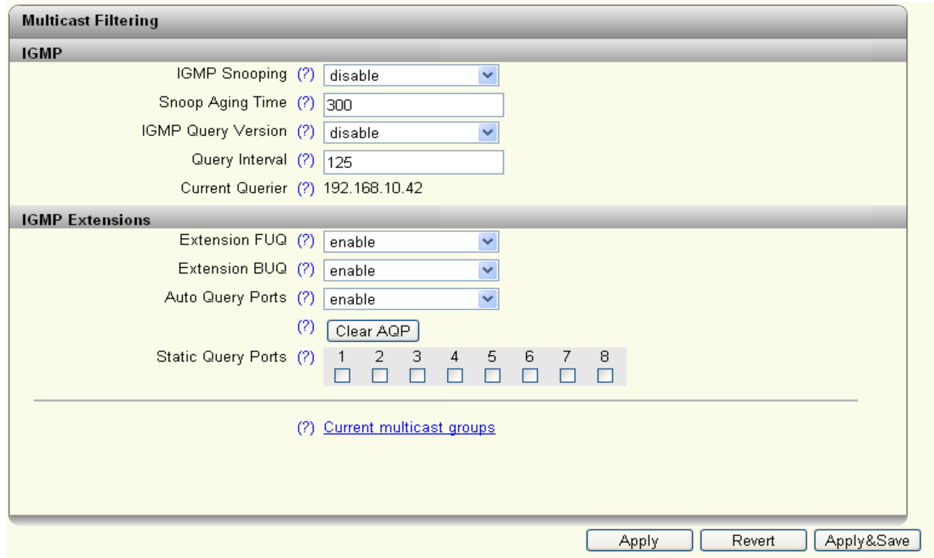



Figure 5-24 “Multicast Filtering” web page

For additional information on “Multicast”, refer to “Multicast filtering” on page 69.

### 5.2.2.8 Network Redundancy

#### Spanning-Tree Configuration

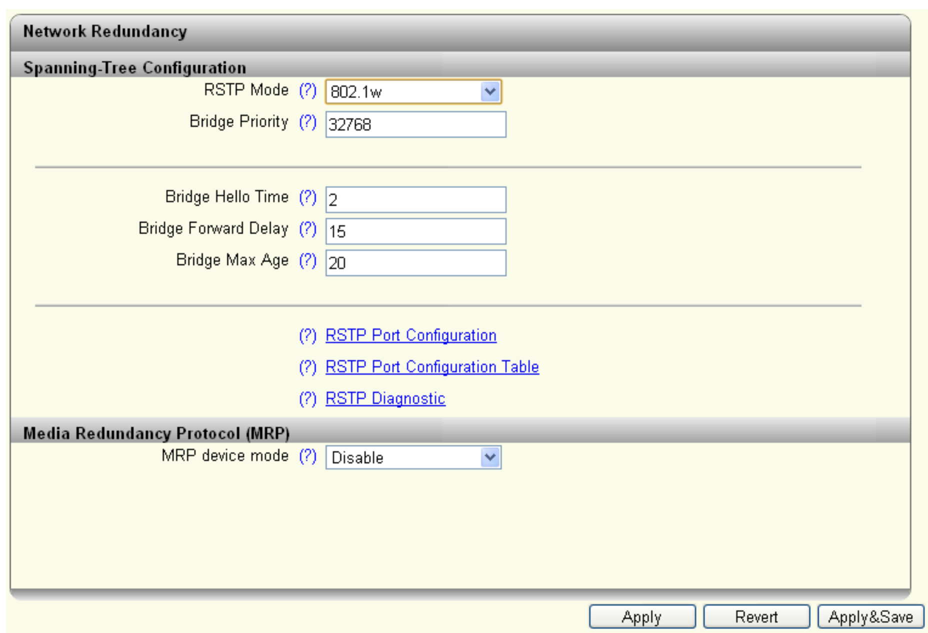



Figure 5-25 “Spanning-Tree Configuration” configuration area

RSTP Mode:

– Disable: the RSTP function is not activated
– 802.1w: the RSTP function is activated globally and operates according to standard 802.1w

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

– 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 provides easy diagnostics. RSTP fast ring detection provides each ring with an ID. This ID is made known to each switch in the relevant ring. A switch can belong to several different rings at the same time.
– Bridge Priority: the bridge and backup roots can be specified via “Bridge Priority”. Only multiples of 4096 are permitted. The value will be rounded automatically to the next multiple of 4096. Once you have clicked on “Apply&Save”, the initialization mechanism is started (default value: 32768).
– Bridge Hello Time: specifies the time interval within which the root bridge regularly reports to the other switches via BPDU.
– Bridge Forward Delay: the bridge forward delay value indicates how long the switch is 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 make sure that each switch in the network has a constant value, against which the age of the saved configuration is tested.

Clicking on the “RSTP Port Configuration” button takes you to the “RSTP Port Configuration” pop-up.

Clicking on the “RSTP Port Configuration Table” button takes you to the “RSTP Port Configuration Table” pop-up (see page 47).

Clicking on the “RSTP Diagnostic” button opens the “RSTP Diagnostic” page as a pop-up (see page 52).

**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 manager function is only available for the 2200/2300 versions provided that the SD card is inserted and has a MRP master license (MRM) (see “Ordering data” on page 85).

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

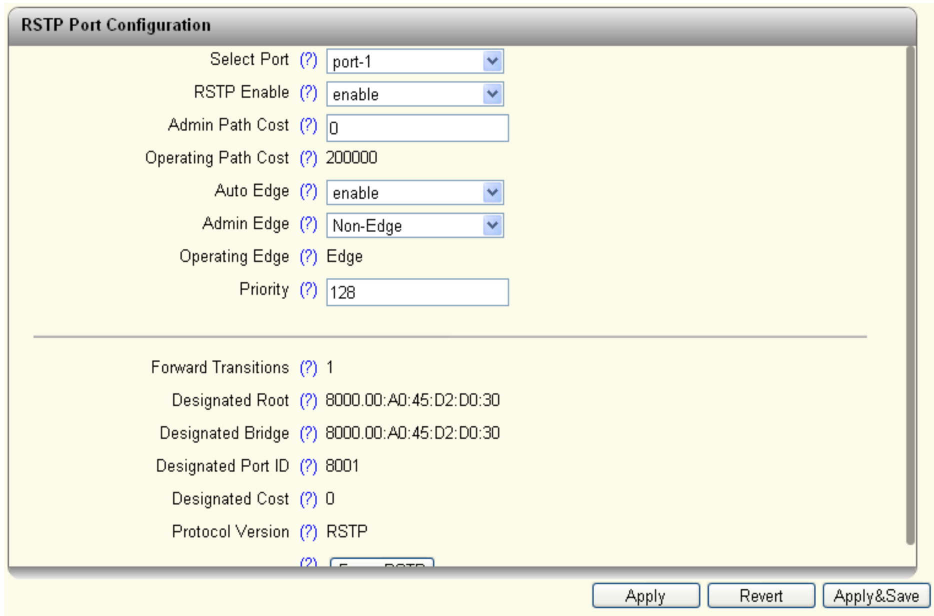



Figure 5-26 “RSTP Port Configuration” web page

Select Port: select the port for which you want to change the RSTP settings here.

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 the cost calculation according to the transmission speed (10 Mbps = 2000000; 100 Mbps = 200000).

Operating Path Cost: displays the path costs used for this port.

Auto Edge: here you can set whether an automatic change from non-edge port to edge port is to be carried out after a link up.

Admin Edge: here you can set whether this port is to be operated as an edge port (default setting), if possible.

Operating Edge: indicates whether this port is operated as an edge port or a non-edge port.

Priority: indicates the priority set for this port (default value: 128).

Forward Transitions: indicates the number of times the port switches from the “Discarding” state to the “Forwarding” state.

Designated Root: indicates 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: displays the path costs of this segment to the root switch.

Protocol Version: displays the protocol version.

#### Pop-up: RSTP Port Configuration Table

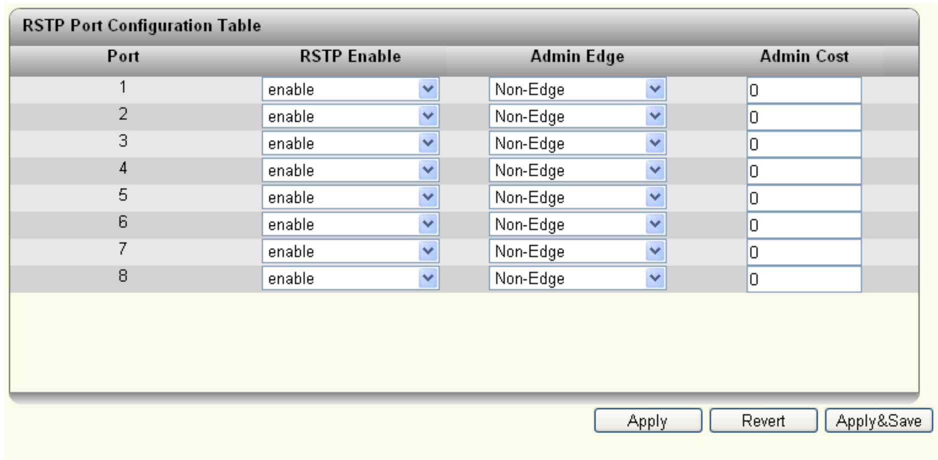



Figure 5-27 “RSTP Port Configuration Table” web page

Port: indicates the ports for which RSTP is available.

RSTP Enable: here you can individually activate or deactivate RSTP for each port.

Admin Edge: here you can set 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 the cost calculation according to the transmission speed (10 Mbps = 2000000; 100 Mbps = 200000).

### 5.2.2.9 Security

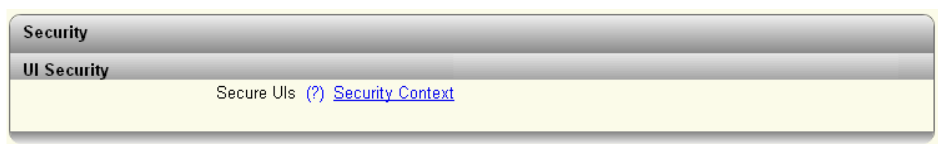



Figure 5-28 “Security” web page

Secure UIs: clicking on the “Security Context” link opens the pop-up of the same name (see page 37).

#### 5.2.2.10 DHCP Service

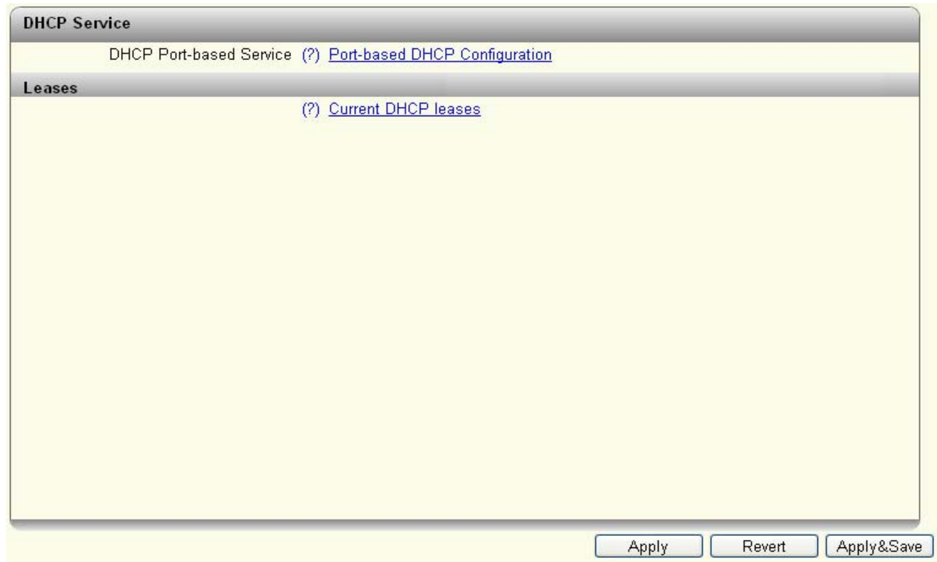



Figure 5-29 “DHCP Service” web page

DHCP Mode: select the DHCP service you wish to use here.

