AUTOMATION

User manual

UM EN FL SWITCH LM

Order No.: 2888851

Hardware and software for Lean Managed Switches

PHOENIX CONTACT
INSPIRING INNOVATIONS

AUTOMATION

User manual

Hardware and software for Lean Managed Switches

2011-09-01

Designation: UM EN FL SWITCH LM

Revision: 05

Order No.: 2888848

This user manual is valid for:

Designation	Oder No.
FL SWITCH LM 8TX / FL SWITCH LM 8TX-E	2832632 / 2891466
FL SWITCH LM 4TX/2FX / FL SWITCH LM 4TX/2FX-E	2832658 / 2891660
FL SWITCH LM 4TX/2FX SM / FL SWITCH LM 4TX/2FX SM-E	2891916 / 2891864
FL SWITCH LM 5TX/FL SWITCH LM 5TX-E	2989527 / 2989336
FL SWITCH LM 4TX/2FX ST/FL SWITCH LM 4TX/2FX ST-E	2989132 / 2989831
FL SWITCH LM 4TX/2FX SM ST/FL SWITCH LM 4TX/2FX SM ST-E	2989239 / 2989938
FL SWITCH LM 4TX/1FX/FL SWITCH LM 4TX/1FX-E	2989624 / 2989433
FL SWITCH LM 4TX/1FX ST/FL SWITCH LM 4TX/1FX ST-E	2989721 / 2989530
FL SWITCH LM 4TX/1FX SM/FL SWITCH LM 4TX/1FX SM-E	2989828 / 2989637
FL SWITCH LM 4TX/1FX SM ST/FL SWITCH LM 4TX/1FX SM ST-E	2989925 / 2989734

Please observe the following notes

In order to ensure the safe use of the product described, you have to read and understand this manual. The following notes provide information on how to use this manual.

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.

Phoenix Contact accepts no liability for erroneous handling or damage to products from Phoenix Contact or third-party products resulting from disregard of information contained in this manual.

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 messages that follow this symbol to avoid possible injury or death.

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.

The following types of messages provide information about possible property damage and general information concerning proper operation and ease-of-use.

NOTE
This symbol and the accompanying text alerts the reader to a situation which may cause damage or malfunction to the device, either hardware or software, or surrounding property.

This symbol and the accompanying text provides additional information to the reader. It is also used as a reference to other sources of information (manuals, data sheets, literature) on the subject matter, product, etc.

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 data sheets, installation instructions, manuals, etc.) does not constitute any further duty on the part of Phoenix Contact to furnish information on alterations to products and/or technical documentation. Any other agreement shall only apply if expressly confirmed in writing by Phoenix Contact. Please note that the supplied documentation is product-specific documentation only and that you are responsible for checking the suitability and intended use of the products in your specific application, in particular with regard to observing the applicable standards and regulations. Although Phoenix Contact makes every effort to ensure that the information content is accurate, up-to-date, and state-of-the-art, technical inaccuracies and/or printing errors in the information cannot be ruled out. Phoenix Contact does not offer any guarantees as to the reliability, accuracy or completeness of the information. All information made available in the technical data is supplied without any accompanying guarantee, whether expressly mentioned, implied or tacitly assumed. This information does not include any guarantees regarding quality, does not describe any fair marketable quality, and does not make any claims as to quality guarantees or guarantees regarding the suitability for a special purpose.

Phoenix Contact accepts no liability or responsibility for errors or omissions in the content of the technical documentation (in particular data sheets, installation instructions, manuals, etc.).

The aforementioned limitations of liability and exemptions from liability do not apply, in so far as liability must be assumed, e.g., according to product liability law, in cases of premeditation, gross negligence, on account of loss of life, physical injury or damage to health or on account of the violation of important contractual obligations. Claims for damages for the violation of important contractual obligations are, however, limited to contract-typical, predictable damages, provided there is no premeditation or gross negligence, or that liability is assumed on account of loss of life, physical injury or damage to health. This ruling does not imply a change in the burden of proof to the detriment of the user.

Statement of legal authority

How to contact us

Internet

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

www.phoenixcontact.com.

Make sure you always use the latest documentation.
It can be downloaded at:

www.phoenixcontact.net/catalog.

