FL SWITCH 7000

User manual

Order No. —

PHOENIX CONTACT
INSPIRING INNOVATIONS

User manual
FL SWITCH 7000

2014-03-26

Designation: UM EN FL SWITCH 7000

Revision: 00

Order No.: —

This user manual is valid for:

Designation	Version	Order No.
FL SWITCH 7008-EIP		2701418
FL SWITCH 7006/2FX-EIP		2701419
FL SWITCH 7005/FX-2FXSM-EIP		2701420

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.

Table of contents

1 Factoryline SWITCH 7000 range

1.1 ?Properties and versions

The Managed Switch from the 7000 series is an Ethernet switch which is suitable for industrial applications. It is available in the following versions:

– With eight 10/100 Mbps RJ45 ports (FL SWITCH 7008-EIP)
– With six 10/100 Mbps RJ45 ports and two fiber optic ports in SC format for multi mode (FL SWITCH 7006/2FX-EIP)
– With five 10/100 Mbps RJ45 ports, one fiber optic port in SC format for multi mode, and two fiber optic ports in SC format for single mode (FL SWITCH 7005/FX-2FXSM-EIP)

1.1.1 Dimensions of the FL SWITCH 7000

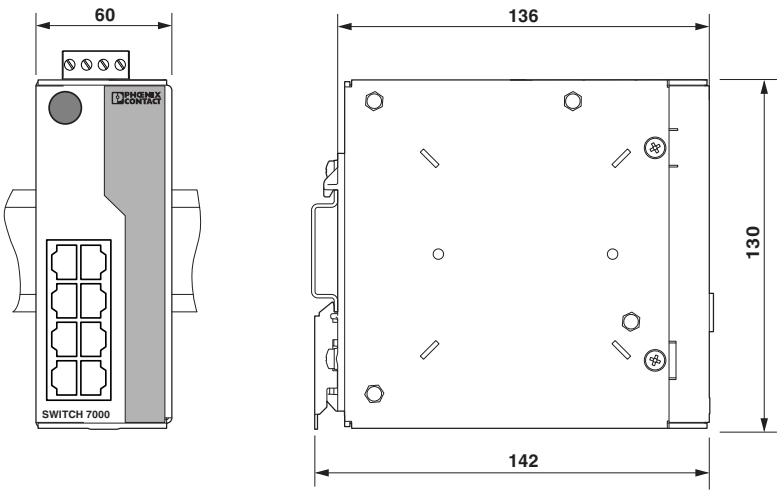


Figure 1-1 Housing dimensions

1.1.2 Elements of the devices

Figure 1-2 Elements of the devices

Number	Meaning
1	Multi-mode fiberglass ports
2	RJ45 ports
3	Slot for optional SD card
4	Diagnostics and status indicators
5	MODE switch with LEDs
6	Diagnostics and status indicators
7	Connection for the supply voltage
8	Connection for the floating signal contacts
9	Multi-mode fiberglass port
10	Single-mode fiberglass ports

1.1.3 Status and diagnostics 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	Green	On	Supply voltage 2 within the tolerance range
		Off	Supply voltage 2 too low
FAIL	Red	On	Signal contact open, i.e., an error has occurred
		Off	Signal contact closed, i.e., an error has not occurred
Each port has a Link LED located on the front of the device.			
LNK (Link)	Green	On	Link active
		Off	Link not active
Each port has an additional LED located on the front of the device. The function of the second LED (MOD) for each port can be set using the MODE button. There are three options (during the boot process the mode and port LEDs are permanently on):			
ACT (Activity)	Green	On	Transmitting/receiving telegrams
		Flashing	The device has no valid IP address
		Off	Not transmitting/receiving telegrams
SPD (Speed)	Green	On	100 Mbps
		Off	10 Mbps if Link LED is active
FD (Duplex)	Green	On	Full duplex
		Off	Half duplex if Link LED is active
ACT/SPD/FD	Green	Flashing	Switch is in Smart mode (see “Using Smart mode” on page 17)
LEDs for Ethernet/IP			
NET	Green/red	Off	Supply voltage not present or no IP parameters configured
		On (green)	CIP connection active
		Flashing (green)	IP parameter configured, no active CIP connection
		On (red)	The device has detected an IP address conflict
		Flashing (red)	An “Exclusive Owner” connection has run into a timeout
		Flashing (Red/green)	The device carries out a “Power on Selftest - POST”

Des.	Color	Status	Meaning
MOD	Green/red	Off	Supply voltage not present
		On (green)	The device is operating correctly
		Flashing (green)	The device is not configured
		On (red)	The device has an irreversible error
		Flashing (red)	The device has an irreversible error
		Flashing (Red/green)	The device carries out a “Power on Selftest - POST”

2 Mounting and installation

2.1 Mounting and removing the SWITCH 7000

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).

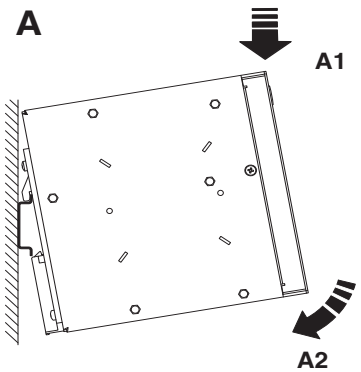


Figure 2-1 Snapping the device onto the DIN rail

1 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).

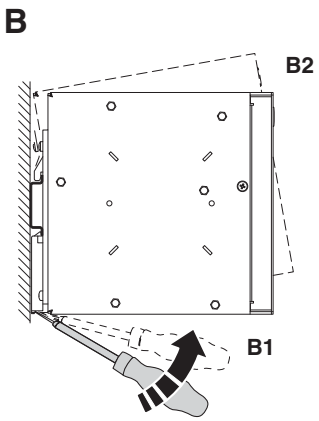


Figure 2-2 Removing the device

2.2 Installing the SWITCH 7000

2.2.1 Connecting the supply voltage

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

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

Operation with one power supply

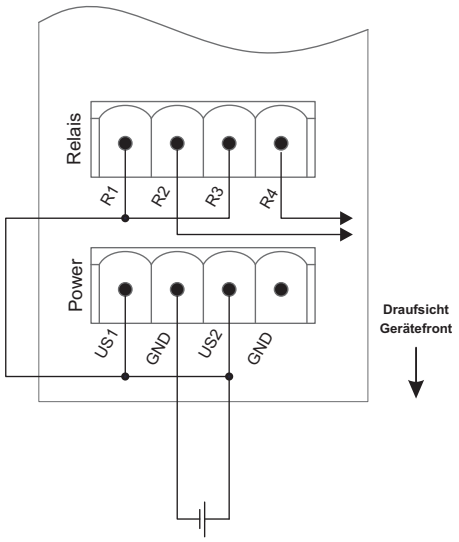


Figure 2-3 Operating the device with one power supply (example)

Redundant operation with two power supplies

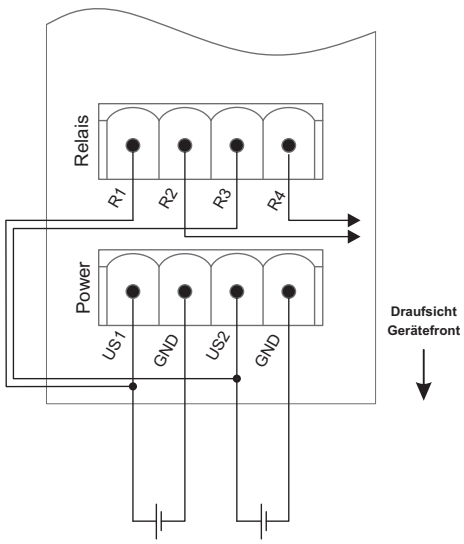


Figure 2-4 Redundant operation with two power supplies

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

2.2.2 Signal contact/assignment of the RJ45 connectors

Signal contact

The device has two floating signal contacts. An error is indicated when the contact is opened.

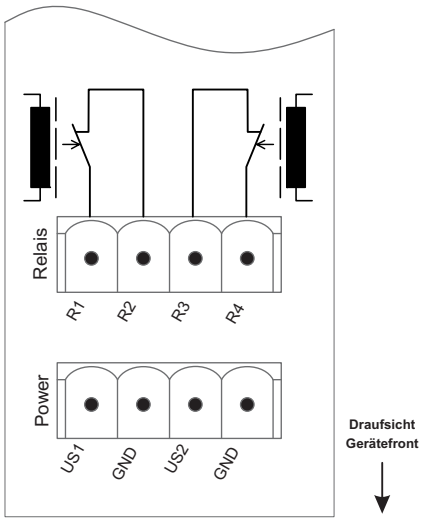


Figure 2-5 Basic circuit diagram for the signal contact

The indicated error states are configured in web-based management or via SNMP.

In the event of a non-redundant voltage supply, the switch indicates the voltage supply failure by opening the signal contact. This error message can be prevented by connecting the supply voltage to both US1/US2 terminal blocks in parallel, as shown in Figure 2-3, or by deactivating redundant power supply monitoring in web-based management or via SNMP.

2.2.3 Assignment of the RJ45 Ethernet connectors

Table 2-1 Pin assignment of RJ45 connectors (MDI)

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

2.2.4 Grounding

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

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

3 Startup and function

3.1 Basic settings

3.1.1 Delivery state/default settings

By default or after the system is reset to the default settings, the following functions and properties are set:

- The username is: “admin”
- The password is: “private”
- All IP parameters are deleted. The switch has no valid IP address.
- The RJ45 ports available are set to auto negotiation and auto crossing.
- All counters of the SNMP agents are reset.
- The web server and SNMP are activated.
- Port mirroring and Rapid Spanning Tree are deactivated.
- The switch is in the “EtherNet/IP” operating mode.
- The alarm contacts open in the event of a non-redundant power supply and missing SD card.
- BootP for assigning IP parameters is activated.
- The MAC address table contains no entries.
- LLDP is activated.

3.2 Using Smart mode

The 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:

- Activating Universal mode
- Resetting the IP configuration
- Activating the EtherNet/IP mode (default setting)
- Operating with a static IP address

3.2.1 Activating Smart mode

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

3.2.1.1 Calling Smart mode

- Following the switch boot phase, as soon as the three mode LEDs **go out**, press and hold down the mode button for more than five seconds. If Smart mode is active, the three LEDs (ACT, SPD and FD) will flash.
- When Smart mode is started, the switch is initially in the “Exit without changes” state.

3.2.1.2 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).

3.2.1.3 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.

3.2.1.4 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	ACT LED 1	SPD LED 2	FD LED 3
Exit Smart mode without changes	Off	Off	**On**
Setting the Universal mode	Off	**On**	Off
Resetting the IP configuration	**On**	**On**	**On**
Setting the EtherNet/IP mode (default setting)	**On**	Off	Off
Operation with default IP address	**On**	**On**	Off

3.3 Frame switching

The switch operates in store-and-forward mode. When receiving a data packet, the switch analyzes the source and destination addresses. The switch stores up to 16386 MAC addresses in its address table with an adjustable aging time of 10 to 825 seconds.

3.3.1 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.

3.3.2 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 16386 addresses. This is important if more than one termination device is connected to one or more ports. Several independent subnetworks can be connected to one switch.

3.3.3 Learning addresses

The switch independently learns the addresses for termination devices, which are connected via a port, by evaluating the source addresses in the data telegrams. When the switch receives a data telegram, it only forwards this data telegram to the port that connects to the specified device (if the address could be learned beforehand).
The switch can learn up to 16386 addresses and store them in its table. The switch monitors the age of the learned addresses. The switch automatically deletes from its address table address entries that 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 to 825 seconds. For static configuration, an aging time of 300 seconds is recommended.

3.3.4 Prioritization

The switch supports eight priority queues for adjusting the internal packet processing sequence (traffic classes according to IEEE 802.1D). 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.

3.3.4.1 Class of Service - CoS

Class of Service refers to a mechanism used to take into consideration the value of the priority field (value 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.

3.3.4.2 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 (in general, in a preferred way). QoS can be used, e.g., to guarantee a transmission bandwidth for individual data streams. The switch uses QoS in connection with prioritization.

4 Configuration and diagnostics

4.1 Assigning IP parameters via BootP

BootP is activated by default.

In EtherNet/IP mode, the device still continues to send BootP requests, even after receipt of an valid IP address.

For IP address assignment, the device uses the BootP protocol. On the Internet, numerous BootP servers are available. You can use any of these programs for address assignment.

This section explains IP address assignment using the “IP Assignment Tool” Windows software (IPAssign.exe). This software can be downloaded free of charge at phoenixcontact.net/products.

Notes for BootP

During initial startup, the device transmits 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 receiving a BootP reply, the device no longer sends BootP requests. After restarting, the device sends three BootP requests and will only then accept the old IP address if there is no BootP response.

4.1.1 Assigning the IP address using IPAssign.exe

Requirements

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

Step 1: downloading and executing the program

- On the Internet, select the link phoenixcontact.net/products.
- Follow further instructions in order to access the search field.
- Enter order number 2701094 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 “Run”.

Step 2: “IP Assignment Wizard”

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

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

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

- Click on “Next”.

Step 3: “IP Address Request Listener”

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

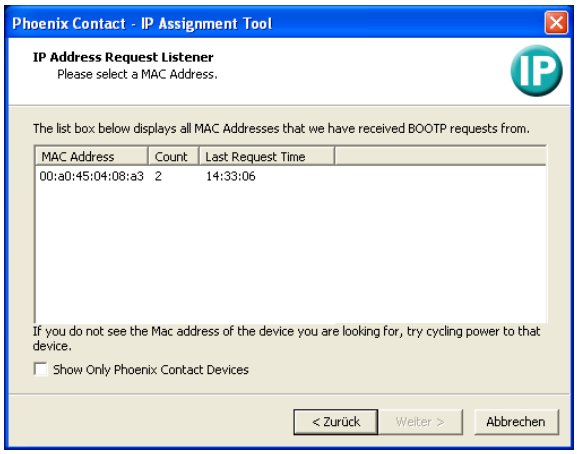


Figure 4-1 “IP Address Request Listener” window

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

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

Step 4: “Set IP Address”

The following information is displayed in the window which opens:

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

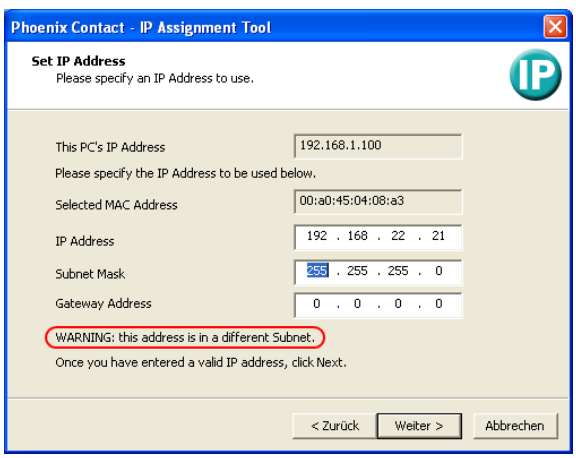


Figure 4-2 “Set IP Address” window with incorrect settings

- Adjust the IP parameters according to your requirements.

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

- Click on “Next”.

Step 5: “Assign IP address”

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

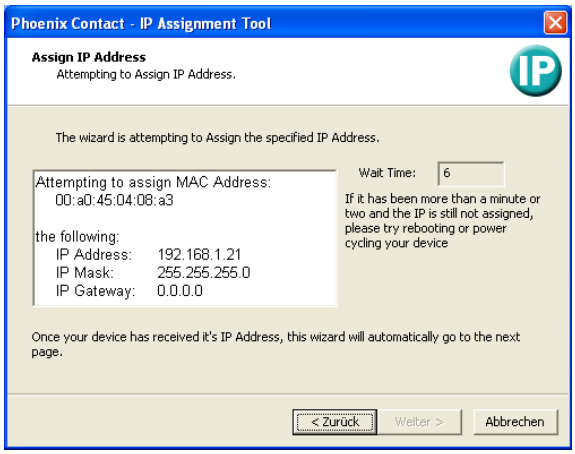


Figure 4-3 “Assign IP Address” window

Following successful transmission, the next window opens.

Step 6: finishing IP address assignment

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

To assign IP parameters for additional devices:

- Click on “Back”.

To exit IP address assignment:

- Click on “Finish”.

If required, the IP parameters set here can be changed on the web interface under ““Network Configuration” web page” on page 32.

4.2 Operating with a default IP address

For operation with a default IP address, the device receives 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 Section “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 Section “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”.
6. Set the desired IP address via web-based management.

4.3 Web-based management

The user-friendly web-based management interface can be used to manage the switch from anywhere in the network using a standard browser (e.g., Internet Explorer 8/9). 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 on 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.

4.3.1 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”. 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 8.0 or 9.0.