– None: a DHCP service is not used on the switch.
– Relay Agent: the DHCP relay agent (DHCP Option 82) is enabled.
– Server: the switch is used as the DHCP server.

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

Option82: select the address which should be used as the remote ID here.

– 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: set the IP address of the DHCP server in your network here.

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

> The following fields are only available after selecting “Server” as the DHCP mode.

– Running State: shows the current status of the DHCP server. The status is “Inactive” if some setting options are incorrect.
– Pool Start Address: set the first IP address of the DHCP server address pool here.
– Pool Size: set the number of IP addresses in the DHCP server address pool here. Please note that the number of IP addresses must match the configured subnetwork.
– Network Mask: set the subnet mask that is assigned to the DHCP clients here.
– Router IP: set the router/default gateway IP address that is assigned to the DHCP clients here.
– DNS IP: set the DNS IP address that is assigned to the DHCP clients here.

- Lease Time (s): the time that the DHCP server leases an IP address to a client before it has to report to the server again can be set here. The value must be between 300 and 2592000 seconds, "0" is interpreted as an infinite time (default: 3600).
- Accept Bootp: here you can set 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.

Port-based DHCP Configuration: opens the "Port-based DHCP Configuration" pop-up.
Current DHCP leases: opens the "Current DHCP Leases" pop-up where the IP addresses that are currently assigned are displayed.
DHCP static leases: opens the "DHCP Static Leases" pop-up for configuring static IP address assignment.

### Pop-up: Port-based DHCP Configuration

The port-based DHCP server functionality can be configured in this pop-up.

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

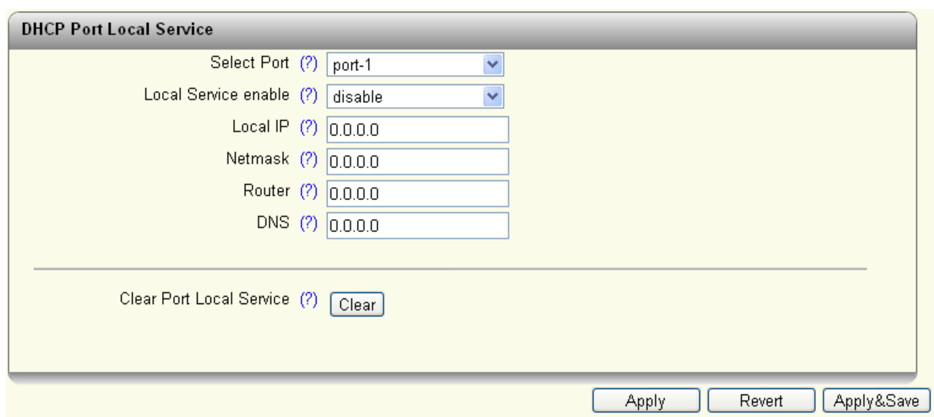



Figure 5-30 "DHCP Port Local Service" pop-up

### 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: indicates the port to which the client is connected.
- State: indicates the status of the client.
- Lease count: displays the number of assigned IP addresses.

– Release: clicking on the “Release” button releases unused entries.

**Pop-up: DHCP Static Leases**

This pop-up displays the configured static IP assignment.

Lease list:

- – IP address: displays the static IP address assigned.
- – Client address: displays the MAC address of the client.
- – Delete: clicking on the red cross deletes the entry.

Create new static entry:

- – IP address: enter the static IP address that you wish to assign here.
- – Client address: enter the MAC address to which you wish to assign a static IP address here.
- – Create: click on the “Create” button to carry out static assignment.

Clear static table: click on the “Clear” button to delete all the static DHCP leases.

### 5.2.2.11 Local Events

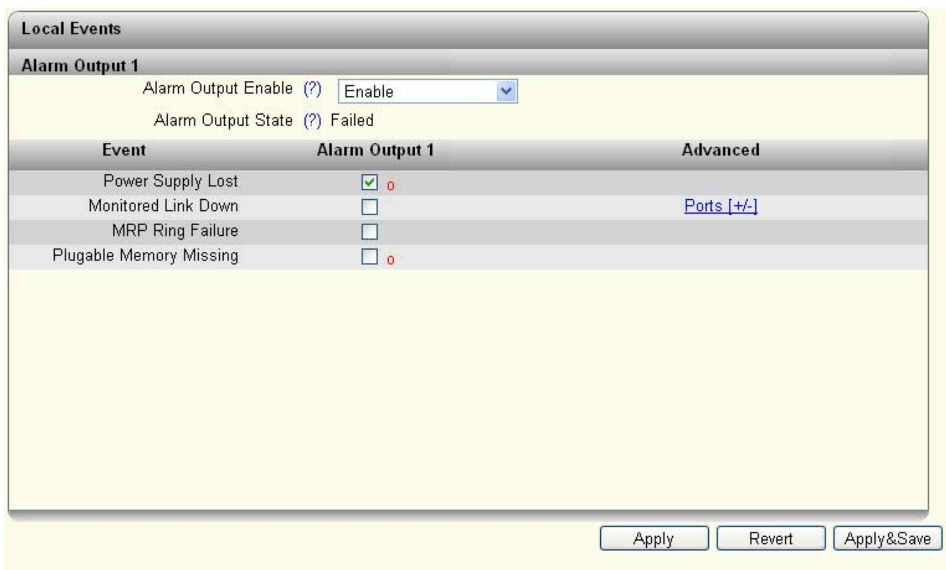



Figure 5-31 “Local Events” web page

Alarm output 1:

Here you can activate the digital alarm output and read the current status (if a red “**o**” is present, this event has occurred).

Events: here you can determine under which conditions a digital alarm output should report an error.

- – Power Supply lost: in the event that US1 or US2 is lost
- – Monitored link down: under “Advanced”, select the ports to which link down behavior should be reported.
- – MRP Ring Failure: indicates an error message in the event of an MRP ring error.

– Pluggable Memory missing: an error message is generated if no memory card is present.

### 5.2.2.12 Quality of Service

#### Broadcast Limiter

Broadcast: the broadcast limiter can be activated or deactivated here.

Broadcast Threshold: set the threshold value in frames per second for the broadcast limiter here. The entered value is rounded down to the next valid value.

Multicast: the multicast limiter can be activated or deactivated here.

Multicast Threshold: set the threshold value in frames per second for the multicast limiter here. The entered value is rounded down to the next valid value.

Unknown Unicast: the limiter for unknown unicasts can be activated or deactivated here. Unicasts of a MAC address that has been learned by the switch are not affected.

Unicast Threshold: set the threshold value in frames per second for the limiter of unknown unicasts here. The entered value 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.

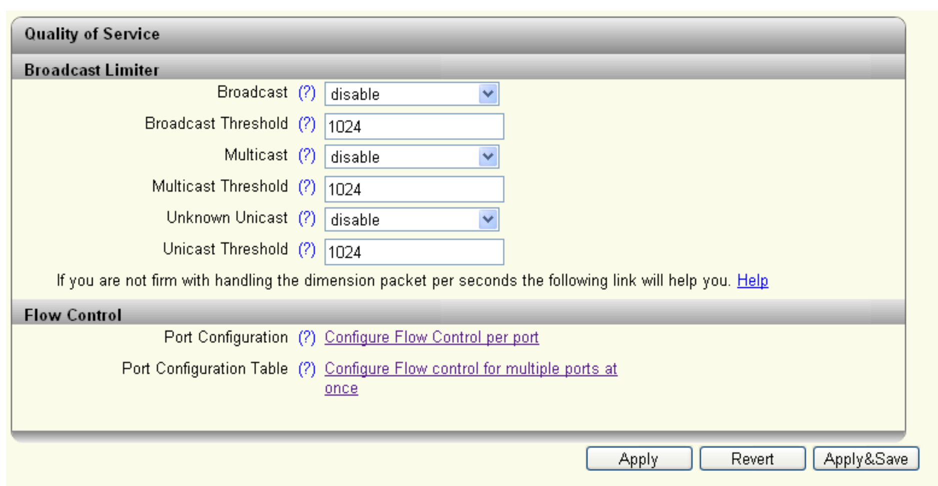



Figure 5-32 “Quality of Service” web page

## 5.2.3 Diagnostics area of WBM

### 5.2.3.1 LLDP Topology

For additional information, please refer to “Link Layer Discovery Protocol (LLDP)” on page 65.

### 5.2.3.2 RSTP Diagnostic

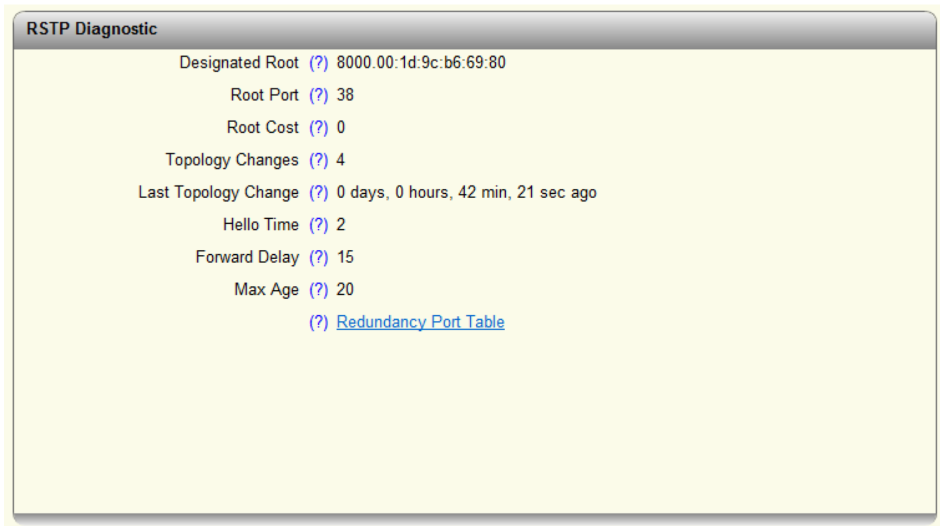



Figure 5-33 “RSTP Diagnostic” web page

Designated Root: indicates the root bridge for this spanning tree.

Root Port: indicates 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: indicates the number of topology changes.

Last Topology Change: indicates when the last topology change 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 max age time set at the root.

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

### 5.2.3.3 MRP Diagnostic

Operating Mode: indicates 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: indicates the current status of the MRP ring.

Change Counter: indicates the number of changes in state in the MRP ring.

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


Figure 5-34 “MRP Diagnostic” web page

#### 5.2.3.4 Current VLANs

For additional information, refer to “Current VLANs” on page 74.

#### 5.2.3.5 Current Multicast Groups

For additional information, refer to “Multicast filtering” on page 69.