Subsidiaries

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

Published by

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
GERMANY
Phone +49 - (0) 52 35 - 3-00
Fax +49 - (0) 52 35 - 3-4 12 00

PHOENIX CONTACT
P.O. Box 4100
Harrisburg, PA 17111-0100
USA
Phone +1-717-944-1300

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.

Table of contents

1 Lean Managed Switch

1.1 Properties

The **L**ean **M**anaged **S**witch (**LMS**) is an Ethernet switch, which is suitable for industrial use. The LMS has five, six or eight ports and is available in various versions:

- FL SWITCH LM 5TX(-E) with five RJ45 ports
- FL SWITCH LM 8TX(-E) with eight RJ45 ports
- FL SWITCH LM 4TX/FX(-E) with four RJ45 ports and one FX port (multi-mode)
- FL SWITCH LM 4TX/FX ST(-E) with four RJ45 ports and one FX port (multi-mode) in ST format
- FL SWITCH LM 4TX/FX SM(-E) with four RJ45 ports and one FX port (single-mode)
- FL SWITCH LM 4TX/FX ST SM(-E) with four RJ45 ports and one FX port (single-mode) in ST format
- FL SWITCH LM 4TX/2FX ST(-E) with four RJ45 ports and two FX ports (multi-mode) in ST format
- FL SWITCH LM 4TX/2FX(-E) with four RJ45 ports and two FX ports (multi-mode)
- FL SWITCH LM 4TX/2FX SM(-E) with four RJ45 ports and two FX ports (single-mode)
- FL SWITCH LM 4TX/2FX SM ST(-E) with four RJ45 ports and two FX ports (single-mode) in ST format

Figure 1-1 Some versions of the Lean Managed Switch

Future-proof networks for the highest possible requirements

Maximum availability

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

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

All information

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

Features and fields of application of the LMS

– Increased network performance by filtering data traffic:
  - Local data traffic remains local.
  - The data volume in the network segments is reduced.
– Easy network expansion and network configuration.
– Coupling segments with different transmission speeds.
  Automatic detection of 10 Mbps or 100 Mbps data transmission speed for the RJ45 ports.
– Increased availability through the use of redundant transmission paths in various topologies and meshed structures as a result of RSTP.
– The switch can be configured using web-based management, SNMP or locally via an RS-232 interface.