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

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 4-4 Login window

4.3.2 Functions/information in WBM

The WBM is split into the following areas:

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

Figure 4-5 “Help & Documentation” web page

Information -> Help

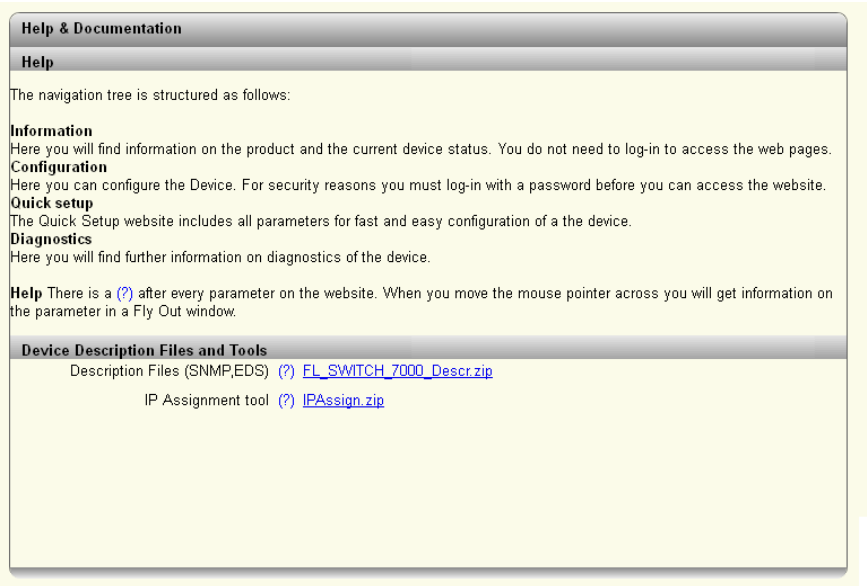
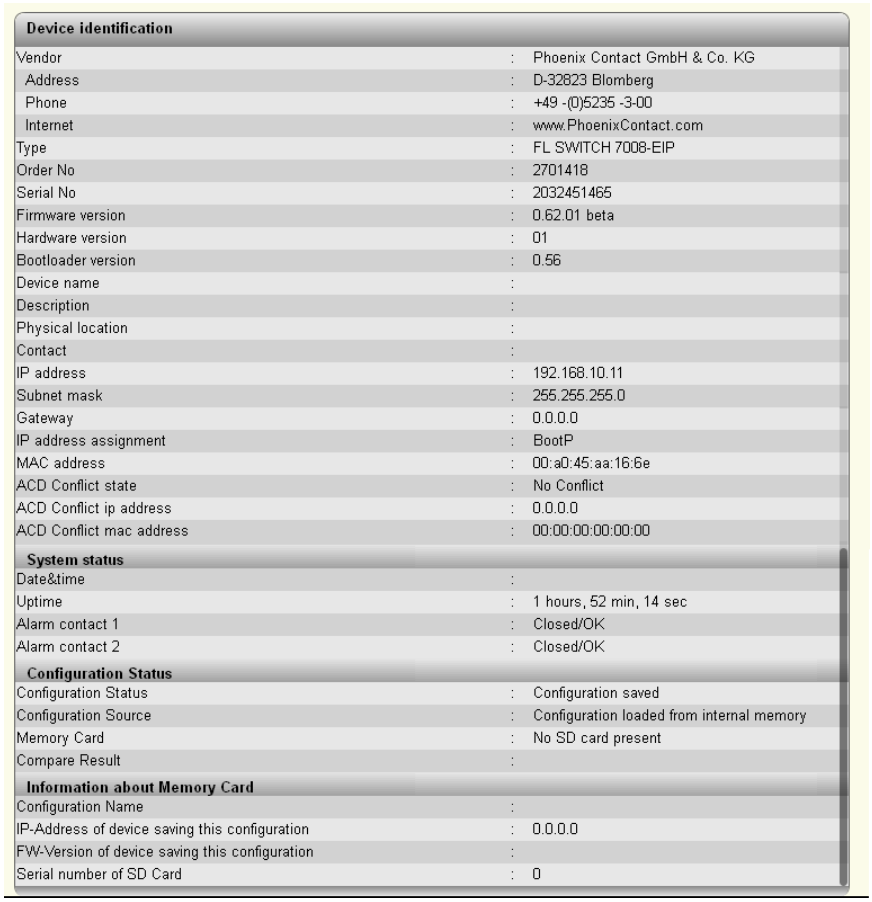


Figure 4-6 “Help” web page

“Device status/Device identification” web page

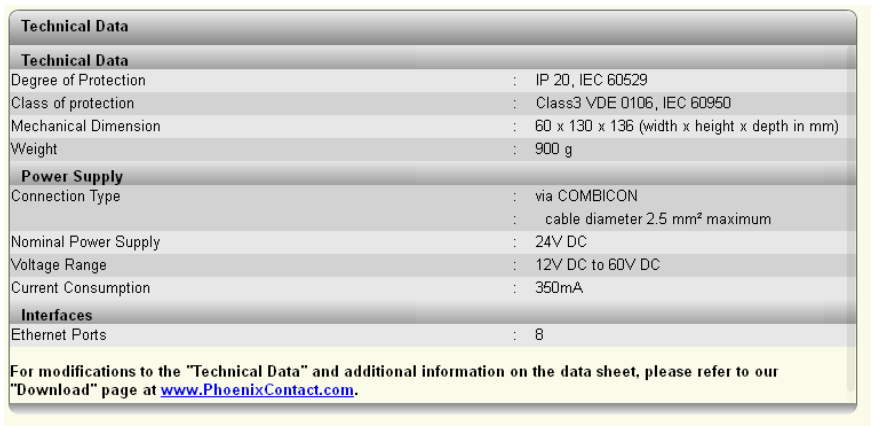
Here you will find general information about your device, such as the serial number, firmware version or hardware version.



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 7008-EIP
Order No	:	2701418
Serial No	:	2032451465
Firmware version	:	0.62.01 beta
Hardware version	:	01
Bootloader version	:	0.56
Device name	:	
Description	:	
Physical location	:	
Contact	:	
IP address	:	192.168.10.11
Subnet mask	:	255.255.255.0
Gateway	:	0.0.0.0
IP address assignment	:	BootP
MAC address	:	00:a0:45:aa:16:6e
ACD Conflict state	:	No Conflict
ACD Conflict ip address	:	0.0.0.0
ACD Conflict mac address	:	00:00:00:00:00:00
System status		
Date&time	:	
Uptime	:	1 hours, 52 min, 14 sec
Alarm contact 1	:	Closed/OK
Alarm contact 2	:	Closed/OK
Configuration Status		
Configuration Status	:	Configuration saved
Configuration Source	:	Configuration loaded from internal memory
Memory Card	:	No SD card present
Compare Result	:	
Information about Memory Card		
Configuration Name	:	
IP-Address of device saving this configuration	:	0.0.0.0
FW-Version of device saving this configuration	:	
Serial number of SD Card	:	0

Figure 4-7 “Device identification” web page

“Technical Data” web page



Technical Data		
Technical Data		
Degree of Protection	:	IP 20, IEC 60529
Class of protection	:	Class3 VDE 0106, IEC 60950
Mechanical Dimension	:	60 x 130 x 136 (width x height x depth in mm)
Weight	:	900 g
Power Supply		
Connection Type	:	via COMBICON
	:	cable diameter 2.5 mm² maximum
Nominal Power Supply	:	24V DC
Voltage Range	:	12V DC to 60V DC
Current Consumption	:	350mA
Interfaces		
Ethernet Ports	:	8

For modifications to the "Technical Data" and additional information on the data sheet, please refer to our "Download" page at www.PhoenixContact.com.

Figure 4-8 “Technical Data” web page

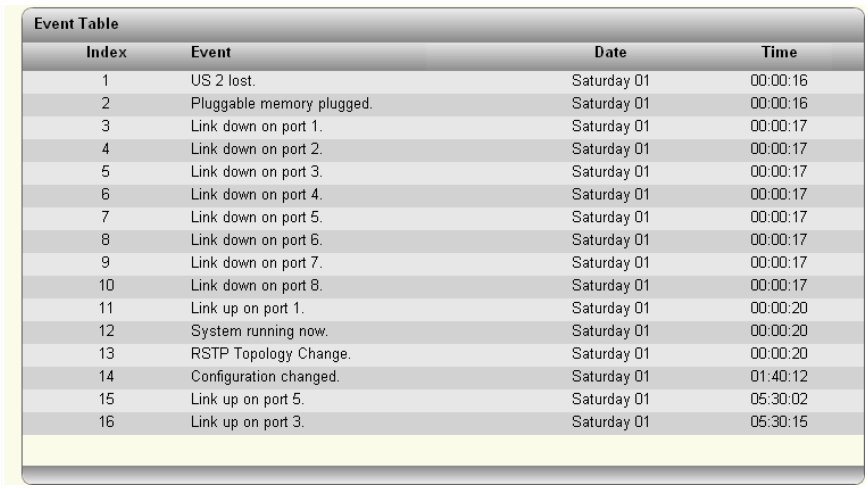
Here you will find the technical data for your device, such as specifications for the voltage supply.

“Local Diagnostics” web page

Local Diagnostics		
Power Supply		
US1	:	Supply Voltage 1 (green LED)
US2	:	Supply Voltage 2 (green LED)
Alarm contact		
FAIL	:	Alarm Contact open (red LED)
Ethernet		
LNK	:	Link (green LED)
	:	There is a link LED for each port.
ACT	:	Activity (green LED)
FD	:	Full Duplex (green LED)
SPD	:	10/100 Mbit/s (LED off/green)
Ethernet/IP		
NET	:	No IP Address (LED OFF)
	:	No Active Connection (green LED flashing)
	:	Active Connection (green LED)
	:	Connection Timeout (red LED Flashing)
	:	Address Conflict Detected (red LED)
MOD	:	Ethernet/IP mode (green LED)
	:	Recoverable minor fault (red LED flashing)
	:	Non-recoverable major fault (red LED)

Figure 4-9 “Local Diagnostics” web page

“Alarm & Events” web page



Event Table

Index	Event	Date	Time
1	US 2 lost.	Saturday 01	00:00:16
2	Pluggable memory plugged.	Saturday 01	00:00:16
3	Link down on port 1.	Saturday 01	00:00:17
4	Link down on port 2.	Saturday 01	00:00:17
5	Link down on port 3.	Saturday 01	00:00:17
6	Link down on port 4.	Saturday 01	00:00:17
7	Link down on port 5.	Saturday 01	00:00:17
8	Link down on port 6.	Saturday 01	00:00:17
9	Link down on port 7.	Saturday 01	00:00:17
10	Link down on port 8.	Saturday 01	00:00:17
11	Link up on port 1.	Saturday 01	00:00:20
12	System running now.	Saturday 01	00:00:20
13	RSTP Topology Change.	Saturday 01	00:00:20
14	Configuration changed.	Saturday 01	01:40:12
15	Link up on port 5.	Saturday 01	05:30:02
16	Link up on port 3.	Saturday 01	05:30:15

Figure 4-10 “Alarm & Events” web page

The entries in the “Event Table” are also retained after powerup. The “Event Table” can be downloaded from the device in CSV format.

“Port Table” web page

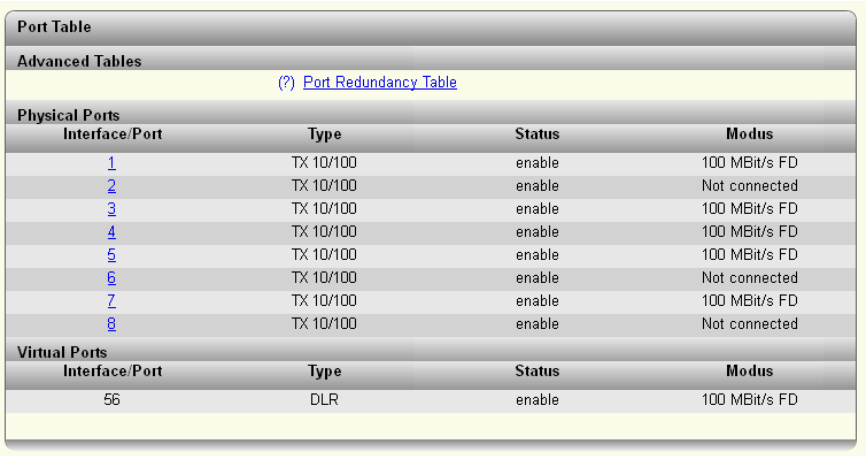


Figure 4-11 “Port Table” web page

“MAC Address Table” web page

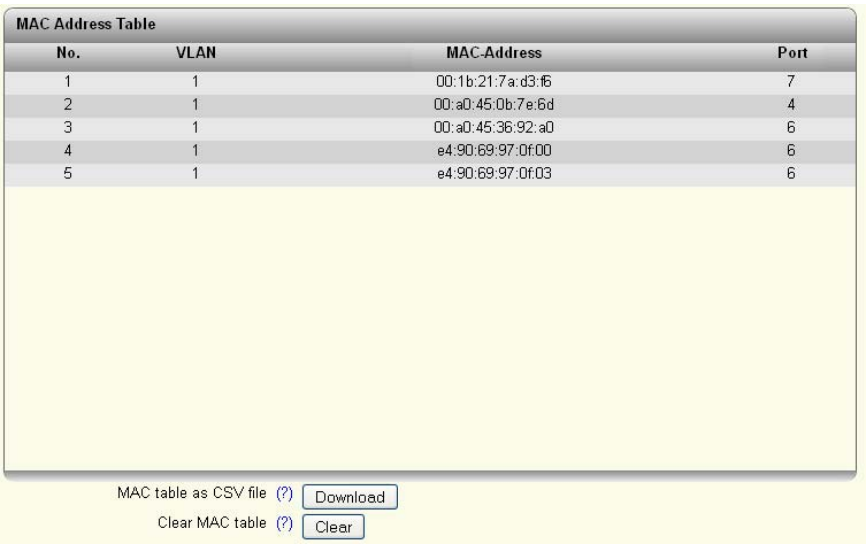


Figure 4-12 “MAC Address Table” web page

“Configuration/System” web page

Reset device

Figure 4-13 “Reset device” configuration area

Reset device: The device restarts.

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

Firmware update

By clicking on the “Update firmware” button, a window opens in which the parameters for the firmware update must be entered.

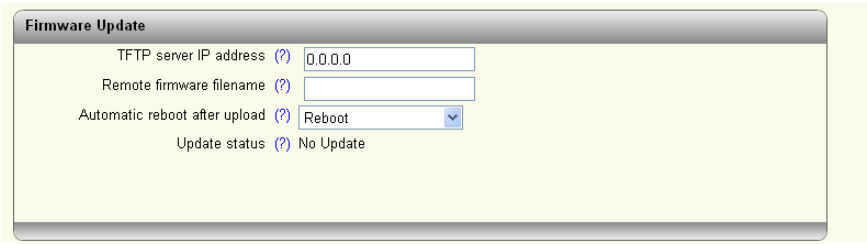


Figure 4-14 “Firmware Update” configuration area

TFTP server IP address
Here you should set the IP address of the computer on which the TFTP server is active.

Remote firmware filename
Here you should set the name of the firmware file which is to be transferred to the device.

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

Configuration handling

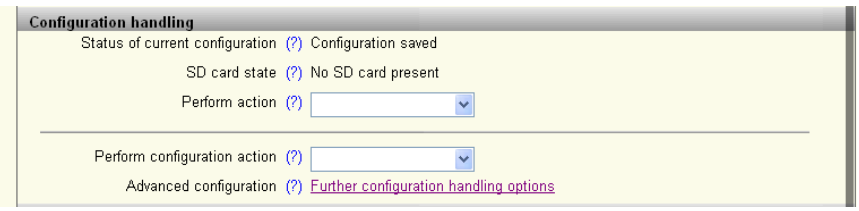


Figure 4-15 “Configuration handling” configuration area

Status of current configuration: Indicates the configuration status on the device.

SD card state: Indicates the status of the SD card in the device.

Performance action: Here you can select whether the configuration saved on the SD card is to be compared with the configuration saved on the device or whether the SD card is to be deleted.

Performance configuration action:

– Factory default: Resets the device to the delivery state.
– Save configuration: Saves the configuration.
– Reload configuration: The configuration is loaded from the card to the device.

By clicking on “Further configuration handling options”, you can access the extended settings for saving the configuration.

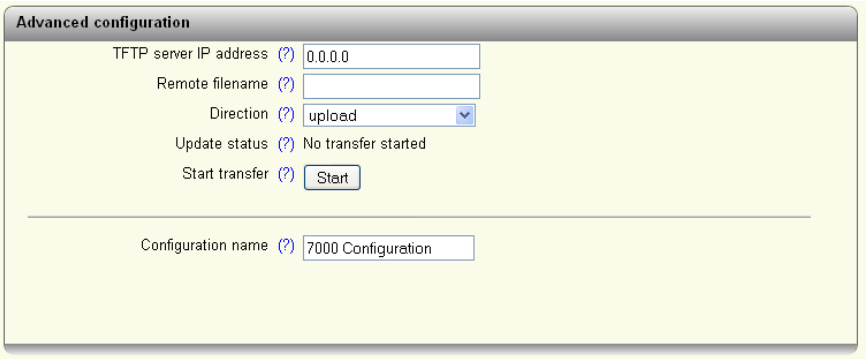


Figure 4-16 “Advanced configuration” configuration area

TFTP server IP address: Here you should enter the IP address at which the TFTP server can be reached.

Remote filename: Here you should set the name of the file to be uploaded or downloaded.

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

Update status: Shows the current transfer status.

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

Configuration name: Here you should enter the name under which the configuration is saved on the PC.