#### 5.2.3.6 Port Mirroring

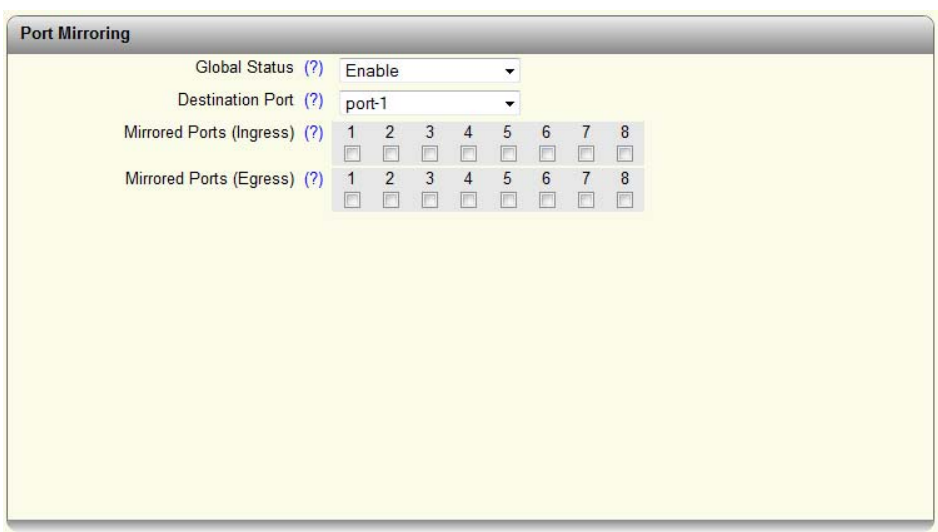



Figure 5-35 “Port Mirroring” web page

Global Status:

– Enable: port mirroring is activated globally
– Disable: port mirroring is deactivated globally

Destination Port: select the port to which the measuring device (PC) is connected here.

Mirrored Ports (Ingress): specify the ports from which the incoming data traffic should be mirrored here.

Mirrored Ports (Egress): specify the ports from which the outgoing data traffic should be mirrored here.

### 5.2.3.7 Trap Manager

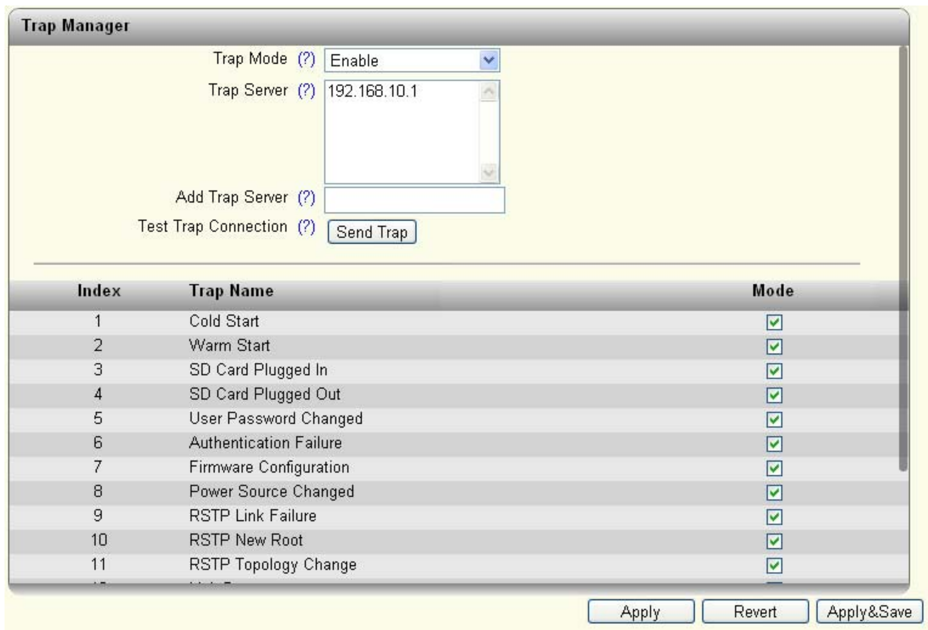



Figure 5-36 “Trap Manager” web page

Trap Mode:

– Enable: sending of SNMP traps is enabled
– Disable: sending of SNMP traps is disabled

Trap Server: all trap servers which are to receive SNMP traps from this device are displayed here.

Add Trap Server: enter the IP address of a trap server and click on “Add&Save” to create this trap server.

Test Trap Connection: the connection to the trap server is tested by clicking on the “Send Trap” button.

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

### 5.2.3.8 Port Counter

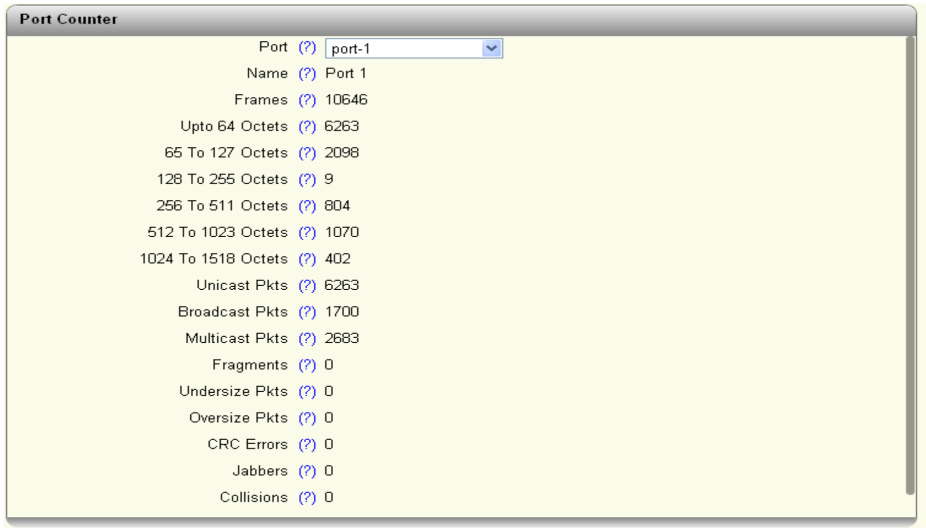



Figure 5-37 “Port Counter” web page

Here you will find an overview of the port statistics.

### 5.2.3.9 Port Utilization

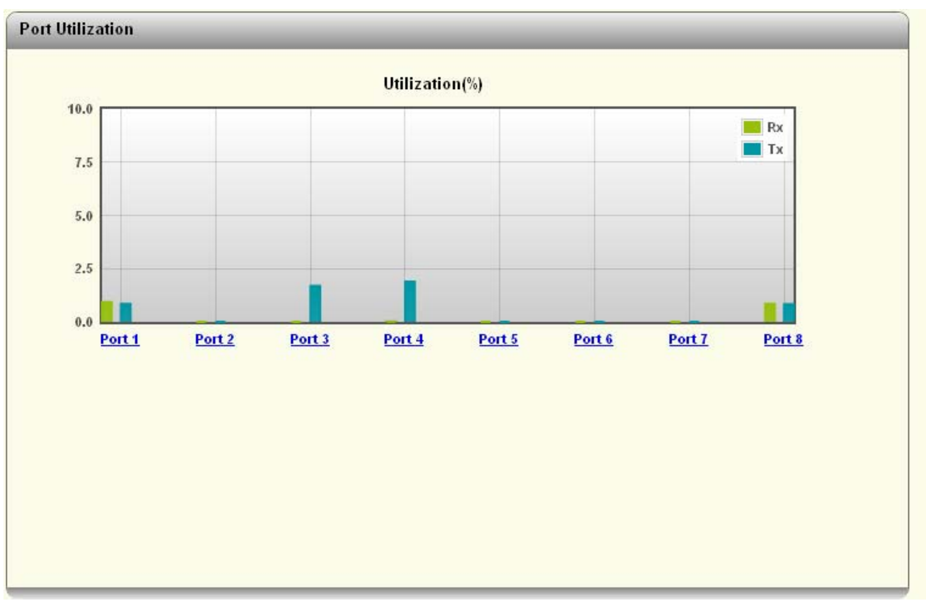
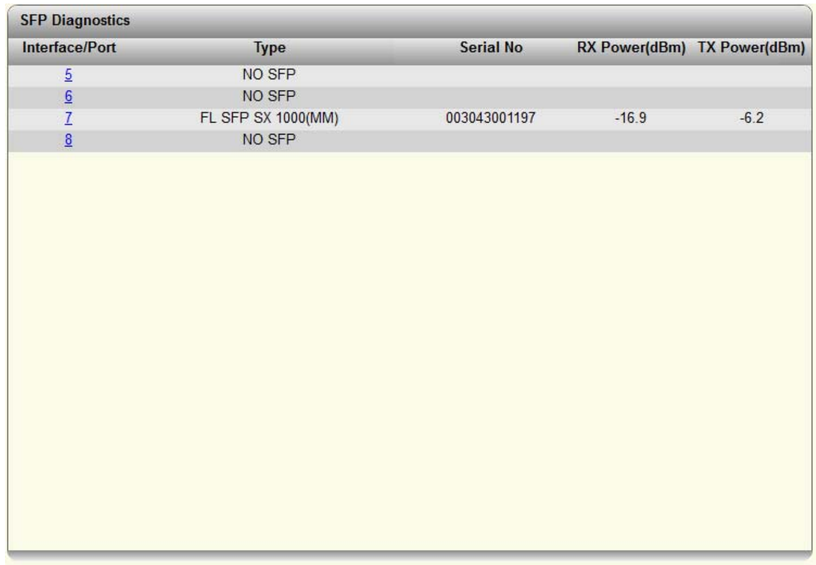



Figure 5-38 “Port Utilization” web page

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

### 5.2.3.10 SFP Diagnostics



SFP Diagnostics

| Interface/Port | Type | Serial No | RX Power(dBm) | TX Power(dBm) |
|---|---|---|---|---|
| 5 | NO SFP | | | |
| 6 | NO SFP | | | |
| 7 | FL SFP SX 1000(MM) | 003043001197 | -16.9 | -6.2 |
| 8 | NO SFP | | | |

Figure 5-39 "SFP Diagnostics" web page

Here you will find an overview of the SFP ports.

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: the serial number of the SFP module used is displayed in this column.

RX Power (dBm): the incoming power level is displayed in this column.

TX Power (dBm): the outgoing power level is displayed in this column.

# 6 Configuration and diagnostics via Command Line Interface (CLI)

## 6.1 Using the Command Line Interface (CLI)

The Command Line Interface (CLI) is a text-based tool that can be used to configure and diagnose the switch. The CLI is accessed by means of a connection via Telnet (factory default) or SSH. The configuration of the CLI service via the switch's web-based management is described in “Assigning IP parameters via BootP” on page 19.

## 6.2 Access to the CLI

The CLI is accessed via a Telnet connection (factory default) or SSH connection from a management host, e.g., a PC. For example, the Windows command prompt or the PuTTY freeware tool can be used as an input terminal.

The switch requires an IP address and a subnet mask in order to access the CLI. The configuration of the switch network parameters is described in “Assigning IP parameters via BootP” on page 19 and “Network” on page 39.