1.1.1 Front view/operating elements/ slots of the LMS

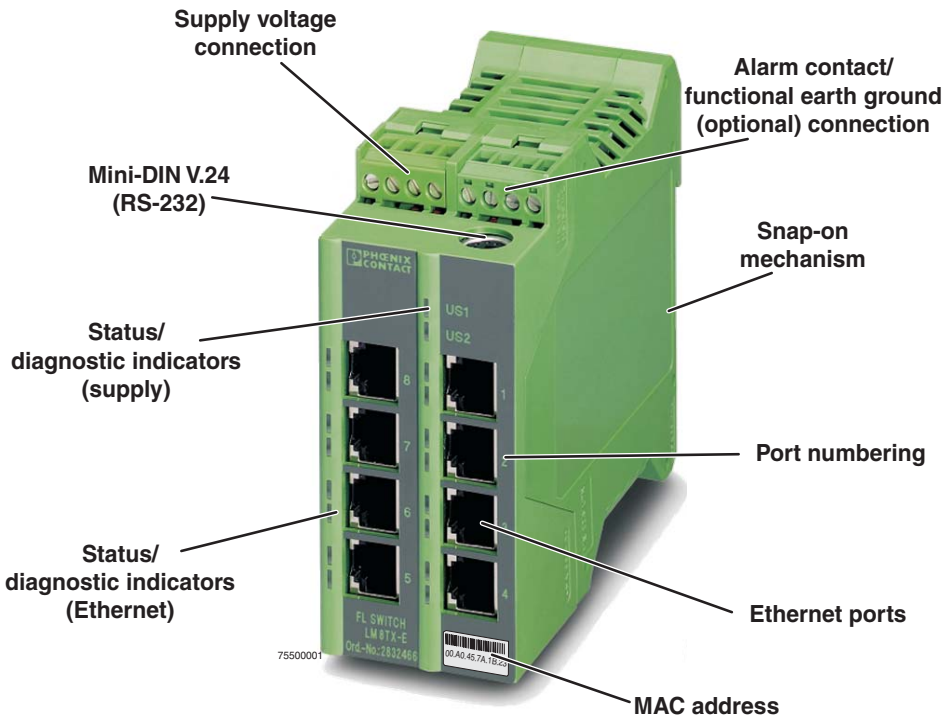


Figure 1-2 Front view/operating elements/slots of the LMS

– Diagnostic/status indicators
  Important information is displayed directly on the device. Each port has two LEDs. The top LED always indicates "LNK/ACT", the bottom LED indicates the data transmission speed.
– Diagnostic and status LEDs
  Two status and diagnostic LEDs are available for the supply voltage and for each port.
– Mini-DIN RS-232
  RS-232 interface in Mini-DIN format for local configuration via the serial interface.
– Alarm contact/functional earth ground
  The floating alarm contact and the optional functional earth ground can be connected here via the COMBICON connector.
– Supply voltage connection
  The supply voltage can also be connected redundantly via the 4-pos. COMBICON connector as an option.

1.1.2 Dimensions of the LMS

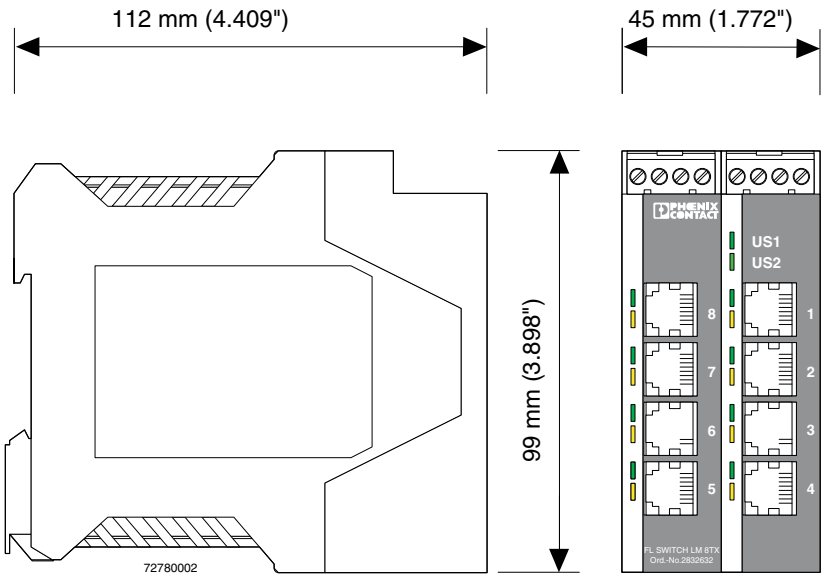


Figure 1-3 Housing dimensions of the LMS in millimeters (inches)

1.1.3 Status and diagnostic indicators

Des.	Color	Status	Meaning
US1	Green	ON	Supply voltage US1 in the tolerance range
		OFF	Supply voltage US1 less than 18 V DC
US2	Green	ON	Supply voltage US2 in the tolerance range
		OFF	Supply voltage US2 less than 18 V DC
LNK	Green	ON	Link active
		OFF	Link not active
		Flashing	Transmitting/receiving
100	Yellow	ON	Full duplex mode
		OFF	Half duplex mode
		Flashing	Collision detected

1.1.4 Firmware versions and their functions

1.1.4.1 For the following switch versions (LM)

– FL SWITCH LM 8TX
– FL SWITCH LM 4TX/2FX
– FL SWITCH LM 4TX/2FX SM

Firmware Version 1.04 provides the standard switch functions.