Administrator password

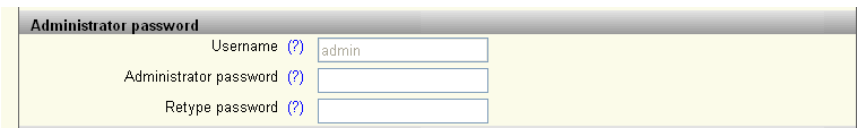


Figure 4-17 “Administrator password” configuration area

You can change the administrator password here. The new password must be between 8 and 14 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.

“Quick setup” web page

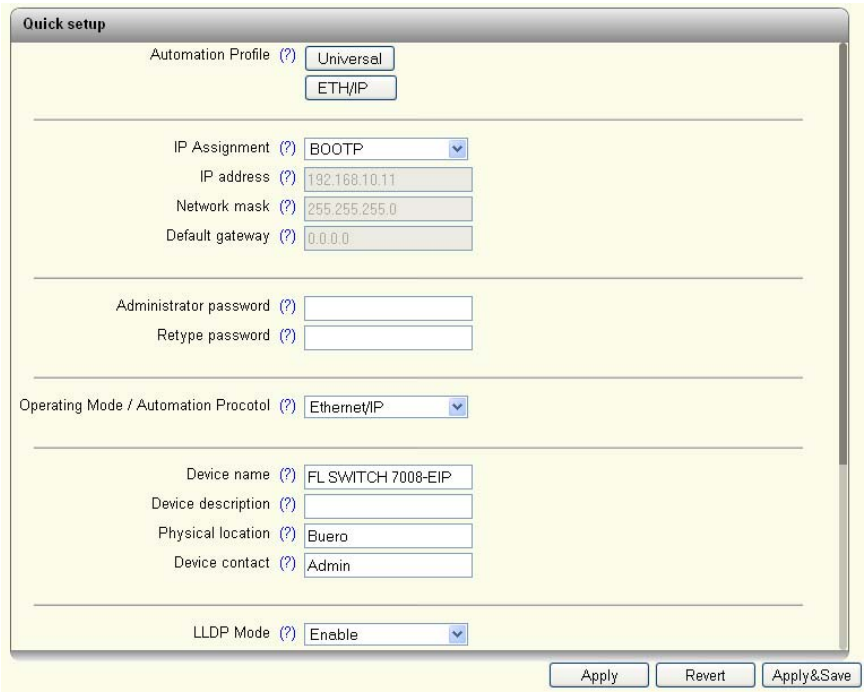


Figure 4-18 “Quick setup” web page

In “Quick setup”, the basic settings can be made:

Automation Profile: Select a profile which is optimized to the desired operating mode.
- Universal: Standard operating mode
- ETH/IP: EtherNet/IP operating mode

IP Assignment: Select the type of 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.

Operating mode: Here you can change the operating mode of the device.
- Default: The device operates without EtherNet/IP stack.
- EtherNet/IP: The EtherNet/IP stack is activated.

Device name: You can input 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: You can switch LLDP on or off here.

LLDP mode:
– Disable: LLDP is deactivated.
– Enable: LLDP is activated.
– Send only: Received LLDP BPDUs are ignored.
– Receive only: No LLDP BPDUs are sent.

“Network Configuration” web page

The basic network settings are made here.

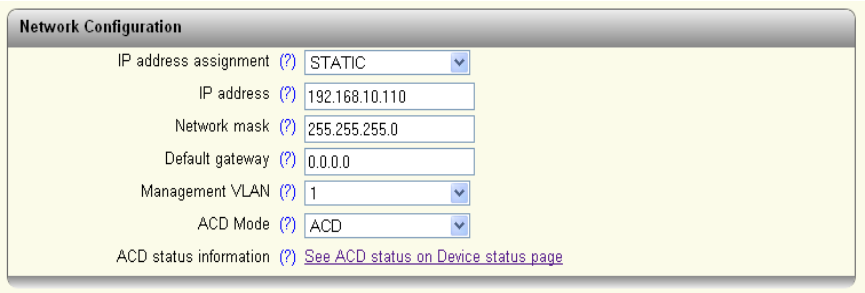


Figure 4-19 “Network Configuration” web page

IP address assignment: Select the type of 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 switch the “Address Conflict Detection” function on or off here.

ACD status information: By clicking the button, you access the ACD status information.

Figure 4-20 ACD status information

“Service” web page

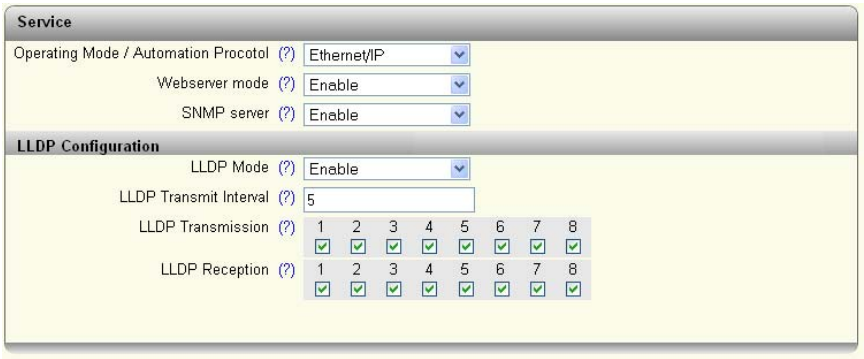


Figure 4-21 “Service” web page

Operating Mode / Automation Protocol:

Universal - standard operating mode

EtherNet/IP - EtherNet/IP operating mode

Webserver mode: You can switch the web server function on/off here.

SNMP server: You can switch the SNMP server function on/off here.

LLDP Configuration

LLDP Mode: Disable: LLDP is switched off.

Enable: LLDP is switched on.

Send Only: Only LLDP BPDUs are sent.

Receive Only: Only LLDP BPDUs are received.

LLDP Transmit Interval: Set the interval here, in which an LLDP telegram should be sent. The value must be between 5 and 32786 seconds. (default: 5 s)

LLDP Transmission: You can switch off/on port-specific forwarding of LLDP telegrams.

LLDP Reception: You can switch on/off port-specific ignoring of LLDP telegrams.

“Port Configuration” web page

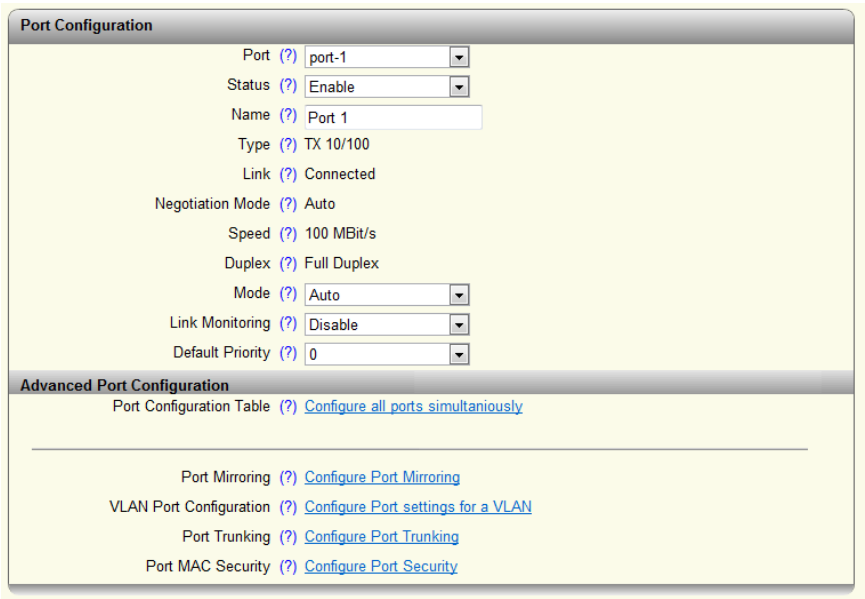


Figure 4-22 “Port Configuration” web page

Port: Select the port which you wish to configure individually.

Status: The port can be switched off here.

– Enable: Port active
– Disable: Port deactivated

Name: You can assign the port a name.

Type: Describes the physical properties of the port.

Link: Shows the current link status of the port.

Negotiation Mode: Displays the negotiation mode.

Speed: Displays the speed at which the port is operating.

Duplex: Indicates the port transmission mode.

Mode: The port can be set to a determined 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 here for incoming data packets to this port.

By clicking on the “Configure all ports simultaneously” button, you can access the “Port Configuration Table”.

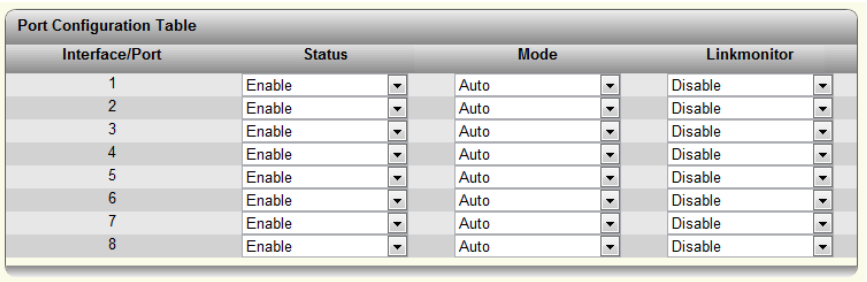


Figure 4-23 “Port Configuration Table” web page

You can set the status, mode, and link monitoring there for all ports.

By clicking on the “Configure Port Mirroring” button, you can access the port mirroring configuration.

By clicking on the “Configure Port settings for a VLAN” button, you can access the “VLAN Port Configuration” page.

By clicking on the “Configure Port Trunking” button, you can access the “Link Aggregation” page.

By clicking on the “Configure Port Security” button, you can access the “Port Based Security” page.

“Link Aggregation” web page

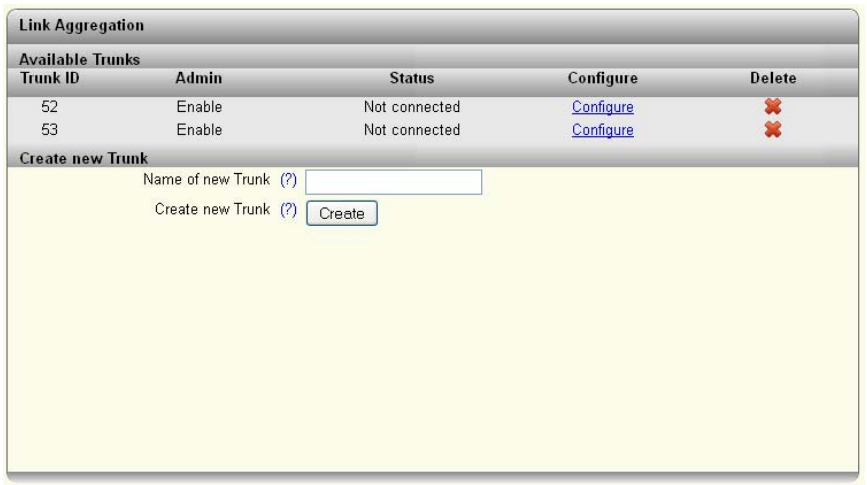


Figure 4-24 “Link Aggregation” web page

In order to create a new trunk, input a name for the trunk in “Name of new Trunk” and click on the “Create” button. The trunk appears in the table in the upper part of the web page.

A maximum of four trunks is possible on one device.

To configure a trunk, click the “Configure” button next to the trunk which you wish to configure. To delete a trunk, use the red “X”.

“Configure Trunk” web page

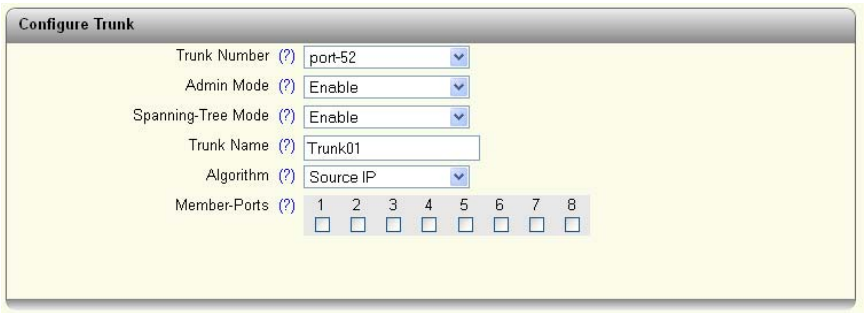


Figure 4-25 “Configure Trunk” web page

Trunk Number: All trunks created by you are displayed here. From there, select the trunk which you wish to configure.

Admin Mode: You can switch a trunk on/off here.

Spanning-Tree Mode: From here, select whether the RSTP protocol for this trunk should be switched on.

Trunk name: You can set a name here for the trunk.

Algorithm:

Member-Ports: Select up to four ports here which should belong to the trunk.

“VLAN configuration” web page

Figure 4-26 “VLAN configuration” web page

For additional VLAN information, please refer to Section “Virtual Local Area Network - VLAN” on page 79.

“Multicast Configuration” web page

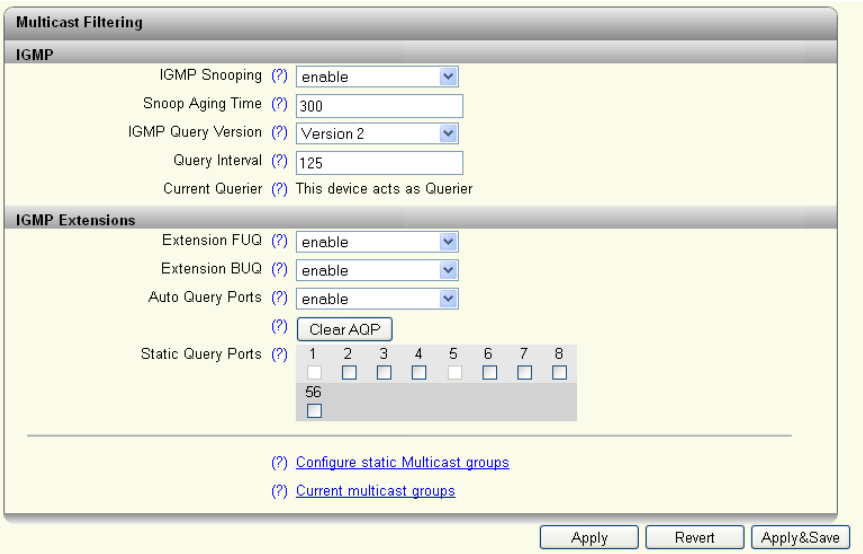


Figure 4-27 “Multicast Configuration” web page

For additional VLAN information, please refer to Section “Multicast filtering” on page 77.

“Network Redundancy” web page

Spanning tree configuration

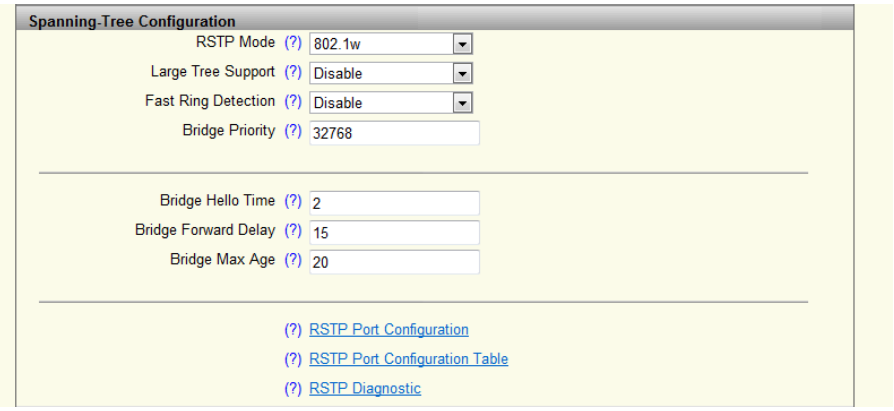


Figure 4-28 “Spanning-Tree Configuration” configuration area

RSTP mode

Disable: The RSTP function is not activated.

802.1w: The RSTP function is activated globally and works according to the 802.1w standard.

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

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 in order 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.

By clicking on the “RSTP Port Configuration” button, you can access the RSTP port configuration.

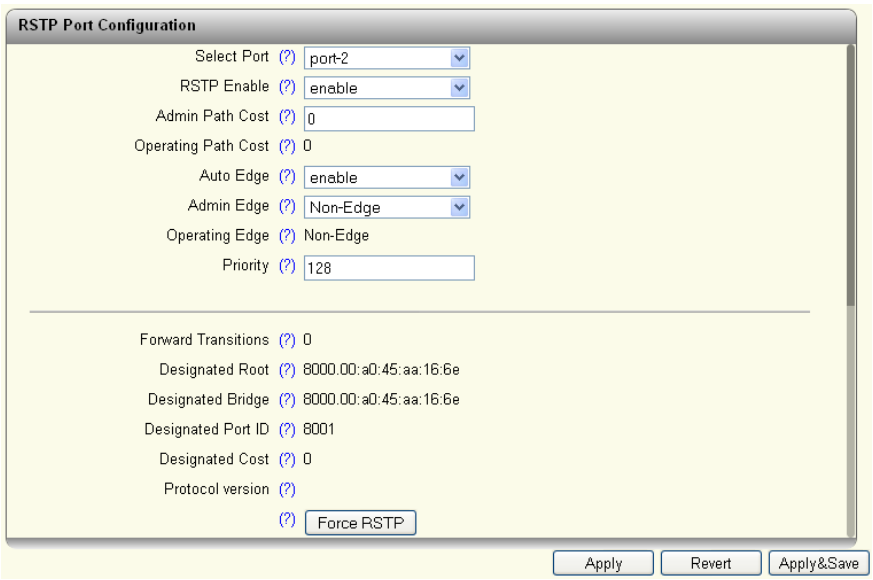


Figure 4-29 “RSTP Port Configuration” web page

Select Port: Select here the port to which you wish to change the RSTP settings.