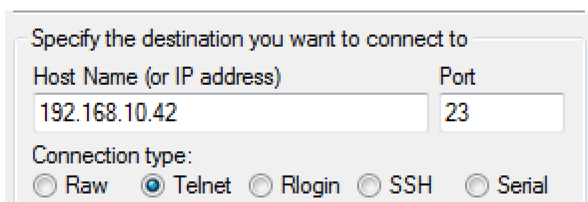



Figure 6-1 Configuration of a Telnet connection in PuTTY

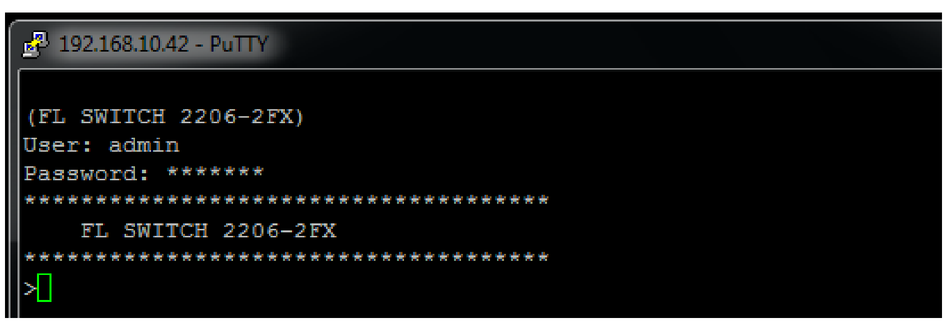



Figure 6-2 Command terminal in PuTTY


Figure 6-3 Establishing a Telnet connection via Windows command prompt


Figure 6-4 Command terminal in Windows command prompt

## 6.3 Basic principles for using CLI commands

In this section, the **CLI command names** are written in bold. *CLI parameters* are written in italics and must be replaced by appropriate values (e.g., names or numbers). If a command has several parameters, the order of these must be strictly observed.

The parameters of a command may be mandatory, optional or a selection of values (see Table “Structure of CLI commands” on page 58).

Table 6-1 Structure of CLI commands

| Symbol | Example | Description |
|---|---|---|
| < > Angle brackets | <Value> | Denotes a mandatory parameter that must be entered in place of the brackets |
| [ ] Square brackets | [Value] | Denotes an optional parameter that can be entered in place of the brackets |
| {} Braces | {choice1 \| choice2} | Denotes the mandatory selection of a value from a given list of values |
| \| Vertical bar | choice1 \| choice2 | Separates mutually exclusive selection options |
| [{}] Braces within square brackets | [{choice 1 \| choice 2}] | Denotes a selection within an optional parameter |

## 6.4 Command syntax

A command consists of one or more terms which can be followed by one or more parameters. These parameters can be mandatory or optional values.

Some commands, e.g., **show network** or **clear config**, do not require parameters. Other commands, e.g., **network parms**, require values to be specified after the command name. The parameters must be entered in the specified order, whereby optional parameters always follow mandatory parameters.

The following example illustrates the syntax using the command **network parms**:

**network parms** *<ipaddr>* *<netmask>* *[gateway]*

• **network parms** is the command name.

• *<ipaddr>* and *<netmask>* are parameters and represent mandatory values, which must be specified after the entry of the command name.

• *[gateway]* is an optional parameter, which means that a value does not have to be specified.

The following examples illustrate the correct syntax for entering the **network parms** command:

**network parms** *192.168.10.42 255.255.255.0*

**network parms** *192.168.10.42 255.255.255.0 192.168.10.0*

The following examples illustrate incorrect syntax for entering the **network parms** command:

network parms 192.168.10.42 - missing mandatory parameter

network parms 255.255.255.0 - missing mandatory parameter

network parms 255.255.255.0 192.168.10.42 - incorrect parameter sequence

## 6.5 Using the CLI Help

Entering a question mark (?) in the command prompt displays a list of all the commands currently available together with a brief description.

Table 6-2 Structure of CLI commands

| Command | Description |
|---|---|
| ? | Display available commands |

Typing a question mark (?) after each entry displays all the available command names or parameters from this point on.

```
>spanning-tree

port                    Configure spanning tree port parameter
max-age                 Configure bridge maximum aging time.
fwd-delay               Configure bridge forward delay.
hello-time              Configure bridge hello time.
bdg-prio                Configure bridge priority.
frd                     Configure fast ring detection.
lts                     Configure large tree support.
status                  Select spanning tree status.

>spanning-tree bdg-prio
```

If the Help output displays a parameter in angle brackets, this parameter must be replaced by a value. Example:

*<ipaddr>* Enter the IP address

```
>network parms

<ipaddress>             Enter IP address.

>network parms 192.168.10.43
```

If at any point there are no further command names or parameters available or further parameters are optional, the following message appears in the output prompting you to execute the command that was entered:

<cr> Press Enter to execute the command

```
>show mrp

<cr>                    Press Enter to execute the command.

>show mrp

 OK
```

## 6.6 Auto-completion of commands

The Autocomplete command is an additional way of writing a command, provided enough letters have already been entered to clearly identify the command name. As soon as enough letters have been entered, press space or TAB to automatically complete the words.

```
>spanning-tree f
 2 Possibilities:
      fwd-delay
      frd

>spanning-tree fwd-delay
```

## 6.7 Using the CLI Network Scripting UI

The CLI Network Scripting UI enables CLI commands from scripts to be loaded onto the switch via the network. This means that the switch can be configured and diagnosed using a URL via PC or from a controller. Each command that is entered is confirmed by the switch, either with OK (config commands) or by outputting the switch data (show commands).

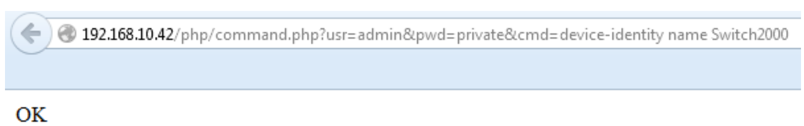
The command entry must follow a specific syntax:

http://ipaddress/php/command.php?usr=username&pwd=password&cmd=cli_command_1 | cli_command_2 | ....

The following examples illustrate the correct syntax for entering commands via the CLI Network Scripting UI:

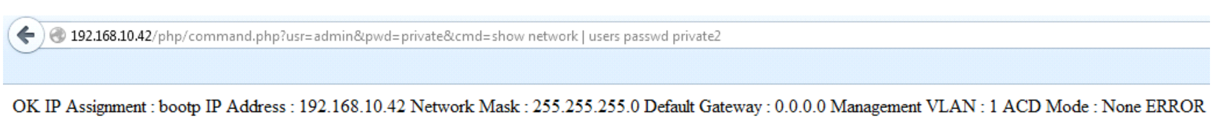
Example: changing the device name

http://192.168.10.42/php/command.php?usr=admin&pwd=private&cmd=device-identity name Switch2000




Example: displaying the network parameters and changing the user password

http://192.168.10.42/php/command.php?usr=admin&pwd=private&cmd=show network | users passwd private2



# 7 Simple Network Management Protocol (SNMP)

## 7.1 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 relevant Management Information Base (MIB), 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 by writing data from the manager to the MIB. In the event of an emergency, the agents can also send messages (traps) directly to the manager.

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

**SNMP interface**

All managed Factoryline components have an SNMP agent. The agent of 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 a MIB browser, can read and modify configuration and diagnostic data from network devices via the Simple Network Management Protocol. In addition, any SNMP tools or network management tools can be used to access Factoryline products via SNMP. To do this, the MIBs supported by the relevant device must be made available to the SNMP management tools.

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

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

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

SNMP 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 secure protocol via which the message content and the passwords are transmitted in encrypted form.

To use SNMPv3, the switch must first be configured accordingly (see “Service” on page 40). In addition, you need to change the MIB browser to SNMPv3 and create an SNMPv3 user with the following parameters:

- MD5 as the algorithm for authentication

- DES as the algorithm for privacy

- User name: “admin”

- Password: current device password (Note: the password must be at least 8 characters long. If the default password is “private”, “private_” must be used for access.).

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

### 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 a request of a manager or on the occurrence of 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. Note that the MIB is located in a firmware’s respective software package (zip file).

# 8 Link Layer Discovery Protocol (LLDP)

## 8.1 Basics

**LLDP**

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

Advantages of using LLDP:
- Improved error location detection
- Improved device replacement
- More efficient network configuration

The following information is received by or sent to neighbors, as long as LLDP is activated:
- The device transmits its own management and connection information to neighboring devices.
- The device receives management and connection information from neighboring devices.

**Displaying LLDP information**

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

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

**LLDP general**

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

**Function**

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

The information learned from the BPDUs is saved for a defined period of time 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. When the TTL elapses, the neighbor information is deleted.

> The switch manages a maximum of 50 items of neighborhood information, all other information is ignored.

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

Table 8-1 Event table for LLDP

| Event | Activity of the individual LLDP agent | Response of the neighboring LLDP agent |
|---|---|---|
| Activate LLDP agent or device startup | Transmit LLDP BPDUs to all ports | Include sender in the list of neighbors |
| Deactivate LLDP agent or software reset | Transmit LLDP BPDUs with a TTL value of 0 seconds to all ports | Delete sender from the list of neighbors |
| Link up | 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 neighborhood information | - |
| Receiving a BPDU from a new neighbor | Extend list of neighbors and respond with port-specific BPDU | Include sender in the list of neighbors |

**Link Layer Discovery Protocol**

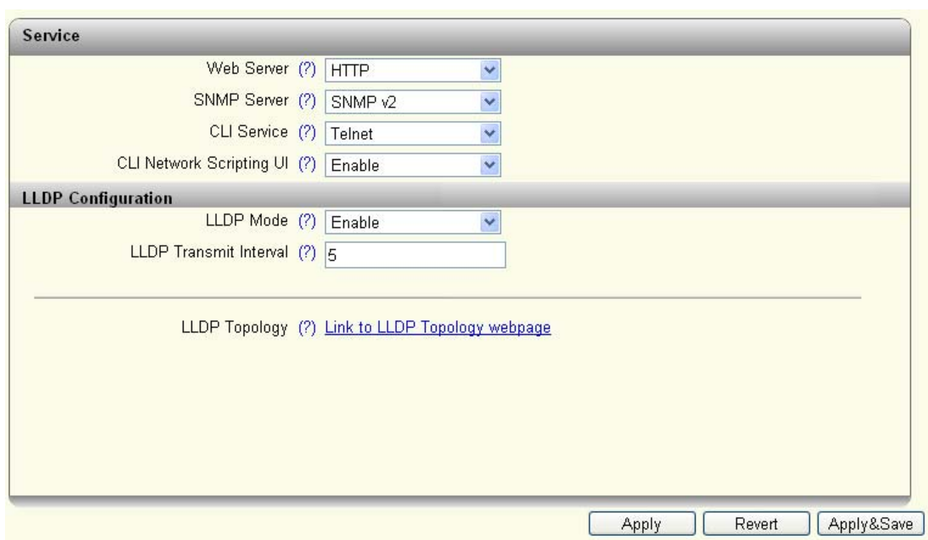
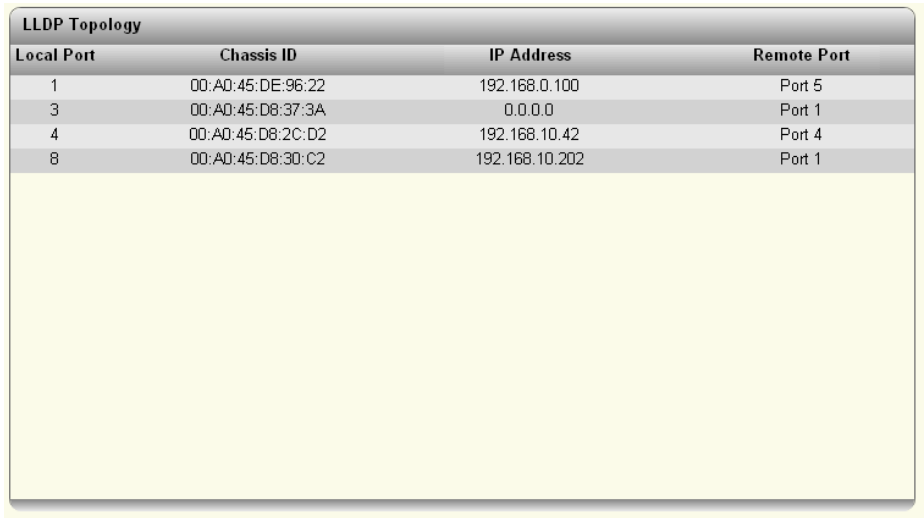



Figure 8-1 “Link Layer Discovery Protocol” web page

For devices in the 2000/2100 version, LLDP can be activated or deactivated globally for all ports. Devices in the 2200/2300 version also offer a port-based configuration option for sending and receiving LLDP telegrams.