Firmware 2.02 offers the following additional functions:

– Multicast filter mechanisms
– IGMP snooping and querier function
– Port mirroring
– Port statistics
– Link status via alarm contact
– MAC address clearing

Firmware 2.13 offers the following additional functions:

– Optimized IGMP function, query port is not entered in GDA
– Optimized Rapid Spanning Tree Protocol (RSTP), RSTP function optimized in connection with fiberglass FX port

Firmware 3.03 offers the following additional functions:

– Optimized Rapid Spanning Tree Protocol (RSTP)
– Optimized IGMP snooping and querier function
– RSTP extension: Fast ring detection
– RSTP extension: Large tree support
– BootP and IP parameter storage optimized
– Ping requests > 1500 bytes are answered

Firmware 3.10 offers the following additional functions:

The following versions are supported:
FL SWITCH LM 5TX
FL SWITCH LM 4TX/1FX
FL SWITCH LM 4TX/1FX ST
FL SWITCH LM 4TX/1FX SM
FL SWITCH LM 4TX/1FX SM ST
FL SWITCH LM 4TX/2FX ST
FL SWITCH LM 4TX/2FX SM ST

Firmware 3.40 offers the following additional functions:

– Saving and loading configurations
– Port mirroring/link mirroring
– DHCP server
– Extended multicast filtering

1.1.4.2 For the following switch versions (LM-E)

Firmware 1.11 supports the following versions:

– FL SWITCH LM 8TX-E
– FL SWITCH LM 4TX/2FX-E
– FL SWITCH LM 4TX/2FX SM-E

Firmware 3.40 additionally supports the following versions:

– 2989336 FL SWITCH LM 5TX-E
– 2989433 FL SWITCH LM 4TX/1FX-E
– 2989530 FL SWITCH LM 4TX/1FX ST-E
– 2989637 FL SWITCH LM 4TX/1FX SM-E
– 2989734 FL SWITCH LM 4TX/1FX SM ST-E
– 2989831 FL SWITCH LM 4TX/2FX ST-E
– 2989938 FL SWITCH LM 4TX/2FX SM ST-E

1.2 Mounting/removal

1.2.1 Mounting and removing the LMS

Mount the LMS on a clean DIN rail according to DIN EN 50 022 (e.g., NS 35 ... from Phoenix Contact). To avoid contact resistance only use clean, corrosion-free DIN rails. Before mounting the modules, an end clamp (E/NS 35N, Order No. 0800886) should be mounted on the left-hand side next to the LMS to stop the modules from slipping on the DIN rail. The end clamp should only be mounted on the right-hand side once the LMS has been mounted.

1.2.2 Mounting

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

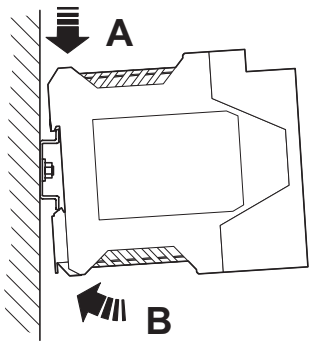


Figure 1-4 Snapping the LMS onto the DIN rail

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

1.2.3 Removal

1. Remove all plug-in connections.
2. Pull down the positive latches using a suitable tool (e.g., screwdriver). Both positive latches remain snapped out. Then swivel the bottom of the module away from the DIN rail slightly (A). Next, lift the module upwards away from the DIN rail (B).

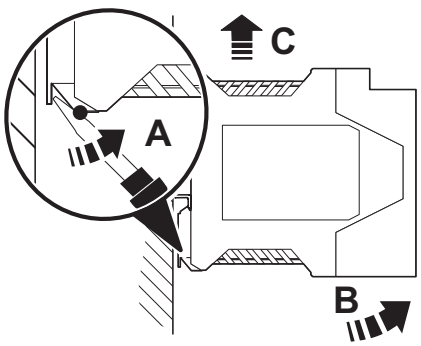


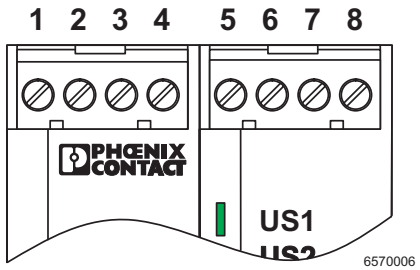
Figure 1-5 Removing the LMS

1.3 Installing the Lean Managed Switch

1.3.1 Connecting the supply voltage

1.3.1.1 Assignment of the COMBICON connector

Terminal block	Meaning
1	Supply voltage +US1
2	GND US1
3	Supply voltage +US2
4	GND US2
5 and 6	Floating alarm contact
7	Functional earth ground (optional)
8	Not used



NOTE: The switch is designed for SELV/PELV operation at +24 V DC according to IEC 60950-1/VDE 0805. Only SELV/PELV according to the defined standards may be used for supply purposes.