RSTP Enable:

Enable: RSTP is activated for the port.

Disable: RSTP is deactivated for the port.

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

Operating Path Cost: Indicates the path cost 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 linkup.

Admin Edge: Here you can specify 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 cost of this segment to the root switch.

Protocol Version: Displays the protocol version.

By clicking on the “RSTP Port Configuration Table” button, you can access the RSTP port configuration table.

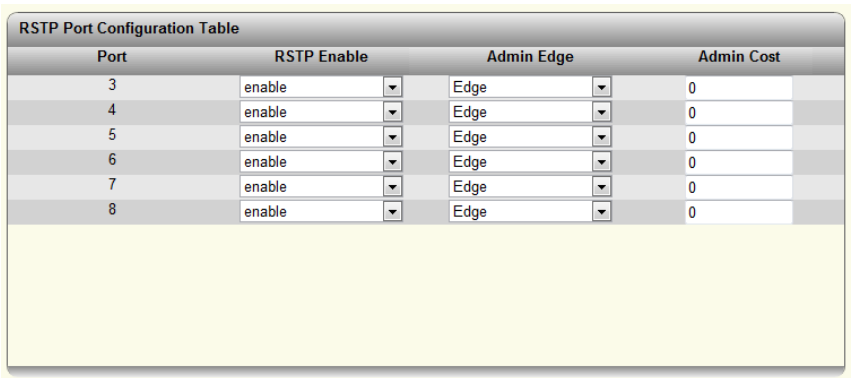


Figure 4-30 “RSTP Port Configuration Table” web page

Port: Indicates the ports for which RSTP is available.

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

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

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

By clicking on the “RSTP Diagnostics” button, you can access the “RSTP Diagnostic” page:

Figure 4-31 “RSTP Diagnostic” web page

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

Root Port: Indicates which port the root is connected to. If the root is not directly connected, it shows the direction of the root.

Root Cost: Indicates the entire path cost to the root.

Topology Changes: Indicates the number of topology changes.

Last Topology Change: Indicates when the last topology changes took place.

Hello Time: Indicates the hello time set at the root.

Forward Delay: Indicates the forward delay set at the root.

Max Age: Indicates the max age time set at the root.

By clicking on “Redundancy Port Table” you receive a table with information on the individual ports and their redundancy mechanism assignment.

“Redundancy Port Table” web page

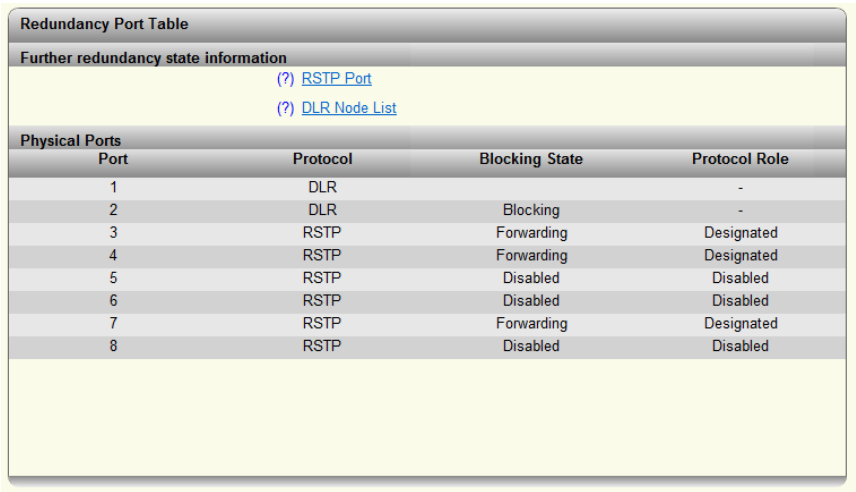


Figure 4-32 “Redundancy Port Table” web page

“Device Level Ring Configuration” web page

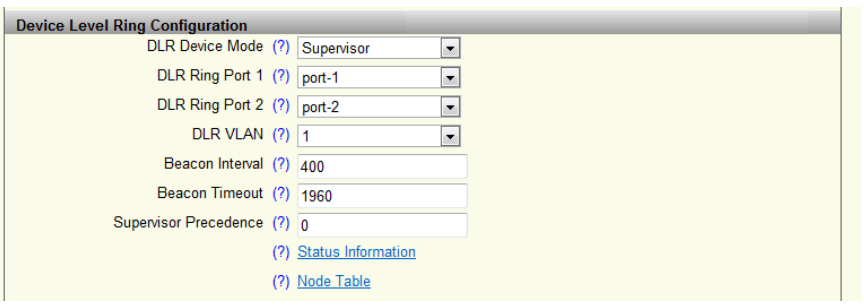


Figure 4-33 “Device Level Ring Configuration” web page

DLR Device Mode: Select the role of the switch in your device level ring.

– Supervisor: The device functions as the master in the ring.
– Node: The device functions as a node in the ring.

DLR Ring Port 1: Determines the first ring port for the device level ring.

DLR Ring Port 2: Determines the second ring port for the device level ring.

The following fields are only available in supervisor mode.

Make sure that the DLR ports available on the supervisor are only connected to the DLR ports of the other devices.

DLR VLAN: Here you can set the virtual LAN in which the redundancy mechanism should work (default: 1).

Beacon Interval: Here you can set the interval in which the beacon telegrams are sent. The value must be between 100 and 100000 (default: 400).

Beacon Timeout: Here you can set the permitted timeout of a beacon telegram. The value must be between 200 and 500000 (default: 1960).

Supervisor Precedence: Set the priority of the supervisor here. The highest value has the highest priority in the network. The value must be between 0 and 255 (default: 0)

For the two configured DLR ports, the physical settings remain available. Settings for VLAN or port trunking are deleted and are reset to the default value.

By clicking on the “Status Information” button, you receive detailed information on the status of the device level ring.

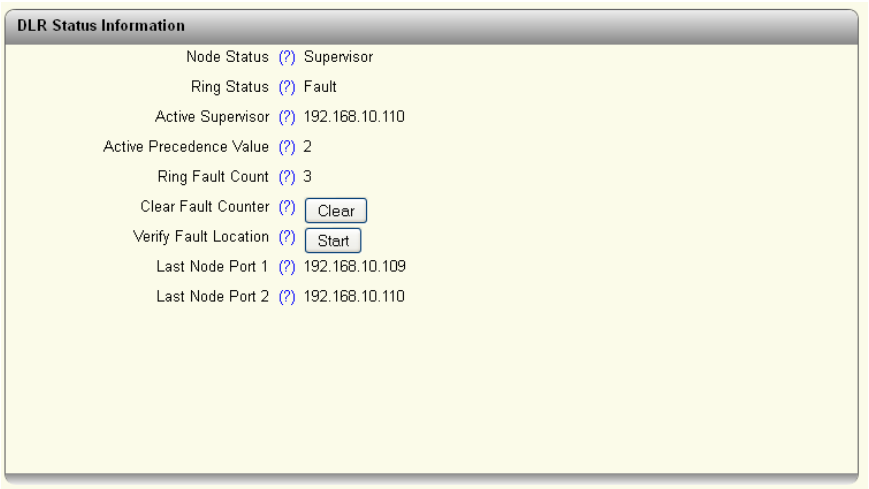


Figure 4-34 “DLR Status Information” web page

Node Status: Reflects the status of the device in the device level ring.

Ring Status: Indicates the status of the ring.

– OK: No errors have occurred.
– Fault: An error has occurred.

Rapid Fault: An error has occurred which must be reset manually at the device functioning as the supervisor for this ring.

Active Supervisor: Indicates the IP address of the active supervisor in the network.

Active Precedence Value: Indicates the priority of the active supervisor in the network.

The following parameters can only be seen by the supervisor.

Ring Fault Count: Counter which monitors the number of redundancy switching operations.

Clear Fault Counter: Button to delete the “Ring Fault Count”.

Verify Fault Location: Button to start the localization of the error position in the ring.

Last Node Port 1: Indicates the IP address of the first device, where the error is located.

Last Node Port 2: Indicates the IP address of the second device, where the error is located.

By clicking on the “Node Table” button, you receive a list of all devices integrated in the device level ring. The “DLR Node Table” is only available in supervisor mode.

“DLR Node Table” web page

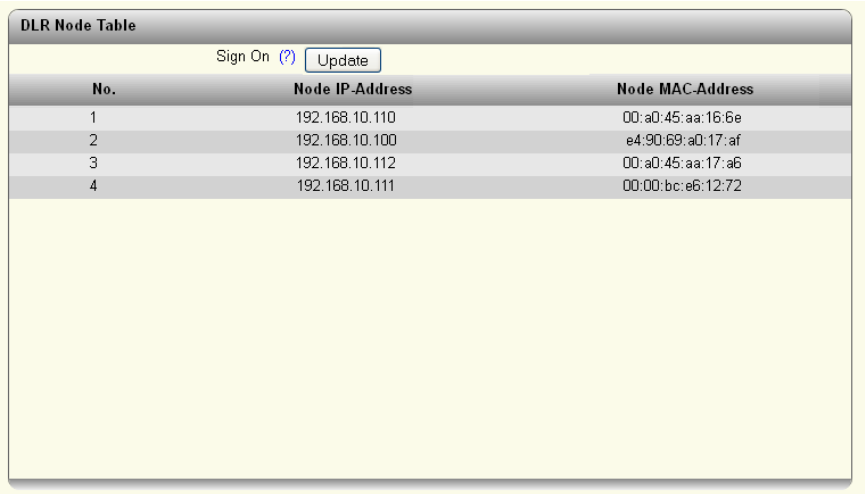


Figure 4-35 “DLR Node Table” web page

“Security” web page

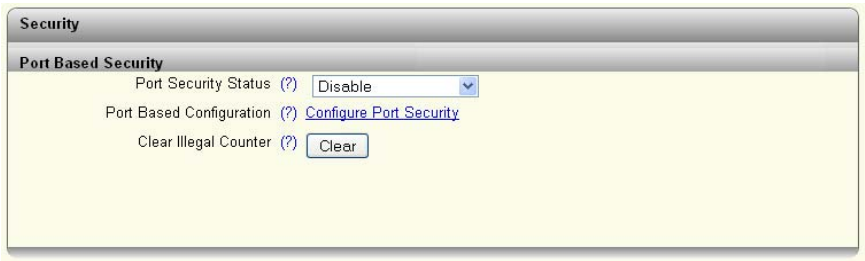


Figure 4-36 “Security” web page

Port Security Status: The port security can be globally activated here.

Port Based Configuration: By clicking on the button, you can access the security relating to the port.

Clear Illegal Counter: By clicking on the button, the counter is set to “0”.

“Port Based Security” web page

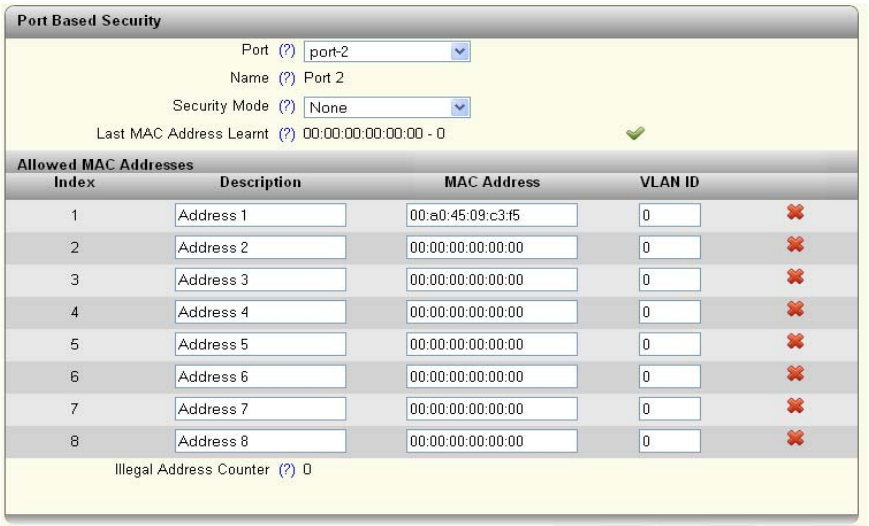


Figure 4-37 “Port Based Security” web page

Port: Select the port here for which the security settings should be made.

Name: Indicates the name of the selected port.

Security Mode: Set here what the process is if a non-permitted MAC address is detected by the device.

None: No security settings are available for this port.

Trap: If a MAC address that is not permitted is detected at the port, a trap is sent to the predefined trap target address.

The packets are not blocked.

Block: If a MAC address that is not permitted is detected at the port, all packets are blocked at the port and a trap is sent to the predefined trap target address.

The packets at this block remain blocked until a permitted MAC address is detected.

Last MAC Address Learnt: Displays the MAC address of the last device connected. Using the green tick, this MAC address can be accepted into the list of permitted MAC addresses.

Allowed MAC Addresses

Index: The permitted MAC addresses are shown in the index.

Description: A description can be stored for a permitted MAC address here.

MAC Address: Enter a MAC address, you want to allow access, alternatively you can select the green box behind the “Last MAC Address Learnt” to use the last MAC address which was learned.

VLAN ID: Enter the VLAN here, where the device is located and which the permitted MAC address occupies.

You can delete the permitted MAC address for this port using the red “X” behind each column.

Illegal Counter: Counter which totals the packets of non-permitted MAC addresses.

“DHCP Services” web page

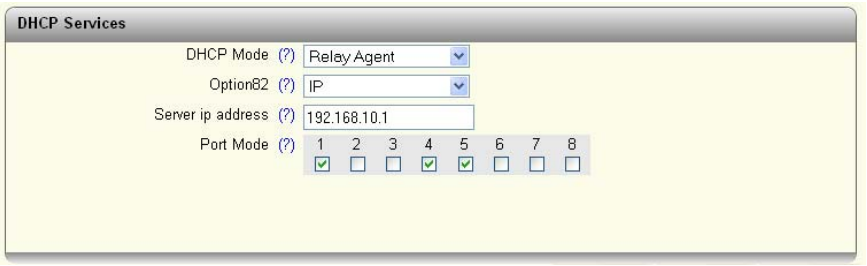


Figure 4-38 “DHCP Services” web page

DHCP Mode: Select the DHCP service you wish to use.

– None: A DHCP service is not used on the switch.
– Relay Agent: The DHCP relay agent (DHCP Option 82) is switched on.

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

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

Server ip address: Enter the IP address of the DHCP server in your network.

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

“Local Events” web page

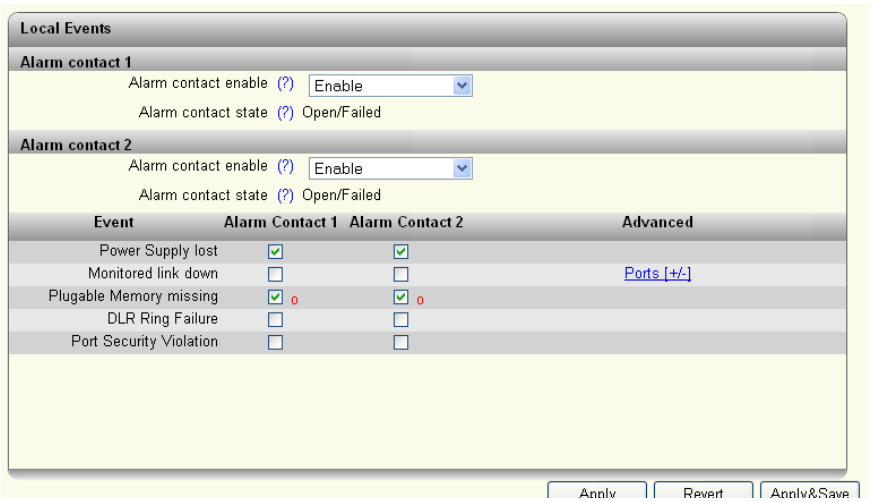


Figure 4-39 “Local Events” web page

Alarm contact 1:

Here you can switch alarm contact 1 on and read the current status of the alarm contact (if an “o” is present, this event has occurred).

Alarm contact 2:

Here you can switch alarm contact 2 on and read the current status of the alarm contact (if an “o” is present, this event has occurred).

Events:

Here you can set under which conditions an alarm contact should report an error.

Power Supply lost:

In the event of a loss of US1 or US2.

Monitored link down:

In “Advanced”, select the ports to which a link down behavior should be notified.

Pluggable Memory missing:

There is an error message if no memory card is present.

DLR Ring Failure:

If there is an error in the device level ring, there is an error message indicating this.

Port Security Violation: The alarm contact indicates an error if a non-permitted MAC address has been detected at a port.