The LLDP can be configured on the “Service” page in WBM (see “Service” on page 40).

## LLDP topology



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 8-2 “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
  Indicates the management IP address of the neighbor.
– Remote Port
  Indicates the port number of the neighboring switch that is used to connect the neighbor to the local switch.

# 9 Multicast filtering

## 9.1 Multicast Configuration

### 9.1.0.1 Multicast Filtering

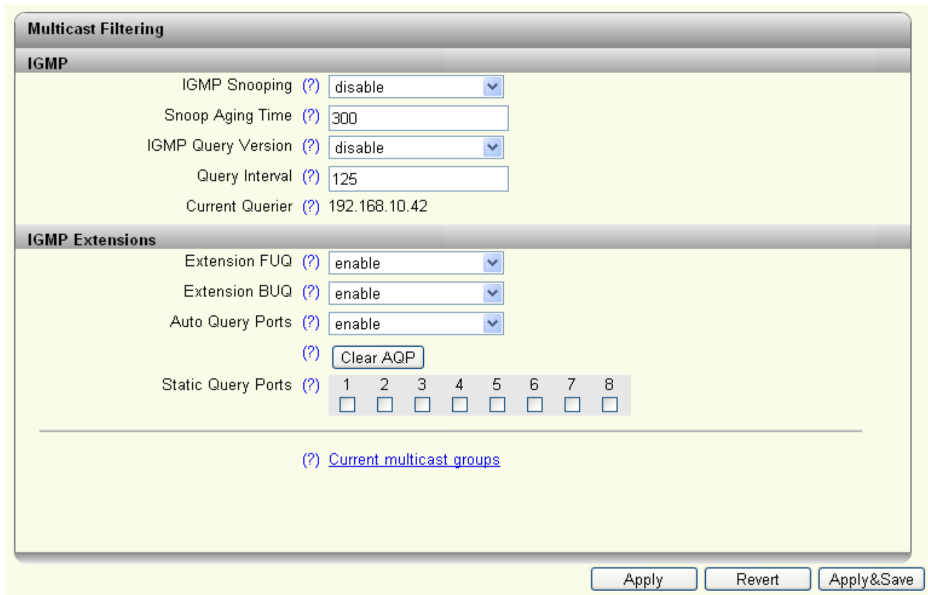



Figure 9-1 “Multicast Filtering” web page

IGMP Snooping:

– disable: the “IGMP Snooping” function is disabled
– enable: the “IGMP Snooping” function is enabled

Snoop Aging Time: the snoop aging time can be set here. 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: you can set the IGMP query version which the switch should use to send the queries here.

Query Interval: set the interval in which the switch should send the queries here.

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

Extension FUQ (Forward Unknown to Querier): select here 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): select here whether unknown multicast packets should be blocked at the querier.

Auto Query Ports: here you can set 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 which ports 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 9-2 "Current Multicast Groups" web page

# 10 Virtual Local Area Network (VLAN)

### 10.0.0.1 VLAN Configuration

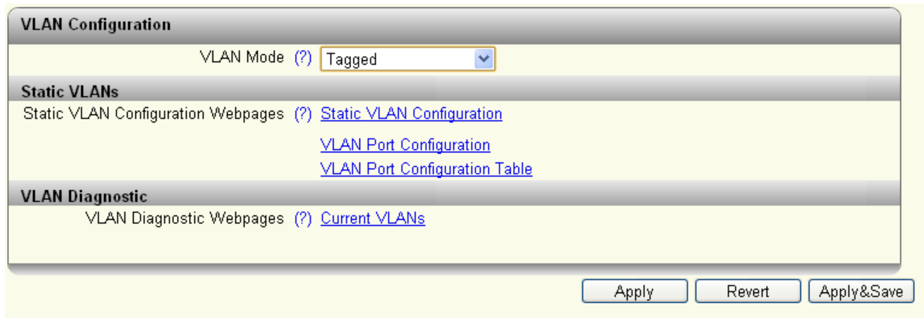



Figure 10-1 “VLAN Configuration” web page

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 depending on the VLAN assignment.

Clicking on the “Static VLAN Configuration” button takes you to the “Static VLAN Configuration” page. Up to 8 (2000/2100 version) or up to 32 (2200/2300 version) static VLANs can be set up here.

### Pop-up: Static VLAN Configuration

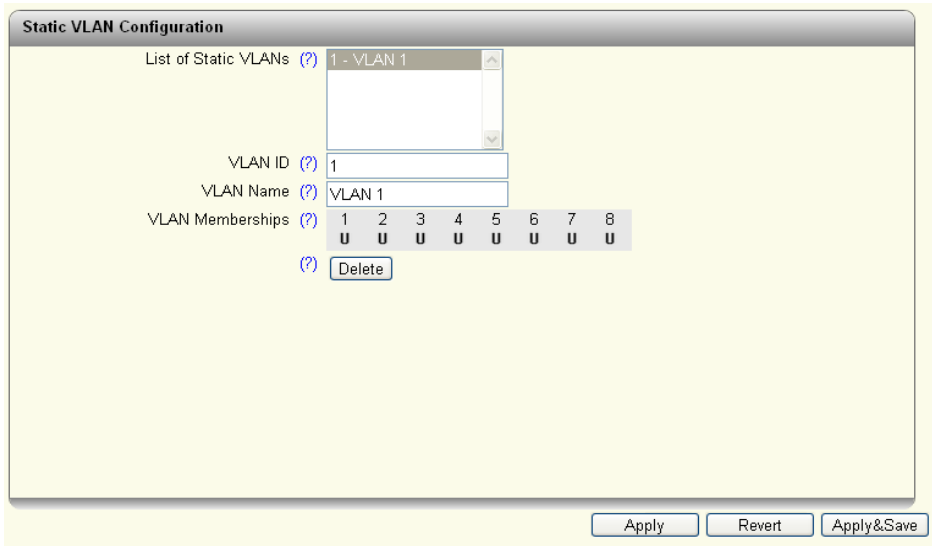



Figure 10-2 “Static VLAN Configuration” web page

List of Static VLANs: all VLANs created up to this point are displayed here.

VLAN ID: set the VLAN ID which you wish to assign to the new VLAN here. The value must be between 2 and 4094.

VLAN Name: specify the name of the VLAN which you wish to create here.

VLAN Memberships: specify which ports should 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. |

Clicking on the “VLAN port configuration” button takes you to the “VLAN Port configuration” page.

**Pop-up: VLAN Port configuration**

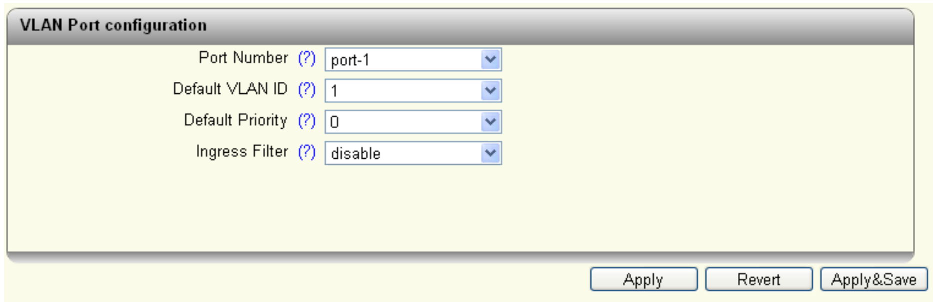



Figure 10-3 “VLAN Port configuration” web page

Port number: enter the port for which you wish to change the VLAN settings.

Default VLAN ID: set the VLAN ID to which the port should be assigned here.

Default Priority: set the VLAN priority for the selected port here.

Ingress Filter: set here whether the ingress filter should be activated.

Clicking on the “VLAN Port Table” button takes you to the VLAN port table.

**Pop-up: VLAN Port Configuration Table**

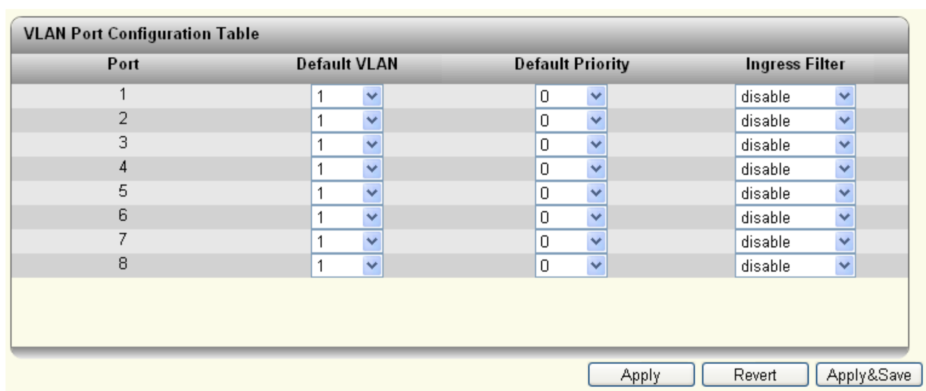



Figure 10-4 “VLAN Port Configuration Table” web page

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

### Current VLANs

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

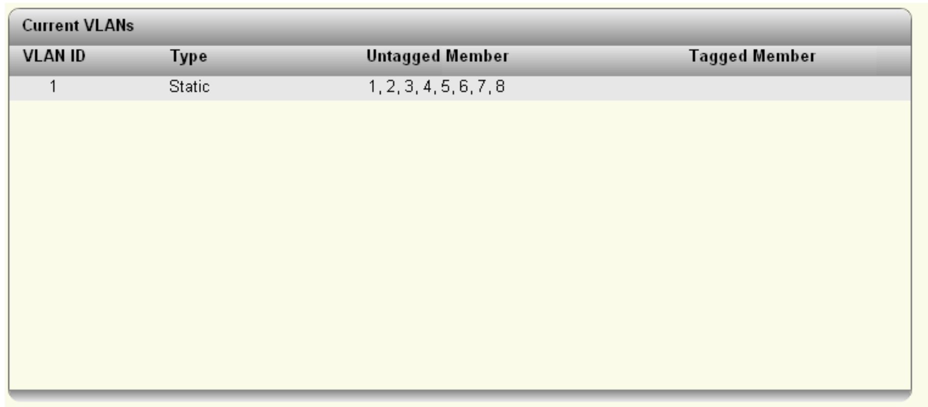



Figure 10-5 “Current VLANs” web page

# 11 Technical data and ordering data

## 11.1 Technical data for devices in the 2000 version

| General data | |
|---|---|
| Function | Ethernet/Fast Ethernet Switch; conforms to standard IEEE 802.3/802.3u |
| Switch principle | Store and forward |
| Address table | 8192 MAC addresses |
| SNMP | Version 2c, Version 3 |
| Transmission capacity per port<br>64-byte packet size, half duplex | At 10 Mbps: 14880 pps (packets per second)<br>At 100 Mbps: 148800 pps |
| Supported MIBs | MIB II and private SNMP objects from Phoenix Contact |
| Housing dimensions (width x height x depth) in mm | 45 x 130 x 115 (depth from top edge of DIN rail) |
| Permissible operating temperature | 0°C to 60°C |
| Permissible storage temperature | -40°C to +85°C |
| Degree of protection | IP20 (not assessed in compliance with UL, assessed by PTL), IEC 60529 |
| Protection class | Class 3 VDE 0106; IEC 60536, for inside use only |
| Humidity | |
| Operation | 10% to 95%, non-condensing |
| Storage | 10% to 95%, non-condensing |
| Air pressure | |
| Operation | 86 kPa to 108 kPa, 1500 m above sea level |
| Storage | 66 kPa to 108 kPa, 3500 m above sea level |
| Ambient compatibility | Free from substances that would hinder coating with paint or varnish according to VW specification |
| Mounting position | Perpendicular to a standard DIN rail |
| Connection to protective earth ground | Snapped onto a grounded DIN rail |
| Pollution degree | 2 |
| Overvoltage category | None |
| Weight | Up to 220 g, typical |