“LLDP Topology” web page

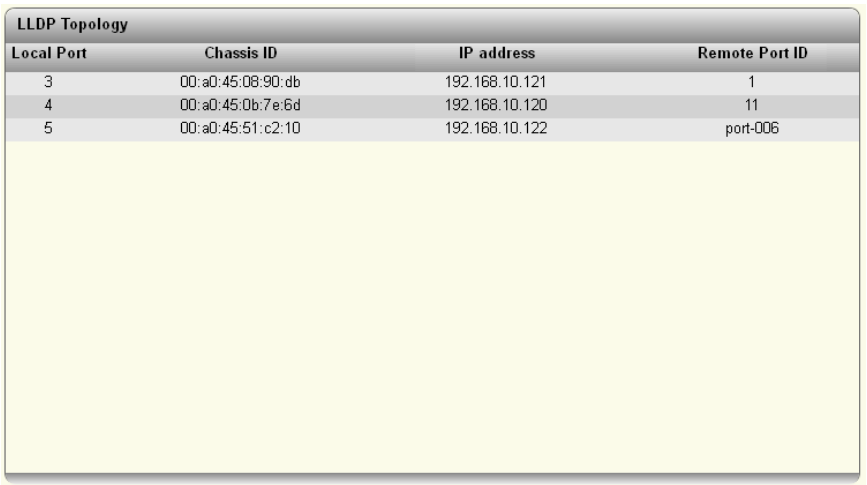


Figure 4-40 “LLDP Topology” web page

From the web page, you receive the neighboring/topology information, which the device can extract from the network it is connected to.

“RSTP Diagnostic” web page

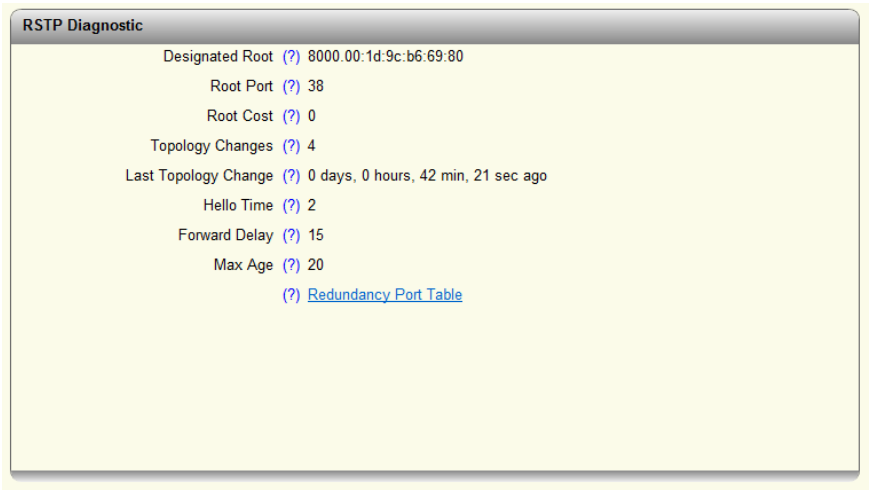


Figure 4-41 “RSTP Diagnostic” web page

“DLR Status Information” web page

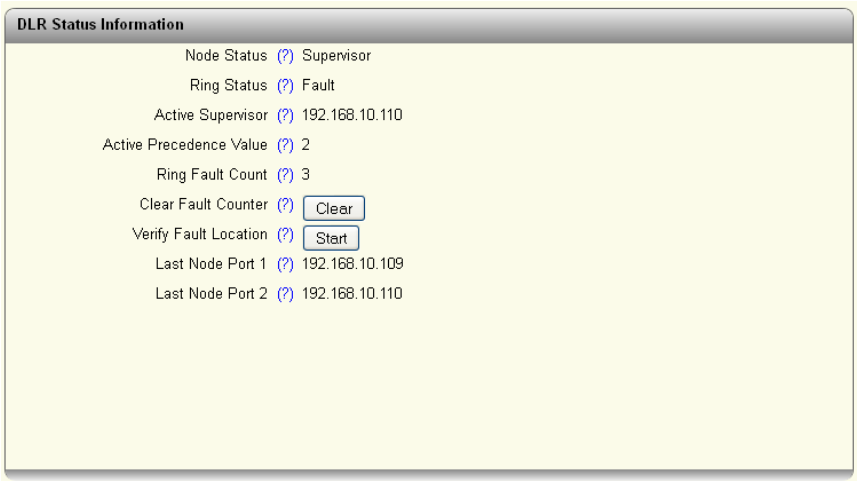


Figure 4-42 “DLR Status Information” web page

“Mirroring Configuration” web page

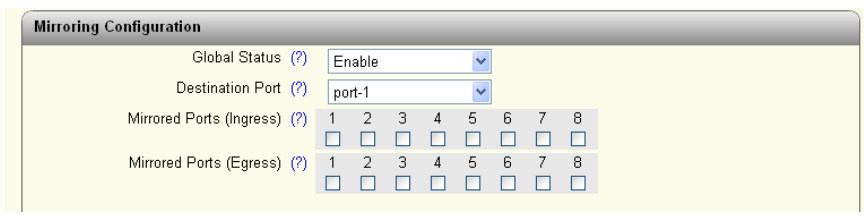


Figure 4-43 “Mirroring Configuration” web page

Global Status: Enable: Port mirroring is globally activated./Disable: Port mirroring is globally deactivated.

Destination Port: Select here the port to which the measuring instrument (PC) is connected.

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

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

“Trap Manager” web page

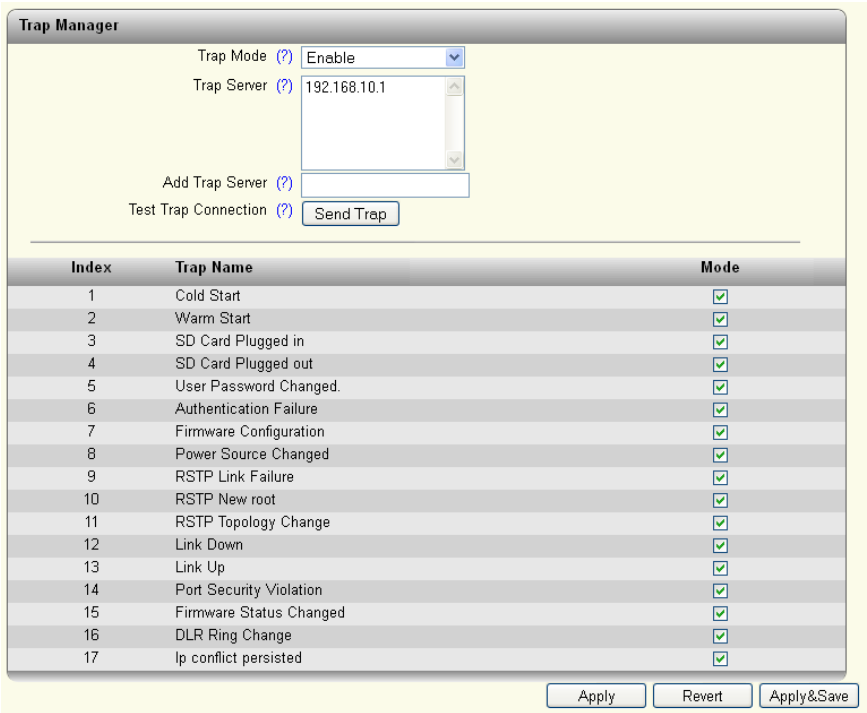


Figure 4-44 “Trap Manager” web page

Trap Mode:

Enable: The sending of SNMP traps is activated.

Disable: The sending of SNMP traps is deactivated.

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

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 “Send Trap”.

The table list the SNMP traps which can be transmitted by the device. Here you can specify the actions that should be followed by the sending of traps.

“Port Counter” web page

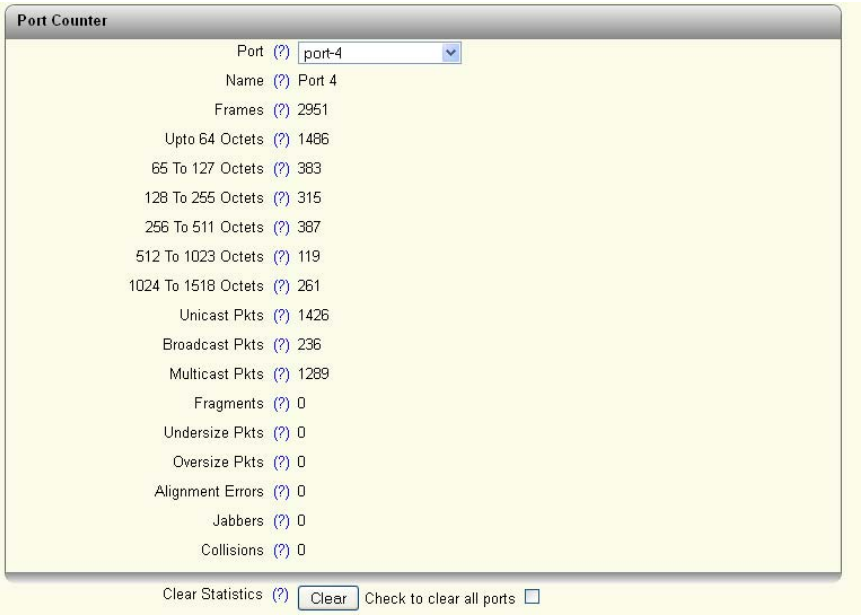


Figure 4-45 “Port Counter” web page

Here you will find an overview of port statistics.

“Utilization” web page

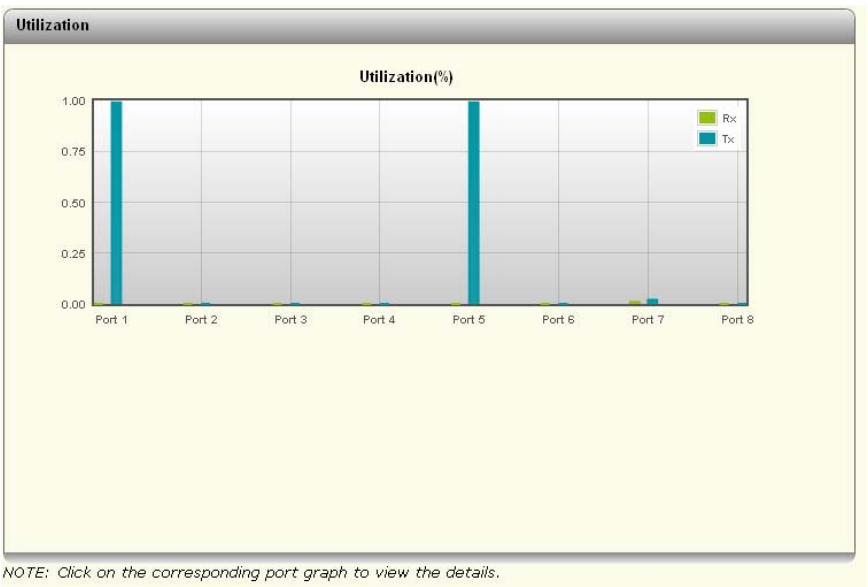


Figure 4-46 “Utilization” web page

Here you will find an overview of the device ports with regard to their percentage utilization. A detailed overview will be provided by clicking on the graph of an individual port.

5 Simple Network Management Protocol - SNMP

5.1 General function

SNMP is a manufacturer-independent standard for Ethernet management. It defines commands for reading and writing information, and defines formats for error and status messages. SNMP is also a structured model that 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 terminal modules, routers, and other devices that support SNMP. The task of the agents is to collect and provide data in the MIB. The manager regularly requests and displays this information. The devices can be configured by writing data from the manager to the MIB. In the event of an emergency, the agents can also send messages (traps) directly to the manager.

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

5.1.1 Schematic view of SNMP management

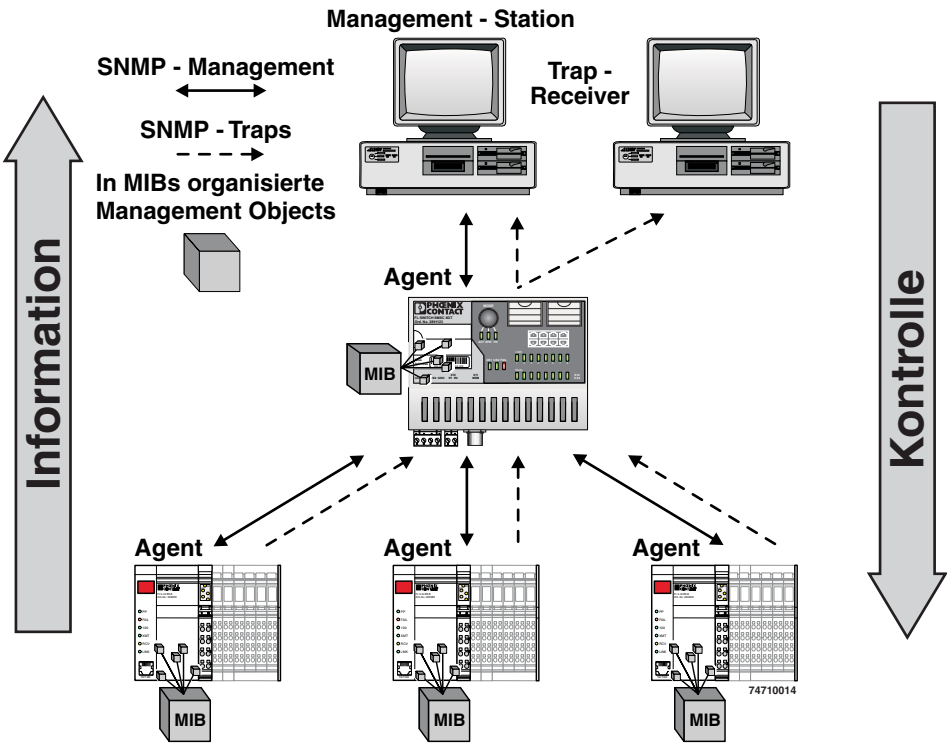


Figure 5-1 Schematic view of SNMP

SNMP interface

All managed Factoryline components have an SNMP agent. The agent of such a device manages the following MIBs (Management Information Base):

- 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 Factory Manager, 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 (Request 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 is assigned to an object ID (object name and parameters) and can be published. If an object is no longer needed, it can be labeled as “expired”, but it cannot be reused with other parameters under any circumstances.

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

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

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

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

Management Information Base (MIB)

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

Agent

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

Traps

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

trapPasswd

OID	1.3.6.1.4.1.4346.11.11.3.0.1
description	Sent to the defined trap receivers on each modification or attempted modification of the device password and contains information about the status of the last modification or attempted modification.

trapFWHealth

OID	1.3.6.1.4.1.4346.11.11.3.0.2
description	Sent on each firmware-related modification and contains additional information about the firmware status.

trapFWConf

OID	1.3.6.1.4.1.4346.11.11.3.0.3
description	Sent each time the configuration is saved and informs the management station that the configuration has been saved successfully. This trap is sent in the event of configuration modifications (port name, port mode, device name, IP address, trap receiver address, port mirroring, etc.), which are not yet saved permanently. The trap also provides a warning that, if not saved permanently, the changes will be lost on a reset.

trapPowerSupply

OID	1.3.6.1.4.1.4346.11.11.3.0.4
description	Sent each time the redundant power supply fails.

trapRstpRingFailure

OID	1.3.6.1.4.1.4346.11.11.3.0.6
Description	Sent in the event of a link interrupt in the redundant RSTP ring.

trapManagerConnection

OID	1.3.6.1.4.1.4346.11.11.3.0.99
description	Trap to test the connection between the SNMP agent and the network management station.

5.2 Tree structure of the MIB

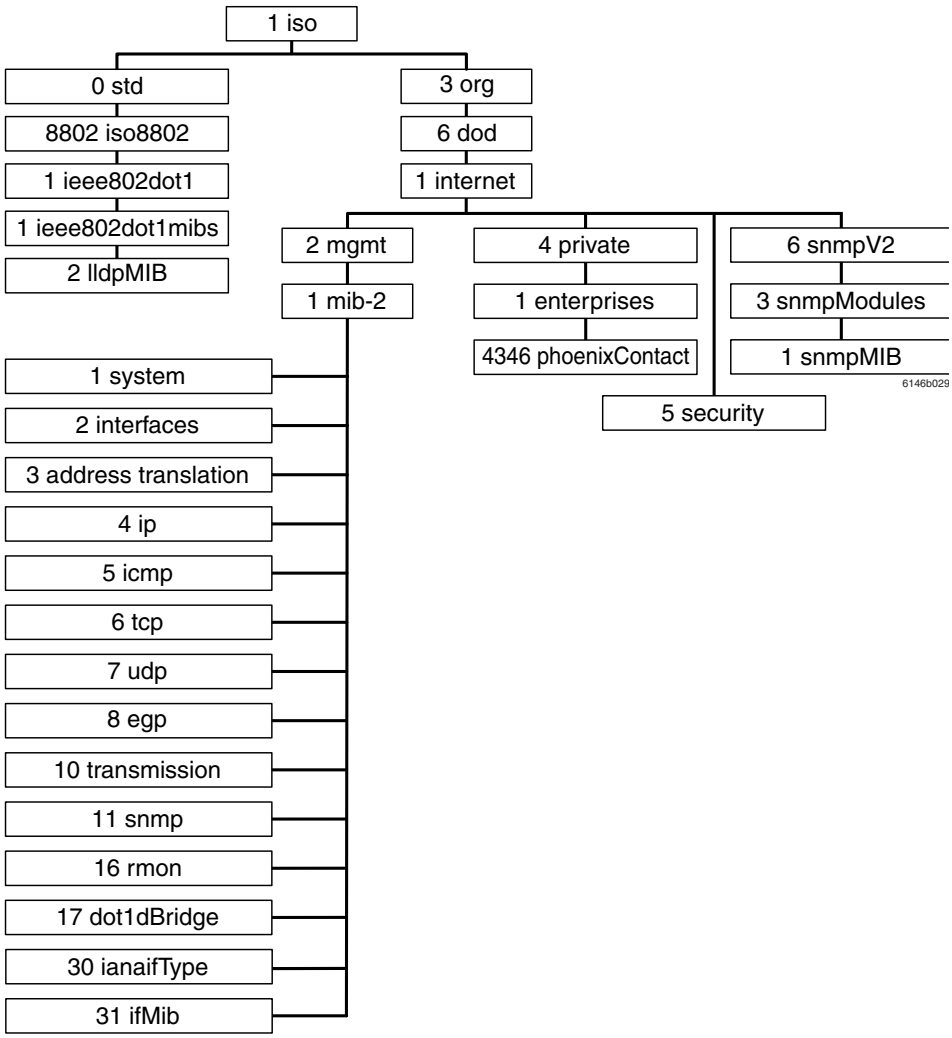


Figure 5-2 Tree structure of the MIB

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

The 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 packet (zip file).

Please note that the following MIB objects are **not** available on the DLR ports:

INTERFACE MIB

IfOutErrors, IfDiscards, IfUnknownProtos, IfOutDiscards

EtherStatsTable

EtherStatsUndersizePkts, EtherStatsOversizePkts, EtherStatsBroadcastPkts, EtherStatsMulticastPkts, EtherStatsFragments, EtherStatsJabbers, EtherStatsCollisions, EtherStats64Octets, EtherStats65-127Octets, EtherStats128-255Octets, EtherStats256-511Octets, EtherStats512-1023Octets, EtherStats1024-1518Octets

6 General information on the Device Level Ring - DLR

DLR increases the network availability, thanks to a redundant ring topology with a switch-over time of less than 3 ms for error detection and reconfiguration. DLR is a protocol that works on Layer 2 for multi-port EtherNet/IP devices. The use of DLR is transparent for the protocols which work on higher levels such as TCP/IP.

If a device is to be configured as ring supervisor in a DLR topology, the other switches in the ring must support DLR. Operating non-DLR switches in the ring is not recommended.

6.1 Possible topologies

The DLR protocol supports the 1-ring topology; multiple rings or overlapping rings are not possible. It is possible, when using suitable switches, to connect a redundant ring or operate multiple, restricted rings. As such, DLR protocol information may not leave the individual ring and appear in other rings.

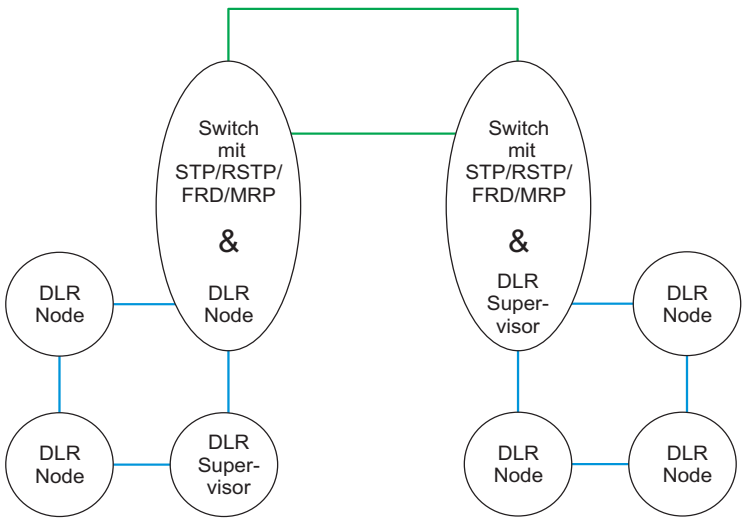


Figure 6-1 Redundant coupling of two DLR rings via STP/RSTP/FRD/MRP

The following topology shows four DLR rings, which each make up individual segments. These segments are redundantly meshed and connected with one another. As such, the individual segments are respectively separated from other segments, so that no protocol information can leave the particular ring.

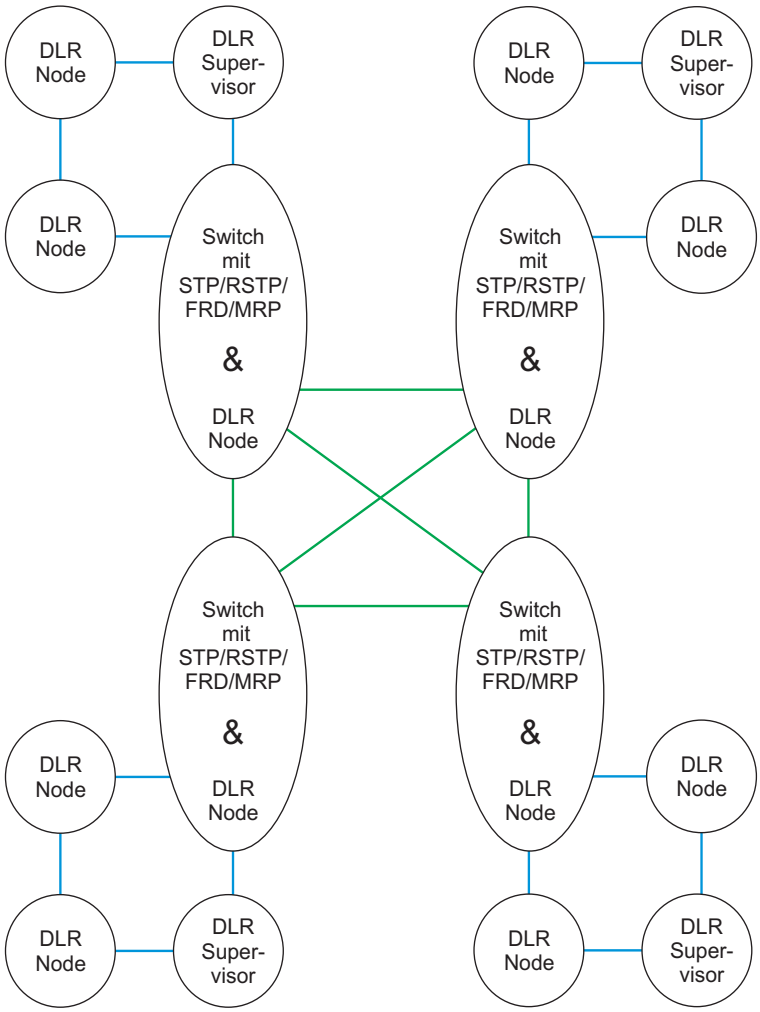


Figure 6-2 Meshed coupling of multiple DLR rings

Other possible topologies

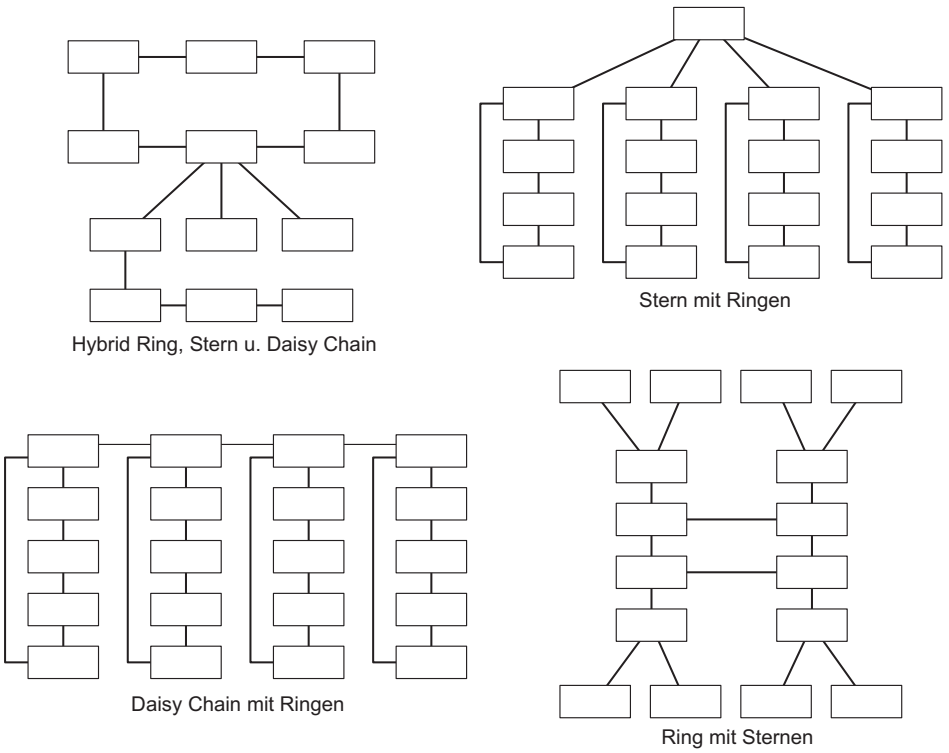


Figure 6-3 Other possible topologies

Ensure that the DLR standard does **not** provide support for the following MIB objects:

Interface MIB

IfOutErrors, IfDiscards, IfUnknownProtos, IfOutDiscards

EtherStatsTable

EtherStatsUndersizePkts, EtherStatsOversizePkts, EtherStatsBroadcastPkts, EtherStatsMulticastPkts, EtherStatsFragments, EtherStatsJabbers, EtherStatsCollisions, EtherStats64Octets, EtherStats65-127Octets, EtherStats128-255Octets, EtherStats256-511Octets, EtherStats512-1023Octets, EtherStats1024-1518Octets

7 Common Industrial Protocol – CIP

The switch supports the Common Industrial Protocol (CIP) and implements the “Managed Switch Profile”. The CIP can be accessed by all ports assigned to the “Management VLAN” (VLAN 1, factory default).

EtherNet/IP uses the Common Industrial Protocol as application layer. IP and TCP or UDP are used for the network and transport layers.

CIP and EtherNet/IP are standardized by ODVA (www.odva.org) on a manufacturer-neutral basis.

The Common Industrial Protocol is an object-oriented protocol with two different types of communication between controller and termination devices.

The following table describes the two communication types.

Table 7-1 CIP communication types

Connection type	Description
Explicit messaging	Explicit messaging is based on the principle of “request/response”. This means that a controller or engineering system sends a request and the termination device responds. For example, explicit messaging can be used for configuration and/or diagnostics purposes.
Implicit messaging	Implicit messaging is used for the cyclic transmission of I/O data. That means, for example, that a termination device sends an analog value which is present at an termination device input. The time for a transmission cycle can be set via the Requested Packet Interval (RPI).

Electronic data sheets – EDS files

EDS files enable integration in a control system such as RSLogix.

The EDS file contains information on parameters which can be set and configured via CIP.

Table 7-2 Devices and EDS file

Order No.	Device designation	File designation
2701418	FL SWITCH 7008-EIP	FL_SWITCH_7008_EIP.eds
2701419	FL SWITCH 7006/2FX-EIP	FL_SWITCH_7005_2FX_EIP.eds
2701420	FL SWITCH 7005/FX-2FXSM-EIP	FL_SWITCH_7005_1FX_2FXSM_EIP.eds

The EDS files can be loaded directly from the device via web-based management.

To do so, go to “Information” and then select the “Help & Documentation” menu item.

The EDS files are also available in the download area.

7.1 Supported EtherNet/IP objects

The device supports the following EtherNet/IP objects. Please refer to the EtherNet/IP specification for more detailed information, which can be obtained from the Open DeviceNet Vendor Association (ODVA).

7.1.1 Identity object (class code 01)

Table 7-3 1.1 Instance attributes

ID	Attributes	Access rule	Data type	Description
1	Vendor ID	Get	UINT	562 (Phoenix Contact)
2	Device Type	Get	UINT	44 (Managed Ethernet switch device)
3	Product Code	Get	UINT	8400 (FL SWITCH 7008-EIP) 8401 (FL SWITCH 7006/2FX-EIP) 8402 (FL SWITCH 7005/FX-2FXSM-EIP)
4	Revision	Get	STRUCT of:	Revision of the item represented by the Identity object
	Major Revision		USINT	Major revision of the device
	Minor Revision		USINT	Minor revision of the device
5	Status	Get	WORD	Bit 0
				Bit 1
				Bit 2
				Bit 3
6	Serial Number	Get	UDINT	Serial number of the device
7	Product Name	Get	SHORT_STRING	Product name of the device

Table 7-4 1.2 Services

Service code	Class	Instance	Name of service
0x01	X	X	Get_Attribute_All
0x05	X	X	Reset
0x0E	X	X	Get_Attribute_Single

Table 7-5 1.2.1 Reset services

Value	Description
0	Normal reset without modifications to the device configuration
1	Reset to factory default
2	The device will execute the following steps: – Save IP address, subnet mask and gateway to temporary location – Clear the configuration database/configuration file – Restore saved IP parameters – Save configuration (now only containing IP parameters)

7.1.2 Message Router object (class code 02)

Table 7-6 2.1 Class attributes

ID	Attributes	Access rule	Data type	Description
1	Revision	Get	UINT	Revision of this object
2	Max Instance	Get	UINT	Maximum instance number of this object
3	Number of Instance	Get	UINT	Instance number of this object
4	Optional attribute List	Get	STRUCT of:	List of optional instance attributes used in an object class implementation
	Number of attributes		UINT	Number of attributes in the optional attribute list
	Optional attributes		ARRAY of UINT	List of optional attribute numbers
5	Optional Service List	Get	SRUCT of:	List of optional services used in an object class implementation
	Number services		UINT	Number of services in the optional service list
	Optional services		ARRAY of UINT	List of optional service codes
6	Maximum ID Number Instance class Attributes	Get	UINT	Attribute ID number of the last class attribute of the class definition implemented in the device
7	Maximum ID Number Instance Attributes	Get	UINT	Attribute ID number of the last instance attribute of the class definition implemented in the device

Table 7-7 2.2 Instance attributes

ID	Attributes	Access rule	Data type	Description
1	Object_list	Get	STRUCT of:	List of supported objects
	Number		UINT	Number of supported classes in the class array
	Classes		ARRAY OF UINT	List of supported class codes
2	Number available	Get	UINT	Maximum number of supported connections

Table 7-8 2.3 Services

Service code	Class	Instance	Name of service
0x01	X	X	Get_Attribute_All
0x0E	X	X	Get_Attribute_Single
0x0A		X	Multiple_Service_Packet

7.1.3 Connection Manager object (class code 06)

Table 7-9 3.1 Class attributes

ID	Attributes	Access rule	Data type	Description
1	Revision	Get	UINT	Revision of this object
2	Max Instance	Get	UINT	Maximum instance number of this object
3	Number of Instance	Get	UINT	Instance number of this object
4	Optional attribute List	Get	STRUCT of:	List of optional instance attributes used in an object class implementation
	Number of attributes		UINT	Number of attributes in the optional attribute list
	Optional attributes		ARRAY of UINT	List of optional attribute numbers
6	Maximum ID Number Instance class Attributes	Get	UINT	Attribute ID number of the last class attribute of the class definition implemented in the device
7	Maximum ID Number Instance Attributes	Get	UINT	Attribute ID number of the last instance attribute of the class definition implemented in the device

Table 7-10 3.2 Instance attributes

ID	Attributes	Access rule	Data type	Description
1	Open Requests	Get/ Set	UINT	Number of Forward Open service requests received
2	Open Format Rejects	Get/ Set	UINT	Number of Forward Open service requests which were rejected due to bad format
3	Open Resources Rejects	Get/ Set	UINT	Number of Forward Open service requests which were rejected due to lack of resources
4	Open Other Rejects	Get/ Set	UINT	Number of Forward Open service requests which were rejected for reasons other than bad format or lack of resources
5	Close Requests	Get/ Set	UINT	Number of Forward Close service requests received
6	Close Format Rejects	Get/ Set	UINT	Number of Forward Close service requests which were rejected due to bad format
7	Close other Rejects	Get/ Set	UINT	Number of Forward Close service requests which were rejected for reasons other than bad format or lack of resources
8	Connection Timeouts	Get/ Set	UINT	Total number of connections timeouts that have occurred in connections controlled by this connection manager

Table 7-11 3.3 Services

Service code	Class	Instance	Name of service
0x01	X	X	Get_Attribute_All
0x02	-	X	Set_Attribute_All
0x0E	X	X	Get_Attribute_Single
0x10	-	X	Set_Attribute_Single

7.1.4 TCP/IP Interface object (class code F5)

Table 7-12 4.1 Class attributes

ID	Attributes	Access rule	Data type	Description
1	Revision	Get	UINT	Revision of this object