| Supply voltage (US) | |
|---|---|
| Connection | Via COMBICON; maximum conductor cross section = 1.5 $mm^2$, use copper wires that are suitable for 75°C or equivalent |
| Nominal value | 24 V DC |
| Permissible voltage range | 18 V DC to 32 V DC |
| Permissible ripple (within the permissible voltage range) | 3.6 $V_{PP}$ |
| Current consumption at US for 18 V DC, maximum | 300 mA (FL SWITCH 2005)<br>350 mA (FL SWITCH 2008) |
| Current consumption at US for 24 V DC, maximum | 165 mA (FL SWITCH 2005)<br>180 mA (FL SWITCH 2008) |
| Test voltage | 170 V DC for one minute |

| Interfaces | |
|---|---|
| Number of Ethernet ports | 5 / 8 |

| Ethernet interfaces | |
|---|---|
| **Properties of the RJ45 ports** | |
| Number | Up to 8 with auto crossing and auto negotiation |
| Connection format | 8-pos. RJ45 socket on the switch |
| Connection medium | Twisted pair cable |
| Cable impedance | 100 ohms |
| Transmission speed | 10/100 Mbps |
| Maximum network segment expansion | 100 m |

| Mechanical tests | |
|---|---|
| Shock testing according to IEC 60068-2-27 | Operation: 30g,<br>half-sine shock pulse |
| Vibration resistance according to IEC 60068-2-6 | Operation/storage/transport: 2g, 10 Hz - 150 Hz |
| Free fall according to IEC 60068-2-32 | 1 m |

| Conformance with EMC Directives | |
|---|---|
| Developed according to IEC 61000-6-2 | |
| Noise emission according to EN 55022: 1998<br>+ A1: 2000 + A2: 2003 (interference voltage) | Class A (industrial applications) |
| Noise emission according to EN 55011: 1998<br>+ A1: 1999 + A2: 2002 (electromagnetic interference) | Class A (industrial applications) |
| Noise immunity according to EN 61000-4-2 (IEC 1000-4-2) (ESD)<br>Contact discharge:<br>Air discharge:<br>Indirect discharge: | Requirements according to DIN EN 61000-6-2<br>Test intensity 3, criterion B<br>Test intensity 3, criterion A<br>Test intensity 3, criterion A |
| Noise immunity according to EN 61000-4-3 (IEC 1000-4-3)<br>(electromagnetic fields) | Requirements according to DIN EN 61000-6-2<br>Test intensity 3, criterion A |
| Noise immunity according to EN 61000-4-6 (IEC 1000-4-6) (conducted) | Requirements according to DIN EN 61000-6-2<br>Test intensity 3, criterion A |
| Noise immunity according to EN 61000-4-4 (IEC 1000-4-4) (burst)<br>Data cables:<br>Power supply: | Requirements according to DIN EN 61000-6-2<br>Test intensity 3, criterion A<br>Test intensity 3, criterion A |
| Noise immunity according to EN 61000-4-5 (IEC 1000-4-5) (surge)<br>Data cables:<br>Power supply: | Requirements according to DIN EN 61000-6-2<br>Test intensity 2, criterion A<br>Test intensity 1, criterion A |

| Additional certifications | |
|---|---|
| RoHS | |

## 11.2 Technical data for devices in the 2100 version

| General data | |
|---|---|
| Function | Ethernet/Fast Ethernet/Gigabit Switch; conforms to standard IEEE 802.3/802.3u/802.3ab |
| Switch principle | Store and forward |
| Address table | 8192 MAC addresses |

| General data | |
|---|---|
| SNMP | Version 2c, Version 3 |
| Transmission capacity per port<br>64-byte packet size, half duplex | At 10 Mbps: 14880 pps (packets per second)<br>At 100 Mbps: 148800 pps<br>At 1000 Mbps: 1488100 pps |
| Supported MIBs | MIB II and private SNMP objects from Phoenix Contact |
| Housing dimensions (width x height x depth) in mm | 45 x 130 x 115 (depth from top edge of DIN rail) |
| Permissible operating temperature | 0°C to 60°C |
| Permissible storage temperature | -40°C to +85°C |
| Degree of protection | IP20 (not assessed in compliance with UL, assessed by PTL), IEC 60529 |
| Protection class | Class 3 VDE 0106; IEC 60536, for inside use only |
| Humidity | |
| Operation | 10% to 95%, non-condensing |
| Storage | 10% to 95%, non-condensing |
| Air pressure | |
| Operation | 86 kPa to 108 kPa, 1500 m above sea level |
| Storage | 66 kPa to 108 kPa, 3500 m above sea level |
| Ambient compatibility | Free from substances that would hinder coating with paint or varnish according to VW specification |
| Mounting position | Perpendicular to a standard DIN rail |
| Connection to protective earth ground | Snapped onto a grounded DIN rail |
| Pollution degree | 2 |
| Overvoltage category | None |
| Weight | Up to 240 g, typical |

| Supply voltage (US) | |
|---|---|
| Connection | Via COMBICON; maximum conductor cross section = 1.5 mm2, use copper wires that are suitable for 75°C or equivalent |
| Nominal value | 24 V DC |
| Permissible voltage range | 18 V DC to 32 V DC |
| Permissible ripple (within the permissible voltage range) | 3.6 $V_{PP}$ |
| Current consumption at US for 18 V DC, maximum | 350 mA (FL SWITCH 2105)<br>400 mA (FL SWITCH 2108) |
| Current consumption at US for 24 V DC, maximum | 225 mA (FL SWITCH 2105)<br>275 mA (FL SWITCH 2108) |
| Test voltage | 170 V DC for one minute |

| Interfaces | |
|---|---|
| Number of Ethernet ports | 5 / 8 |

| Ethernet interfaces | |
|---|---|
| **Properties of the RJ45 ports** | |
| Number | Up to 8 with auto crossing and auto negotiation |
| Connection format | 8-pos. RJ45 socket on the switch |
| Connection medium | Twisted pair cable |

| Ethernet interfaces (Fortsetzung) | |
|---|---|
| Cable impedance | 100 ohms |
| Transmission speed | 10/100/1000 Mbps |
| Maximum network segment expansion | 100 m |

| Mechanical tests | |
|---|---|
| Shock testing according to IEC 60068-2-27 | Operation: 30g,<br>half-sine shock pulse |
| Vibration resistance according to IEC 60068-2-6 | Operation/storage/transport: 2g, 10 Hz - 150 Hz |
| Free fall according to IEC 60068-2-32 | 1 m |

| Conformance with EMC Directives | |
|---|---|
| Developed according to IEC 61000-6-2 | |
| Noise emission according to EN 55022: 1998<br>+ A1: 2000 + A2: 2003 (interference voltage) | Class A (industrial applications) |
| Noise emission according to EN 55011: 1998<br>+ A1: 1999 + A2: 2002 (electromagnetic interference) | Class A (industrial applications) |
| Noise immunity according to EN 61000-4-2 (IEC 1000-4-2) (ESD) | Requirements according to DIN EN 61000-6-2 |
| Contact discharge: | Test intensity 3, criterion B |
| Air discharge: | Test intensity 3, criterion A |
| Indirect discharge: | Test intensity 3, criterion A |
| Noise immunity according to EN 61000-4-3 (IEC 1000-4-3)<br>(electromagnetic fields) | Requirements according to DIN EN 61000-6-2<br>Test intensity 3, criterion A |
| Noise immunity according to EN 61000-4-6 (IEC 1000-4-6) (conducted) | Requirements according to DIN EN 61000-6-2<br>Test intensity 3, criterion A |
| Noise immunity according to EN 61000-4-4 (IEC 1000-4-4) (burst) | Requirements according to DIN EN 61000-6-2 |
| Data cables: | Test intensity 3, criterion A |
| Power supply: | Test intensity 3, criterion A |
| Noise immunity according to EN 61000-4-5 (IEC 1000-4-5) (surge) | Requirements according to DIN EN 61000-6-2 |
| Data cables: | Test intensity 2, criterion A |
| Power supply: | Test intensity 1, criterion A |

| Additional certifications | |
|---|---|
| RoHS | @EEE 2002/95/EC - WEEE 2002/96/EC<br>CE |