Table 7-13 4.2 Instance attributes

ID	Attributes	Access rule	Data type	Description	
1	Status	Get	DWORD	Bits 0 - 3	Interface configuration status
				Bit 4	Mcast pending (always 0)
				Bit 5	Interface configuration pending
				Bit 6	AcdStatus
				Bit 7	AcdFault
2	Configuration Capability	Get	DWORD	Bit 0	BOOTP client
				Bit 2	DHCP client
				Bit 4	TCP/IP config settable via ETH/IP
				Bit 7	AcdCapable
3	Configuration Control	Get/set	DWORD	Bits 0 - 3	0 = The device uses static IP configuration. 1 = The device uses BOOTP. 2 = The device uses DHCP.
4	Physical Link Object	Get	STRUCT of:	Path to Physical Link object	
	Path Size		UINT	4	
	Path		Padded EPATH	0x20, 0xF6, 0x25, 0x01	

Table 7-13 4.2 Instance attributes

ID	Attributes	Access rule	Data type	Description
5	Interface Configuration	Get/Set	STRUCT of:	TCP/IP network interface configuration
	IP Address		UDINT	Device IP address
	Network Mask		UDINT	Device network mask
	Gateway Address		UDINT	Default gateway address
	Name Server		UDINT	Primary name server (always 0.0.0.0)
	Name server 2		UDINT	Secondary name server (always 0.0.0.0)
	Domain Name		STRING	Default domain name (always empty)
6	Host Name	Get/Set	STRING	Device host name
10	SelectedAcd	Set	BOOL	Activates the use of ACD
11	LastConflictDetected	Set	STRUCT of:	Structure containing information related to the last conflict detected
	AcdActivity		USINT	State of ACD activity when last conflict detected
	RemoteMAC		Array of 6 USINT	MAC address of remote node from the ARP PDU in which a conflict was detected
	ArpPdu		ARRAY of 28 USINT	Copy of the raw ARP PDU in which a conflict was detected

Table 7-14 4.3 Services

Service code	Class	Instance	Name of service
0x01	X	X	Get_Attribute_All
0x02	-	X	Set_Attribute_All
0x0E	X	X	Get_Attribute_Single
0x10	-	X	Set_Attribute_Single

7.1.5 Ethernet Link object (class code F6)

Table 7-15 5.1 Class attributes

ID	Attributes	Access rule	Data type	Description
1	Revision	Get	UINT	Revision of this object
2	Max Instance	Get	UINT	Maximum number of an object currently created in this device class level
3	Number of Instances	Get	UINT	Number of instances currently created in this device class

Table 7-16 5.2 Instance Attributes

ID	Attributes	Access rule	Data type	Description	
1	Interface Speed	GET	UDINT	Interface speed currently in use. Speed in Mbps (e.g., 10, 100)	
2	Interface Flags	GET	DWORD	Bit 0	Link state
				Bit 1	Duplex mode
				Bit 2-4	Auto-negotiation status 0 = Auto-negotiation in progress 2 = Auto-negotiation failed but detected speed 3 = Successfully negotiated 4 = Auto-negotiation not attempted
				Bit 5	Not supported
				Bit 6	Not supported
3	Physical Address	GET	ARRAY of 6 USINTs	Physical MAC Address of the device	
7	Interface Type	GET	USINT	Interface type 2 = Twisted-pair 3 = Optical fiber	
8	Interface State	GET	USINT	Interface state 0 = Unknown interface state 1 = Interface enabled 2 = Interface disabled	
9	Admin State	SET	USINT	1 = Enable interface 2 = Disable interface	
10	Interface Lable	GET	STRING	Interface name	

Table 7-17 5.3 Services

Service code	Class	Instance	Name of service
0x01	X	X	Get_Attribute_All
0x0E	X	X	Get_Attribute_Single
0x10	-	X	Set_Attribute_Single

7.1.6 Device Level Ring (DLR) object (class code 47)

Table 7-18 6.1 Class attributes

ID	Attributes	Access rule	Data type	Description
1	Revision	Get	UINT	Revision of this object

Table 7-19 6.2 Instance attributes

ID	Attributes	Access rule	Data type	Description
1	Network Topology	Get	USINT	0 = Linear 1 = Ring
2	Network Status	Get	USINT	0 = Normal 1 = Ring fault 2 = Unexpected loop detected 3 = Partial network fault 4 = Rapid fault/restore cycle
3	Ring Supervisor Status	Get	USINT	0 = Device is backup device 1 = Device is active ring supervisor 2 = Device is a normal ring node 3 = Device is in a non-DLR topology 4 = Device cannot support the operating ring parameters (beacon interval and/or beacon timeout)
4	Ring Supervisor Config	Set	STRUCT of:	Ring supervisor configuration parameters
			BOOL	Ring supervisor enable
			USINT	Ring supervisor precedence
			UDINT	Beacon interval
			UDINT	Beacon timeout
			UINT	DLR VLAN ID
5	Ring Faults Count	Get	UINT	Number of ring faults since power up
6	Last Active Node on Port 1	Get	STRUCT of:	Last active node at the end of chain through port 1 of active ring supervisor during ring fault
			UDINT	Device IP address
			ARRAY of 6 USINTs	Device MAC address
7	Last Active Node on Port 2	Get	STRUCT of:	Last active node at the end of chain through port 2 of active ring supervisor during ring fault
			UDINT	Device IP address
			ARRAY of 6 USINTs	Device MAC address
8	Ring Protocol Participants Count	Get	UINT	Number of devices in ring protocol participant list
9	Ring Protocol Participants List	Get	ARRAY of	List of device participants in ring protocol
			STRUCT of:	
			UDINT	Device IP address
			ARRAY of 6 USINTs	Device MAC address
10	Active Supervisor Address	Get	STRUCT of:	IP and/or MAC address of the active ring supervisor
			UDINT	Supervisor IP address
			ARRAY of 6 USINTs	Supervisor MAC Address
11	Active Supervisor Precedence	Get	USINT	Precedence value of the active ring supervisor
12	Capability Flags	Get	DWORD	Describes the DLR capabilities of the device (1)

Table 7-20 6.3 Services

Service code	Class	Instance	Name of service
0x01	X	X	Get_Attribute_All
0x0E	X	X	Get_Attribute_Single
0x10	-	X	Set_Attribute_All
0x18		X	Get_Member

Table 7-21 6.4 Services

Service code	Class	Instance	Name of service
0x4B	-	X	Verify_Fault_Location
0x4C	-	X	Clear_Rapid_Faults
0x4D	-	X	Restart_Sign_On

7.1.7 Simple Network Management (SNMP) object (class code 0x52)

Table 7-22 7.1 Class attributes

ID	Attributes	Access rule	Data type	Description
1	Revision	Get	UINT	Revision of this object

Table 7-23 7.2 Instance attributes

ID	Attributes	Access rule	Data type	Description
1	SnmpAgent	Get	USINT	Status of the SNMP agent
2	SnmpAgentVersion	Get	USINT	Version of SNMP agent provided (1=SNMPv1, 3=SNMPv3; 31=SNMPv1 + v3)
3	Primary Network Management Identifier	Get	STRUCT of:	Network address of primary network manager
	Identifier Format		USINT	Type of identifier
	Identifier		STRING	Value of identifier

Table 7-23 7.2 Instance attributes

ID	Attributes	Access rule	Data type	Description
4	Secondary Network Management Identifier	Get	STRUCT of:	Network address of primary network manager
	Identifier Format		USINT	Type of identifier
	Identifier		STRING	Value of identifier
5	Notifications	Get	BOOL	Indicates if the SNMP agent will enable the sending of notifications 5
6	TrapType	Get	USINT	Indicates which trap type the SNMP agent will send 6

Table 7-24 7.3 Services

Service code	Class	Instance	Name of service
0x0E	-	X	Get_Attribute_Single

Table 7-25 7.4 Specific services

Service code	Class	Instance	Name of service
0x0E	X	X	Get_Attribute_Single

7.1.8 QoS object (class code 48)

Table 7-26 8.1 Class attributes

ID	Attributes	Access rule	Data type	Description
1	Revision	Get	UINT	Revision of this object

Table 7-27 8.2 Instance attributes

ID	Attributes	Access rule	Data type	Description
4	DSCP Urgent	Set	USINT	DSCP value for CIP transport class 0/1 urgent priority messages
5	DSCP Schedule	Set	USINT	DSCP value for CIP transport class 0/1 scheduled priority messages

Table 7-27 8.2 Instance attributes

ID	Attributes	Access rule	Data type	Description
6	DSCP High	Set	USINT	DSCP value for CIP transport class 0/1 high priority messages
7	DSCP Low	Set	USINT	DSCP value for CIP transport class 0/1 low priority messages
8	DSCP Explicit	Set	USINT	DSCP value for CIP explicit messages (transport class 2/3 and UCMM) and all other EtherNet/IP encapsulation messages

Table 7-28 8.3 Services

Service code	Class	Instance	Name of service
0x0E	X	X	Get_Attribute_Single
0x10		X	Set_Attribute_Single

Table 7-29 8.4 Services

Service code	Class	Instance	Name of service
0x0E	-	X	Get_Attribute_Single
0x10	-	X	Set_Attribute_Single

7.1.9 Base Switch object (class code 51)

Table 7-30 9.1 Class attributes

ID	Attributes	Access rule	Data type	Description
1	Revision	Get	UINT	Revision of this object

Table 7-31 9.2 Instance attributes

ID	Attributes	Access rule	Data type	Description
1	Device Up Time	Get	UDINT	Revision of this object
2	Total port count	Get	UDINT	Number of physically available ports
3	System Firmware Version	Get	SHORT_STRING	Human readable representation of system firmware version

Table 7-31 9.2 Instance attributes

ID	Attributes	Access rule	Data type	Description	
4	Power Source	Get	Word	Bits 0 - 1	Status of switch power source 1 00 = Not present 01 = Not powered 11 = Powered and OK
				Bits 2 - 3	Status of switch power source 2 00 = Not present 01 = Not powered 11 = Powered and OK
5	Port Mask Size	Get	UINT	Number of DWORDs in port array attributes	
6	Existing Ports	Get	ARRAY OF DWORD	Port mask Indicates whether a port is absent or present	
7	Global Port Admin State	Get, Set	ARRAY of DWORD	Port admin status	
8	Global Port Link Status	Get	ARRAY of DWORD	Port link status	
9	System Boot Loader Version	Get	SHORT_STRING	Human readable representation of system firmware version	
10	Contact Status	Get	WORD	Switch contact closure	

Table 7-32 9.3 Services

Service code	Class	Instance	Name of service
0x0E	X	X	Get_Attribute_Single

Table 7-33 9.4 Services

Service code	Class	Instance	Name of service
0x0E	-	X	Get_Attribute_Single
0x10	-	X	Set_Attribute_Single

7.1.10 Assembly object

Table 7-34 10.1 Class attributes

ID	Attributes	Access rule	Data type	Description
1	Revision	Get	UINT	Revision of this object
2	Max Instance	Get	UINT	Maximum instance number of this object
3	Number of Instance	Get	UINT	Instance number of this object
4	Optional attribute List	Get	STRUCT of:	List of optional instance attributes used in an object class implementation
	Number of attributes		UINT	Number of attributes in the optional attribute list
	Optional attributes		ARRAY of UINT	Optional attributes
6	Maximum ID Number Instance class Attributes	Get	UINT	Attribute ID number of the last class attribute of the class definition implemented in the device
7	Maximum ID Number Instance Attributes	Get	UINT	Attribute ID number of the last instance attribute of the class definition implemented in the device

Table 7-35 10.3 Services

Service code	Class	Instance	Name of service
0x0E	X	X	Get_Attribute_Single
0x10	-	X	Set_Attribute_Single

7.1.11 Input assemblies

Connection ID: T->O: 101: Input assembly

Table 7-36 11.1 Input assemblies

Description	Length of data	Data format	Remarks
Port admin mode	4 bytes	Array of BOOL values (1 = enabled)	LSB = Any port summary bit LSB + 1 = Port 1 e.g., 0x05 means at least one port enabled and port 2 enabled
Port link status	4 bytes	Array of BOOL values (1 = link up)	LSB = Any port summary bit LSB + 1 = Port 1 e.g., 0x05 means at least one port has link up and port 2 has link up
Padding	24 bytes	-	Reserved for future

Table 7-36 11.1 Input assemblies

Description	Length of data	Data format	Remarks
Port RX utilization percentage	24 bytes	SINT values representing the utilization percentage	1st byte representing port 1; if less than 24 bytes are supported, further bytes will be padding bytes
Port TX utilization percentage	24 bytes	SINT values representing the utilization percentage	1st byte representing port 1; if less than 24 bytes are supported, further bytes will be padding bytes
Alarm contact status	1 byte	Array of BOOL values (1 = contact open = fail condition)	Value similar to EIP Base Switch object (51Hex) instance attribute 10
Power supply status	1 byte	Array of BOOL values (1 = power supply present)	Value similar to EIP Base Switch object (51Hex) instance attribute 4
DLR supervisor status	1 byte	SINT value	Value similar to EIP DLR object (47hx) instance attribute 3
DLR network status	1 byte	SINT value	Value similar to EIP DLR object (47hx) instance attribute 2
Padding	4 bytes	-	Reserved for future

7.1.12 Output assemblies

Connection ID: O->T: 100: Output assembly

Description	Length of data	Data format	Remarks
Admin port status	4 bytes	Array of BOOL values (1 = enabled)	LSB = Disable all ports e.g., 0x0E means that only ports 1, 2 and 3 are enabled

7.1.13 Power source and link status assembly

Connection ID: 1: Power source and link status assembly

Table 7-37 13.1 Power source and link status assembly

Byte	Data type	Description
0	BYTE	Power source status (least significant byte)
1	BYTE	Power source status (most significant byte)
2 - 5	DWORD	Global link status (ports 1 – 4)
6 - 9	DWORD	Global link status (ports 5 – 8)

8 Multicast filtering

8.1 Multicast configuration

“Multicast Configuration” web page

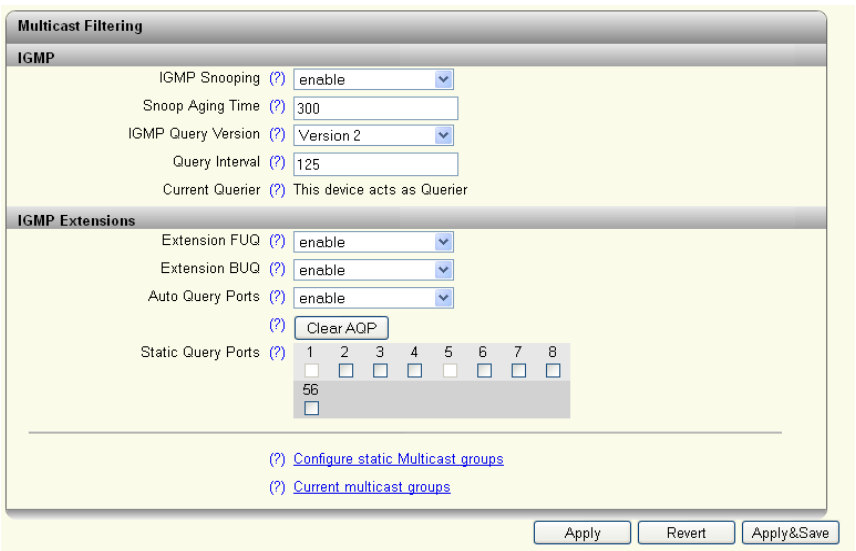


Figure 8-1 “Multicast Configuration” web page

IGMP Snooping:

– Disable: The IGMP snooping function is deactivated.
– Enable: The “IGMP Snooping” function is activated.

Snoop Aging Time: The snoop aging time can be set here. The snoop aging 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 here, with which the switch should send the queries.

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

Extensions 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): Here you can set whether unknown multicast packets should be blocked at the querier.

Auto Query Ports: Here you can set, whether the automatic selection of additional query ports is activated by means of fast ring detection and/or DLR. 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 deletion of the ports automatically assigned to the groups.

Static Query Ports: Select the ports that are static query ports.

By clicking on the “Static multicast group configuration” button, you can access the web page to create static multicast groups.

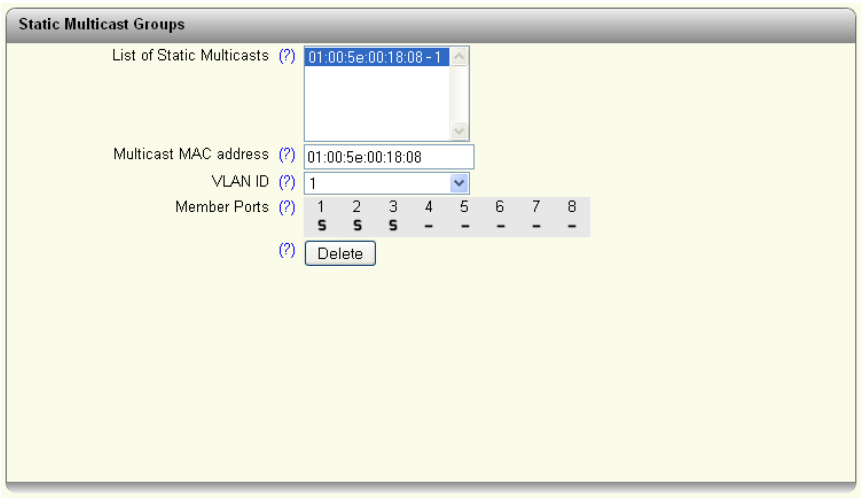


Figure 8-2 “Static Multicast Groups” web page

List of Static Multicasts: List of all static multicast groups created.