## 11.3 Technical data for devices in the 2200 version

| General data | |
|---|---|
| Function | Ethernet/Fast Ethernet Switch; conforms to standard IEEE 802.3/802.3u |
| Switch principle | Store and forward |
| Address table | 8192 MAC addresses |
| SNMP | Version 2c, Version 3 |
| Transmission capacity per port<br>64-byte packet size, half duplex | At 10 Mbps: 14880 pps (packets per second)<br>At 100 Mbps: 148800 pps |
| Supported MIBs | MIB II and private SNMP objects from Phoenix Contact |
| Housing dimensions (width x height x depth) in mm | 45 x 130 x 115 (depth from top edge of DIN rail) |

| General data | |
|---|---|
| Permissible operating temperature | -40°C to 70°C |
| Permissible storage temperature | -40°C to +85°C |
| Degree of protection | IP20 (not assessed in compliance with UL, assessed by PTL), IEC 60529 |
| Protection class | Class 3 VDE 0106; IEC 60536, for inside use only |
| Humidity | |
| Operation | 10% to 95%, non-condensing |
| Storage | 10% to 95%, non-condensing |
| Air pressure | |
| Operation | 68 kPa to 108 kPa, 3000 m above sea level |
| Storage | 66 kPa to 108 kPa, 3500 m above sea level |
| Ambient compatibility | Free from substances that would hinder coating with paint or varnish according to VW specification |
| Mounting position | Perpendicular to a standard DIN rail |
| Connection to protective earth ground | Snapped onto a grounded DIN rail |
| Pollution degree | 2 |
| Overvoltage category | None |
| Weight | Up to 260 g, typical |

| Supply voltage (US1/US2 redundant) | |
|---|---|
| Connection | Via COMBICON; maximum conductor cross section = 1.5 $mm^2$, use copper wires that are suitable for 75°C or equivalent |
| Nominal value | 24 V DC |
| Permissible ripple (within the permissible voltage range) | 3.6 $V_{PP}$ |
| Permissible voltage range | **9 V DC** to 57 V DC for the following devices<br>FL SWITCH 2205<br>FL SWITCH 2208<br>FL SWITCH 2207-FX<br>FL SWITCH 2207-FX SM<br>FL SWITCH 2206-2FX<br>FL SWITCH 2206-2FX SM<br>FL SWITCH 2206-2FX ST<br>FL SWITCH 2206-2FX SM ST |
| Permissible voltage range | **12 V DC** to 57 V DC for the following devices<br>FL SWITCH 2204-2TC-2SFX<br>FL SWITCH 2206-2SFX |
| Current consumption at US for **9 V DC**, maximum (without digital output) | 1.2 A (FL SWITCH 2205)<br>1.3 A (FL SWITCH 2208)<br>1.4 A (FL SWITCH 2207-FX)<br>1.4 A (FL SWITCH 2207-FX SM)<br>1.5 A (FL SWITCH 2206-2FX)<br>1.5 A (FL SWITCH 2206-2FX SM)<br>1.5 A (FL SWITCH 2206-2FX ST)<br>1.5 A (FL SWITCH 2206-2FX SM ST) |

| Supply voltage (US1/US2 redundant) (Fortsetzung) | |
|---|---|
| Current consumption at US for **12 V DC**, maximum (without digital output) | 1.4 A (FL SWITCH 2204-2TC-2SFX)<br>1.4 A (FL SWITCH 2206-2SFX) |
| Current consumption at US for 24 V DC, maximum (without digital output) | 170 mA (FL SWITCH 2205)<br>190 mA (FL SWITCH 2208)<br>220 mA (FL SWITCH 2207-FX)<br>220 mA (FL SWITCH 2207-FX SM)<br>260 mA (FL SWITCH 2206-2FX)<br>260 mA (FL SWITCH 2206-2FX SM)<br>260 mA (FL SWITCH 2206-2FX ST)<br>260 mA (FL SWITCH 2206-2FX SM ST)<br>250 mA (FL SWITCH 2204-2TC-2SFX)<br>230 mA (FL SWITCH 2206-2SFX) |
| Test voltage | 170 V DC for one minute |

| Interfaces | |
|---|---|
| Number of Ethernet ports | 5 / 8 |
| Digital alarm output | |
| Voltage | 12 - 58 V DC |
| Current carrying capacity | 100 mA, typical/0.7 A, maximum (1 minute) |

| Ethernet interfaces | |
|---|---|
| **Properties of the RJ45 ports** | |
| Number | Up to 8 with auto crossing and auto negotiation |
| Connection format | 8-pos. RJ45 socket on the switch |
| Connection medium | Twisted pair cable |
| Cable impedance | 100 ohms |
| Transmission speed | 10/100 Mbps |
| Maximum network segment expansion | 100 m |
| **Properties of the fiberglass ports** | |
| Number | Up to 2 |
| Connection format | SC/ST/SFX format (depending on the device used) |
| Connection medium | Fiberglass |
| Connecting plug | SC/ST/LC format (depending on the device used) |
| Transmission speed | 100 Mbps |
| Maximum network segment expansion | Depends on the SFP module/fiber type used |
| Fiber type | Depends on the SFP module/fiber type used |
| Laser protection class | 1 |
| Wavelength | 850/1310 nm (depending on the device/SFP module used) |
| **Properties of the combo ports** | |
| Number | Up to 2 |
| Transmission speed | 100 Mbps |
| Wavelength | Depends on the SFP module used |
| Maximum transmission length | Depends on the SFP module used |

| Mechanical tests | |
|---|---|
| Shock testing according to IEC 60068-2-27 | Operation: 30g,<br>half-sine shock pulse |
| Vibration resistance according to IEC 60068-2-6 | Operation/storage/transport: 5g, 10 Hz - 150 Hz |
| Free fall according to IEC 60068-2-32 | 1 m |

| Conformance with EMC Directives | |
|---|---|
| Developed according to IEC 61000-6-2 | |
| Noise emission according to EN 55022: 1998<br>+ A1: 2000 + A2: 2003 (interference voltage) | Class A (industrial applications) |
| Noise emission according to EN 55011: 1998<br>+ A1: 1999 + A2: 2002 (electromagnetic interference) | Class A (industrial applications) |
| Noise immunity according to EN 61000-4-2 (IEC 1000-4-2) (ESD)<br>Contact discharge:<br>Air discharge:<br>Indirect discharge: | Requirements according to DIN EN 61000-6-2<br>Test intensity 3, criterion B<br>Test intensity 3, criterion A<br>Test intensity 3, criterion A |
| Noise immunity according to EN 61000-4-3 (IEC 1000-4-3)<br>(electromagnetic fields) | Requirements according to DIN EN 61000-6-2<br>Test intensity 3, criterion A |
| Noise immunity according to EN 61000-4-6 (IEC 1000-4-6) (conducted) | Requirements according to DIN EN 61000-6-2<br>Test intensity 3, criterion A |
| Noise immunity according to EN 61000-4-4 (IEC 1000-4-4) (burst)<br>Data cables:<br>Power supply: | Requirements according to DIN EN 61000-6-2<br>Test intensity 3, criterion A<br>Test intensity 3, criterion A |
| Noise immunity according to EN 61000-4-5 (IEC 1000-4-5) (surge)<br>Data cables:<br>Power supply: | Requirements according to DIN EN 61000-6-2<br>Test intensity 2, criterion A<br>Test intensity 1, criterion A |

| Additional certifications | |
|---|---|
| RoHS | @EEE 2002/95/EC - WEEE 2002/96/EC<br>IECEx:<br>IEC 60079-0:2011, 6th Edition<br>IEC 60079-15:2010, 4th Edition<br>ATEX:<br>EN 60079-0:2012+A11:2013<br>EN 60079-15:2010<br>Field of application:<br>II 3 G Ex nA IIC T4 Gc<br>IECEx ULD 16.0018X<br>CE |

## 11.4 Technical data for devices in the 2300 version

| General data | |
|---|---|
| Function | Ethernet/Fast Ethernet/Gigabit Switch; conforms to standard<br>IEEE 802.3/802.3u/802.3ab |
| Switch principle | Store and forward |
| Address table | 8192 MAC addresses |

| General data | |
|---|---|
| SNMP | Version 2c, Version 3 |
| Transmission capacity per port<br>64-byte packet size, half duplex | At 10 Mbps: 14880 pps (packets per second)<br>At 100 Mbps: 148800 pps<br>At 1000 Mbps: 1488100 pps |
| Supported MIBs | MIB II and private SNMP objects from Phoenix Contact |
| Housing dimensions (width x height x depth) in mm | 45 x 130 x 115 (depth from top edge of DIN rail) |
| Permissible operating temperature | -40°C to 70°C |
| Permissible storage temperature | -40°C to +85°C |
| Degree of protection | IP20 (not assessed in compliance with UL, assessed by PTL), IEC 60529 |
| Protection class | Class 3 VDE 0106; IEC 60536, for inside use only |
| Humidity | |
| Operation | 10% to 95%, non-condensing |
| Storage | 10% to 95%, non-condensing |
| Air pressure | |
| Operation | 53 kPa to 108 kPa, 5000 m above sea level |
| Storage | 53 kPa to 108 kPa, 5000 m above sea level |
| Ambient compatibility | Free from substances that would hinder coating with paint or varnish according to VW specification |
| Mounting position | Perpendicular to a standard DIN rail |
| Connection to protective earth ground | Snapped onto a grounded DIN rail |
| Pollution degree | 2 |
| Overvoltage category | None |
| Weight | Up to 310 g, typical |

| Supply voltage (US1/US2 redundant) | |
|---|---|
| Connection | Via COMBICON; maximum conductor cross section = 1.5 mm$^2$, use copper wires that are suitable for 75°C or equivalent |
| Nominal value | 24 V DC |
| Permissible voltage range | 12 V DC to 57 V DC |
| Permissible ripple (within the permissible voltage range) | 3.6 $V_{PP}$ |
| Current consumption at US for 12 V DC, maximum | 1.4 A (FL SWITCH 2308)<br>1.5 A (FL SWITCH 2304-2GC-2SFP)<br>1.5 A (FL SWITCH 2306-2SFP) |
| Current consumption at US for 24 V DC, maximum | 280 mA (FL SWITCH 2308)<br>290 mA (FL SWITCH 2304-2GC-2SFP)<br>280 mA (FL SWITCH 2306-2SFP) |
| Test voltage | 170 V DC for one minute |

| Interfaces | |
|---|---|
| Number of Ethernet ports | 8 |
| Digital alarm output | |
| Voltage | 12 - 57 V DC |
| Current carrying capacity | 100 mA, maximum 700 mA / 1 minute |

## Ethernet interfaces

| | |
|---|---|
| **Properties of the RJ45 ports** | |
| Number | Up to 8 with auto crossing and auto negotiation |
| Connection format | 8-pos. RJ45 socket on the switch |
| Connection medium | Twisted pair cable |
| Cable impedance | 100 ohms |
| Transmission speed | 10/100/1000 Mbps |
| Maximum network segment expansion | 100 m |
| **Properties of the fiberglass ports** | |
| Number | Up to 2 |
| Connection format | Gigabit SFP format |
| Connection medium | Fiberglass |
| Connecting plug | LC format (SFP module) |
| Transmission speed | 100/1000 Mbps (depending on the SFP module used) |
| Maximum network segment expansion | Depends on the SFP module/fiber type used |
| Fiber type | Depends on the SFP module used |
| Laser protection class | 1 |
| Wavelength | 850/1310/1550 nm (depending on the device/SFP module used) |
| **Properties of the combo ports** | |
| Number | Up to 2 |
| Transmission speed | 100/1000 Mbps |
| Wavelength | Depends on the SFP module used |
| Maximum transmission length | Depends on the SFP module used |

## Mechanical tests

| | |
|---|---|
| Shock testing according to IEC 60068-2-27 | Operation: 30g,<br>half-sine shock pulse |
| Vibration resistance according to IEC 60068-2-6 | Operation/storage/transport: 5g, 10 Hz - 150 Hz |
| Free fall according to IEC 60068-2-32 | 1 m |

## Conformance with EMC Directives

| | |
|---|---|
| Developed according to IEC 61000-6-2 | |
| Noise emission according to EN 55022: 1998<br>+ A1: 2000 + A2: 2003 (interference voltage) | Class A (industrial applications) |
| Noise emission according to EN 55011: 1998<br>+ A1: 1999 + A2: 2002 (electromagnetic interference) | Class A (industrial applications) |
| Noise immunity according to EN 61000-4-2 (IEC 1000-4-2) (ESD)<br>Contact discharge:<br>Air discharge:<br>Indirect discharge: | Requirements according to DIN EN 61000-6-2<br>Test intensity 3, criterion B<br>Test intensity 3, criterion A<br>Test intensity 3, criterion A |
| Noise immunity according to EN 61000-4-3 (IEC 1000-4-3)<br>(electromagnetic fields) | Requirements according to DIN EN 61000-6-2<br>Test intensity 3, criterion A |

| Conformance with EMC Directives | |
|---|---|
| Noise immunity according to EN 61000-4-6 (IEC 1000-4-6) (conducted) | Requirements according to DIN EN 61000-6-2<br>Test intensity 3, criterion A |
| Noise immunity according to EN 61000-4-4 (IEC 1000-4-4) (burst)<br>Data cables:<br>Power supply: | Requirements according to DIN EN 61000-6-2<br>Test intensity 3, criterion A<br>Test intensity 3, criterion A |
| Noise immunity according to EN 61000-4-5 (IEC 1000-4-5) (surge)<br>Data cables:<br>Power supply: | Requirements according to DIN EN 61000-6-2<br>Test intensity 2, criterion A<br>Test intensity 1, criterion A |

| Additional certifications | |
|---|---|
| RoHS | @EEE 2002/95/EC - WEEE 2002/96/EC<br>IECEx:<br>IEC 60079-0:2011, 6th Edition<br>IEC 60079-15:2010, 4th Edition<br><br>ATEX:<br>EN 60079-0:2012+A11:2013<br>EN 60079-15:2010<br><br>Field of application:<br>II 3 G Ex nA IIC T4 Gc<br>IECEx ULD 16.0018X<br>CE |

| Differences between this version and previous versions of the user manual | |
|---|---|
| Rev. 00: initial version | |
| Rev. 01: devices added | |

## 11.5 Ordering data

### Products

| Description | Order designation | Order No. | Pcs./Pkt. |
|---|---|---|---|
| Managed Switch with five 10/100 Mbps RJ45 ports | FL SWITCH 2005 | 2702323 | 1 |
| Managed Switch with eight 10/100 Mbps RJ45 ports | FL SWITCH 2008 | 2702324 | 1 |
| Managed Switch with five 10/100/1000 Mbps RJ45 ports | FL SWITCH 2105 | 2702665 | 1 |
| Managed Switch with eight 10/100/1000 Mbps RJ45 ports | FL SWITCH 2108 | 2702666 | 1 |
| Managed Switch with five 10/100 Mbps RJ45 ports | FL SWITCH 2205 | 2702326 | 1 |
| Managed Switch with eight 10/100 Mbps RJ45 ports | FL SWITCH 2208 | 2702327 | 1 |
| Managed Switch with seven 10/100 Mbps RJ45 ports and one FO port in SC format for multimode | FL SWITCH 2207-FX | 2702328 | 1 |
| Managed Switch with seven 10/100 Mbps RJ45 ports and one FO port in SC format for single mode | FL SWITCH 2207-FX SM | 2702329 | 1 |
| Managed Switch with six 10/100 Mbps RJ45 ports and two FO ports in SC format for multimode | FL SWITCH 2206-2FX | 2702330 | 1 |
| Managed Switch with six 10/100 Mbps RJ45 ports and two FO ports in SC format for single mode | FL SWITCH 2206-2FX SM | 2702331 | 1 |
| Managed Switch with six 10/100 Mbps RJ45 ports and two FO ports in ST format for multimode | FL SWITCH 2206-2FX ST | 2702332 | 1 |
| Managed Switch with six 10/100 Mbps RJ45 ports and two FO ports in ST format for single mode | FL SWITCH 2206-2FX SM ST | 2702333 | 1 |
| Managed Switch with four 10/100 Mbps RJ45 ports, two SFX combo ports, and two SFX ports | FL SWITCH 2204-2TC-2SFX | 2702334 | 1 |
| Managed Switch with six 10/100 Mbps RJ45 ports and two SFX ports | FL SWITCH 2206-2SFX | 2702969 | 1 |
| Managed Switch with eight 10/100/1000 Mbps RJ45 ports | FL SWITCH 2308 | 2702652 | 1 |
| Managed Switch with six 10/100/1000 Mbps RJ45 ports and two SFP ports | FL SWITCH 2306-2SFP | 2702970 | 1 |
| Managed Switch with four 10/100/1000 Mbps RJ45 ports, two Gigabit combo ports, and two SFP ports | FL SWITCH 2304-2GC-2SFP | 2702653 | 1 |

### Accessories

| Description | Order designation | Order No. | Pcs./Pkt. |
|---|---|---|---|
| Program and configuration memory, plug-in, 2 Gbytes | SD FLASH 2GB | 2988162 | 1 |
| Program and configuration memory, plug-in, with MRP master license (MRM), 2 Gbytes | FL SD FLASH/MRM | 2700270 | 1 |
| FL Network Manager, SNMP-based configuration and firmware update software, for easy startup of Managed Switches | FL NETWORK MANAGER BASIC | 2702889 | 1 |
| Universal end bracket | E/NS 35 N | 0800886 | 1 |
| Gigabit SFP module for transmission up to 30 km with a wavelength of 1310 nm | FL SFP LX | 2891767 | 1 |
| Gigabit SFP module for transmission up to 1 km with a wavelength of 850 nm | FL SFP SX | 2891754 | 1 |
| Gigabit SFP module for transmission up to 80 km with a wavelength of 1550 nm | FL SFP LX LH | 2989912 | 1 |
| Gigabit SFP module for transmission up to 100 m | FL SFP GT | 2989420 | 1 |
| Gigabit SFP module for transmission up to 2 km with a wavelength of 1310 nm | FL SFP SX2 | 2702397 | 1 |
| The narrow form-factor plug-in module provides a fiber optic interface with a data transmission speed of 100 Mbps with a wavelength of 1310 nm (long) | FL SFP FX | 2891081 | 1 |
| The narrow form-factor plug-in module provides a fiber optic interface with a data transmission speed of 100 Mbps with a wavelength of 1310 nm (long). | FL SFP FX SM | 2891082 | 1 |
| Fast Ethernet SFP WDM module for transmission up to a maximum of 20 km on a single fiber with a wavelength of 1310/1550 nm | FL SFP FE WDM20-A | 2702437 | 1 |

| Description (Fortsetzung) | Order designation | Order No. | Pcs./Pkt. |
|---|---|---|---|
| Fast Ethernet SFP WDM module for transmission up to a maximum of 20 km on a single fiber with a wavelength of 1550/1310 nm. | FL SFP FE WDM20-B | 2702438 | 1 |
| Fast Ethernet SFP WDM set for transmission up to a maximum of 20 km on a single fiber with a wavelength of 1310/1550 nm | FL SFP FE WDM20-SET | 2702439 | 1 |
| Gigabit SFP WDM module for transmission up to a maximum of 10 km on a single fiber with a wavelength of 1310/1550 nm | FL SFP WDM10-A | 2702440 | 1 |
| Gigabit SFP WDM module for transmission up to a maximum of 10 km on a single fiber with a wavelength of 1310/1550 nm | FL SFP WDM10-B | 2702441 | 1 |
| Gigabit SFP WDM set for transmission up to a maximum of 10 km on a single fiber with a wavelength of 13101/1550 nm | FL SFP WDM10-SET | 2702442 | 1 |
| The FL DIN RA is installed in a standard, 19-inch rack (EIA-310-D, IEC 60297-3-100) to allow DIN rail mounted equipment to be rack mounted | FL DIN RA | 2891053 | 1 |
| Network monitoring with HMI/SCADA systems | FL SNMP OPC SERVER V3 | 2701139 | 1 |
| PCB connector, plug, nominal current: 8 A, rated voltage (III/2): 160 V, number of positions: 5, pitch: 3.81 mm, connection method: screw connection with tension sleeve, color: gray, contact surface: tin | MCVW 1.5/ 5-ST-3.81 GY BD-GND | 1715127 | |
| PCB connector, plug, nominal current: 8 A, rated voltage (III/2): 160 V, number of positions: 5, pitch: 3.81 mm, connection method: screw connection with tension sleeve, color: gray, contact surface: tin | MCVW 1.5/ 5-ST-3.81 GY BD-D0 | 1715126 | |
| PCB connector, plug, nominal current: 8 A, rated voltage (III/2): 160 V, number of positions: 5, pitch: 3.81 mm, connection method: Push-in spring connection, color: gray, contact surface: tin | FK-MCP 1,5/ 5-ST-3,81 GY | 1884005 | |
| PCB connector, plug, nominal current: 8 A, rated voltage (III/2): 160 V, number of positions: 5, pitch: 3.81 mm, connection method: Push-in spring connection, color: green, contact surface: tin | FMC 1,5/ 5-ST-3,81 | 1745920 | |
| SNMP-based software in English, for detection and display of Ethernet networks with a maximum of 64 network nodes | FL VIEW 64 | 2701472 | 1 |
| SNMP-based software in English, for detection and display of Ethernet networks with a maximum of 256 network nodes | FL VIEW 256 | 2701473 | 1 |
| SNMP-based software in English, for detection and display of Ethernet networks with a maximum of 512 network nodes | FL VIEW 512 | 2701474 | 1 |
| Fuse terminal block for cartridge fuse-link, cross section: 0.5 - 16 $mm^2$, AWG: 24 - 6, width: 12 mm, color: black | UK 10-DREHSILED 24 (5X20) | 3005138 | 50 |
| Lever-type fuse terminal block, black, for 5 x 20 mm cartridge fuse-links, with LED for 24 V DC | UT 4-HESILED 24 (5X20) | 3046090 | 50 |
| Thermomagnetic circuit breaker, 1-pos., for DIN rail mounting, 2 A | UT 6-TMC M 2A | 0916605 | 6 |
| Pre-assembled relay module with Push-in connection, consisting of: relay base with ejector and power contact relay. Contact type: 1 changeover contact. Input voltage: 24 V DC | RIF-0-RPT-24DC/21 | 2903370 | 1 |
| FO patch cable, multimode, preconfigured, 1.0 m long, LC-LC connector | FL MM PATCH 1,0 LC-LC | 2989158 | 1 |
| FO patch cable, single mode, preconfigured, 1.0 m long, LC-LC connector | FL SM PATCH 1,0 LC-LC | 2989187 | 1 |
| FO patch cable, multimode, preconfigured, 1.0 m long, LC-SC connector | FL MM PATCH 1,0 LC-SC | 2989161 | 1 |
| FO patch cable, multimode, preconfigured, 1.0 m long, SC-SC connector | FL MM PATCH 1,0 SC-SC | 2901805 | 1 |
| FO patch cable, multimode, preconfigured, 1.0 m long, SC-ST connector | FL MM PATCH 1,0 SC-ST | 2901809 | 1 |
| FO patch cable, single mode, preconfigured, 1.0 m long, LC-SC connector | FL SM PATCH 1,0 LC-SC | 2989190 | 1 |
| FO patch cable, single mode, preconfigured, 1.0 m long, SC-SC connector | FL SM PATCH 1,0 SC-SC | 2901829 | 1 |
| FO patch cable, single mode, preconfigured, 1.0 m long, SC-ST connector | FL SM PATCH 1,0 SC-ST | 2901832 | 1 |
| Patch cable, CAT**6**, pre-assembled, 1.0 m long | FL CAT6 PATCH 1,0 | 2891385 | 10 |
| Patch cable, CAT5, pre-assembled, 1.0 m long | FL CAT5 PATCH 1,0 | 2832276 | 10 |

**HOTLINE:**

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

☎ + 49 5281 9-462888

# A Appendix for document lists

## A 1 List of figures

### Section 1



### Section 2



### Section 3



### Section 4

### Section 5

## Section 6

## Section 7

## Section 8



## Section 9



## Section 10



## Section 11

## Appendix A

## B 2 List of tables

## C 3 Index

T



U



V