Multicast MAC address: Enter the multicast MAC address here.

VLAN ID: Enter the VLAN here.

Member Ports: Select here the ports which should be entered into the multicast group.

S: Static - Static member in the multicast group.

F: Forbidden - The port cannot be dynamically added to multicast groups. As such, the port is always excluded from the multicast group.

-: No Member - No member in the multicast group.

Delete: The selected multicast group is deleted.

You can compile up to 32 static multicast groups.

By clicking on the “Current Multicast Table” button, you receive an overview of the current multicast groups.

The device can manage up to 512 dynamic multicast groups.

9 Virtual Local Area Network - VLAN

“Configuration/VLAN configuration” web page

Figure 9-1 “VLAN configuration” web page

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 is 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.

By clicking on the “Static VLAN” button, you can access the “Static VLAN Configuration” page. Up to 32 static VLANs can be set up here.

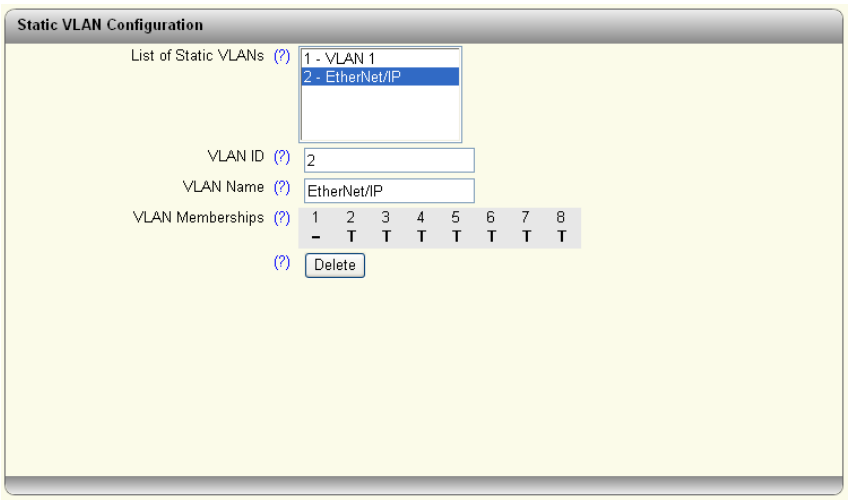


Figure 9-2 “Static VLAN Configuration” page

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

VLAN ID: Set the VLAN ID here, which you wish to assign to the new VLAN. The value must be between 2 and 4095.

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

-: No member in the VLAN

Using the “Delete” button, you can delete the VLAN selected in the list.

The VLAN 1 cannot be deleted.

By clicking on the “VLAN Port configuration” button, you can access the “VLAN Port configuration” page.

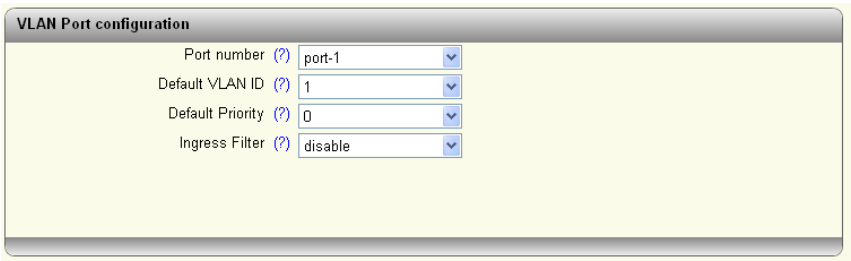


Figure 9-3 “VLAN Port configuration” web page

Port number: Enter the port which you are changing the VLAN settings for.

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 whether the ingress filter should be activated here.

By clicking on the “VLAN Port Table” button, you can access the VLAN port configuration table.

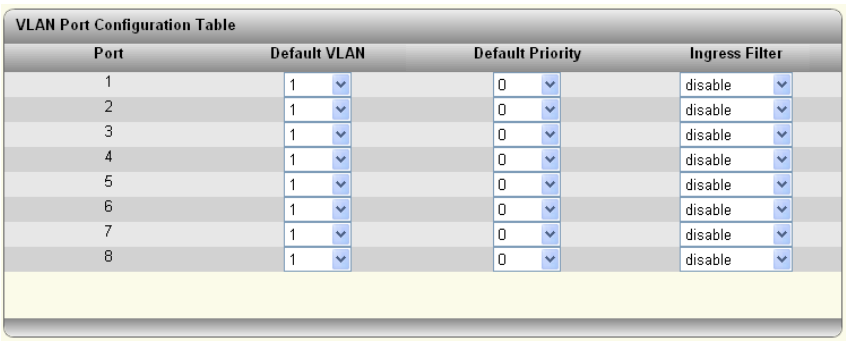


Figure 9-4 “VLAN Port Configuration Table” web page

By clicking on the “Current VLANs” button, you can access a page on which all active VLANs are displayed, with the corresponding ports.

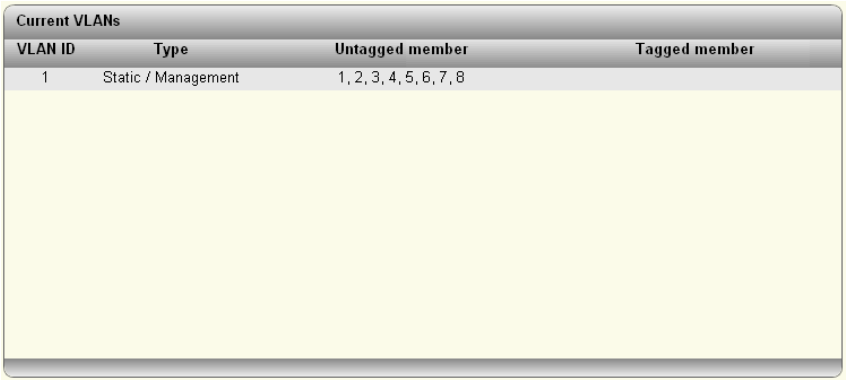


Figure 9-5 “Current VLANs” web page

10 Technical data and ordering data

10.1 Technical data

General data	
Function	Ethernet/Fast Ethernet switch; conforms to standard IEEE 802.3/802.3u/802.3ab
Switch principle	Store-and-forward
Address table	16386 MAC addresses
SNMP	Version 2c
Transmission capacity per port 64-byte packet size, half duplex	At 10 Mbps: 14880 pps (packets per second) At 100 Mbps: 148800 pps
Supported MIBs	MIB II and private SNMP objects from Phoenix Contact
Housing dimensions (width x height x depth) in mm	60 x 130 x 136 (depth from top edge of DIN rail)
Permissible operating temperature	-40°C ... 70°C
Permissible storage temperature	-40°C ... +85°C
Degree of protection	IP20, IEC 60529
Protection class	Class 3 VDE 0106; IEC 60536
Humidity	
Operation	10% ... 95%, non-condensing
Storage	10% ... 95%, non-condensing
Air pressure	
Operation	86 kPa ... 108 kPa, 1500 m above sea level
Storage	66 kPa ... 108 kPa, 3500 m above sea level
Ambient compatibility	Free from substances that would hinder coating with paint or varnish according to VW specification
Mounting position	Perpendicular to a standard DIN rail
Connection to protective earth ground	By snapping it onto a grounded DIN rail
Weight	Typically up to 1000 g

Supply voltage (US1/US2 redundant)	
Connection	Via COMBICON; maximum conductor cross section = 2.5 mm^2
Nominal value	24 V DC
Permissible voltage range	12 V DC ... 58 V DC
Permissible ripple (within the permissible voltage range)	3.6 V_{PP}
Test voltage	500 V DC for one minute
Current consumption at US at 24 V DC, maximum	350 mA (FL SWITCH 7008-EIP) 470 mA (FL SWITCH 7006/2FX-EIP) 520 mA (FL SWITCH 7005/FX-2FXSM-EIP)
Maximum power consumption	8.4 W (FL SWITCH 7008-EIP) 11.3 W (FL SWITCH 7006/2FX-EIP) 12.8 W (FL SWITCH 7005/FX-2FXSM-EIP)

Interfaces

Number of Ethernet ports	8
Floating signal contact	
Voltage	12 ... 58 V DC/60 W, maximum
Current carrying capacity	100 mA, typical; 1 A, maximum

Ethernet interfaces

Properties of RJ45 ports	
Number	Up to 8 with autocrossing and autonegotiation
Connection format	8-pos. RJ45 socket on the switch
Connection medium	Twisted-pair cable with a conductor cross section of 0.14 mm^2 ... 0.22 mm^2
Cable impedance	100 ohms
Transmission speed	10/100 Mbps
Maximum network segment expansion	100 m
General properties of fiberglass ports	
Number	Up to 3
Connection format	SC format
Connection medium	Fiberglass
Connector plug	SC format
Transmission speed	100 Mbps
Laser protection class	1
Properties of 100 Mbps multi-mode ports in SC format	
Data transmission speed	100 Mbps, full duplex
Wavelength	1310 nm
Maximum transmission length	10 km fiberglass with F-G 50/125 µm 0.7 dB/km F1200 4.4 km fiberglass with F-G 50/125 µm 1.6 dB/km F800 17 km fiberglass with F-G 62.5/125 µm 0.7 dB/km F1000 4.6 km fiberglass with F-G 62.5/125 µm 2.6 dB/km F600
Transmission power	
Minimum	-19 dBm 62.5/125 µm -24 dBm 50/125 µm
Maximum	-14 dBm
Receiver sensitivity	
Minimum	-34 dBm
Properties of 100 Mbps single-mode ports in SC format	
Data transmission speed	100 Mbps, full duplex
Wavelength	1310 nm
Maximum transmission length	44 km fiberglass with F-G 9/125 µm 0.36 dB/km 40 km fiberglass with F-G 9/125 µm 0.4 dB/km 32 km fiberglass F-G 9/125 µm 0.5 dB/km
Transmission power	
Minimum	-15 dBm 9/125 µm
Maximum	-7 dBm
Receiver sensitivity	
Minimum	-34 dBm

Mechanical tests

Shock test according to IEC 60068-2-27	Operation: 30g, 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 + A1: 2000 + A2: 2003 (interference voltage)	Class A (industrial applications)
Noise emission according to EN55011: 1998 + A1: 1999 + A2: 2002 (electromagnetic interference)	Class A (industrial applications)
Noise immunity according to EN 61000-4-2 (IEC1000-4-2) (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) (electromagnetic fields)	Requirements according to DIN EN 61000-6-2 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 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 certification

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

Differences between this version and previous versions

Rev. 00: First version

10.2 Ordering data

Products

Description	Order designation	Order No.	Pcs. / Pkt.
Managed Switch with eight Fast Ethernet ports in RJ45 format	FL SWITCH 7008-EIP	2701418	1
Managed switch with six Fast Ethernet ports in RJ45 format and two SC ports in SC format	FL SWITCH 7006/2FX-EIP	2701419	1
Managed Switch with five Fast Ethernet ports in RJ45 format, two single-mode ports and one multi-mode port in SC format	FL SWITCH 7005/FX-2FXSM-EIP	2701420	1
Replaceable configuration memory	FL SD-FLASH 512 MB	2989146	1

Accessories

Description	Order designation	Order No.	Pcs. / Pkt.
Universal end bracket	E/NS 35 N	0800886	1
Network monitoring with HMI/SCADA systems	FL SMNP OPC SERVER	2832166	1
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 mm², 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
Patch box 8 x RJ45 CAT5e, pre-assembled, can be retrofitted	FL PBX 8TX	2832496	1
Patchbox 6 x RJ45 CAT5e and 4 SC-RJ, fiberglass cable pre-assembled, can be retrofitted	FL PBX 6TX/4FX	2832506	1
Angled patch connector with two RJ45 CAT5e network connections including Layer 1 security elements	FL PF SEC 2TX	2832687	1
Angled patch connector with eight RJ45 CAT5e network connections including Layer 1 security elements	FL PF SEC 8TX	2832690	1
Angled patch connector with two RJ45 CAT5e network connections	FL PF 2TX CAT5E	2891165	1
Angled patch connector with eight RJ45 CAT5e network connections	FL PF 8TX CAT5E	2891178	1
Angled patch connector with two RJ45 CAT6 network connections	FL PF 2TX CAT 6	2891068	1
Angled patch connector with eight RJ45 CAT6 network connections	FL PF 8TX CAT 6	2891071	1
Patch cable, CAT**6**, pre-assembled, 0.3 m long	FL CAT6 PATCH 0,3	2891181	10
Patch cable, CAT**6**, pre-assembled, 0.5 m long	FL CAT6 PATCH 0,5	2891288	10
Patch cable, CAT**6**, pre-assembled, 1.0 m long	FL CAT6 PATCH 1,0	2891385	10
Patch cable, CAT**6**, pre-assembled, 1.5 m long	FL CAT6 PATCH 1,5	2891482	10
Patch cable, CAT**6**, pre-assembled, 2.0 m long	FL CAT6 PATCH 2,0	2891589	10
Patch cable, CAT**6**, pre-assembled, 3.0 m long	FL CAT6 PATCH 3,0	2891686	10
Patch cable, CAT**6**, pre-assembled, 5.0 m long	FL CAT6 PATCH 5,0	2891783	10
Patch cable, CAT**6**, pre-assembled, 7.5 m long	FL CAT6 PATCH 7,5	2891880	10
Patch cable, CAT**6**, pre-assembled, 10 m long	FL CAT6 PATCH 10	2891887	10
Patch cable, CAT**6**, pre-assembled, 12.5 m long	FL CAT6 PATCH 12,5	2891369	5
Patch cable, CAT**6**, pre-assembled, 15 m long	FL CAT6 PATCH 15	2891372	5
Patch cable, CAT**6**, pre-assembled, 20 m long	FL CAT6 PATCH 20	2891576	5

Description (Fortsetzung)	Order designation	Order No.	Pcs. / Pkt.
Patch cable, CAT5, pre-assembled, 0.3 m long	FL CAT5 PATCH 0,3	2832250	10
Patch cable, CAT5, pre-assembled, 0.5 m long	FL CAT5 PATCH 0,5	2832263	10
Patch cable, CAT5, pre-assembled, 1.0 m long	FL CAT5 PATCH 1,0	2832276	10
Patch cable, CAT5, pre-assembled, 1.5 m long	FL CAT5 PATCH 1,5	2832221	10
Patch cable, CAT5, pre-assembled, 2.0 m long	FL CAT5 PATCH 2,0	2832289	10
Patch cable, CAT5, pre-assembled, 3.0 m long	FL CAT5 PATCH 3,0	2832292	10
Patch cable, CAT5, pre-assembled, 5.0 m long	FL CAT5 PATCH 5,0	2832580	10
Patch cable, CAT5, pre-assembled, 7.5 m long	FL CAT5 PATCH 7,5	2832616	10
Patch cable, CAT5, pre-assembled, 10.0 m long	FL CAT5 PATCH 10	2832629	10
Color coding for FL CAT5/6 PATCH ..., black	FL PATCH CCODE BK	2891194	20
Color coding for FL CAT5/6 PATCH ..., brown	FL PATCH CCODE BN	2891495	20
Color coding for FL CAT5/6 PATCH ..., blue	FL PATCH CCODE BU	2891291	20
Color coding for FL CAT5/6 PATCH ..., green	FL PATCH CCODE GN	2891796	20
Color coding for FL CAT5/6 PATCH ..., gray	FL PATCH CCODE GY	2891699	20
Color coding for FL CAT5/6 PATCH ..., red	FL PATCH CCODE RD	2891893	20
Color coding for FL CAT5/6 PATCH ..., violet	FL PATCH CCODE VT	2891990	20
Color coding for FL CAT5/6 PATCH ..., yellow	FL PATCH CCODE YE	2891592	20
Lockable security element for FL CAT5/6 PATCH ...	FL PATCH GUARD	2891424	20
Color coding for FL PATCH GUARD, black	FL PATCH GUARD CCODE BK	2891136	12
Color coding for FL PATCH GUARD, blue	FL PATCH GUARD CCODE BU	2891233	12
Color coding for FL PATCH GUARD, green	FL PATCH GUARD CCODE GN	2891631	12
Color coding for FL PATCH GUARD, orange	FL PATCH GUARD CCODE OG	2891330	12
Color coding for FL PATCH GUARD, red	FL PATCH GUARD CCODE RD	2891738	12
Color coding for FL PATCH GUARD, turquoise	FL PATCH GUARD CCODE TQ	2891534	12
Color coding for FL PATCH GUARD, violet	FL PATCH GUARD CCODE VT	2891835	12
Color coding for FL PATCH GUARD, yellow	FL PATCH GUARD CCODE YE	2891437	12
Key for FL PATCH GUARD	FL PATCH GUARD KEY	2891521	1
Security element for FL CAT5/6 PATCH ...	FL PATCH SAFE CLIP	2891246	20

HOTLINE:

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


+ 49 - (0) 52 81 - 946 28 88

A Appendix for document lists

A 1 List of figures

B 1 List of tables

C 1 Index

Numerics

A

B

C

D

E