24 V DC

The LMS is operated with a 24 V DC voltage that can be supplied redundantly, if required (see Figure 1-6 version 2).

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. However, it is also possible to deactivate monitoring in web-based management.

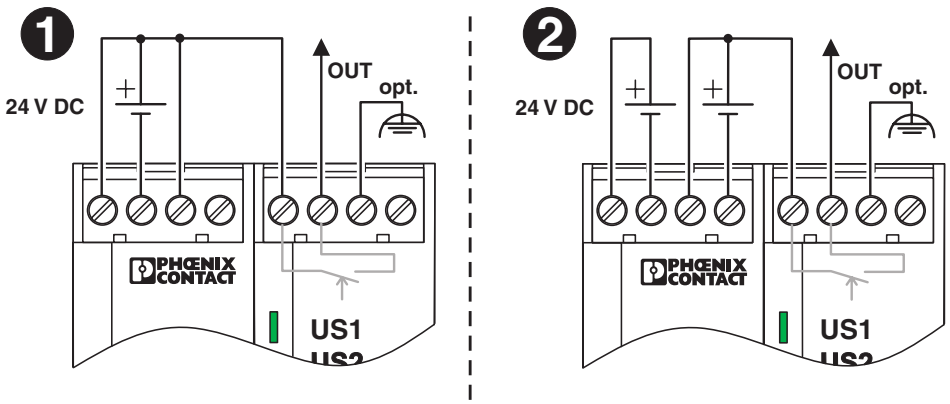


Figure 1-6 LMS supply

1.3.2 Alarm contact

The switch has a floating alarm contact. An error is indicated when the contact is opened.

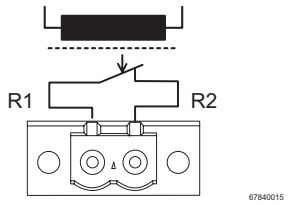


Figure 1-7 Basic circuit diagram for the alarm contact

In the event of non-redundant power supply, the switch indicates a supply voltage failure by opening the alarm contact. This error message can be prevented by connecting the supply voltage to both terminals blocks in parallel, as shown in Figure 1-6, or by deactivating redundant power supply monitoring in web-based management.

1.3.3 RS-232 interface for external management

The 6-pos. Mini-DIN female connector provides a serial interface to connect a local management station. Use the "PRG CAB MINI DIN" programming cable (Order No. 2730611). It can be used to connect a VT100 terminal or a PC with corresponding terminal emulation to the management interface (for an appropriate cable, please refer to "Ordering data" on page 7-3). Set the following transmission parameters:

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

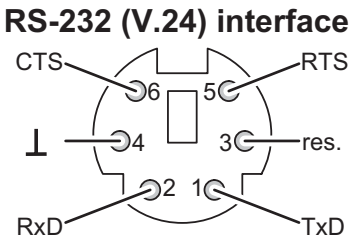


Figure 1-8 Transmission parameters and assignment of the RS-232 interface

1.3.4 Grounding

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

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

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

Option: In an environment particularly prone to EMI, noise immunity can be increased by an additional low-impedance connection to functional earth ground via terminal block 7 (Section "Assignment of the COMBICON connector" on page 1-7).

2 Startup and functions

NOTE: The IGMP snooping function is activated by default upon delivery for "**E**" versions. For other versions, it can be activated as necessary in WBM.

2.1 Basic settings

The basic Ethernet functions do not have to be configured and are available when the supply voltage is switched on.

2.1.1 Default upon delivery/default settings

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

- The password is "private".
- All IP parameters are deleted. The switch has **no** valid IP parameters:
  IP address: 0.0.0.0
  Subnet mask: 0.0.0.0
  Gateway: 0.0.0.0
- BootP is activated as the addressing mechanism.
- All available ports are activated with the following parameters:
  - Auto negotiation and autocrossing for RJ45 ports.
  - 100 Mbps - full duplex for FX ports.
- All information collected by the SNMP agent is deleted.
- The web server, SNMP agent, and RS-232 interface are active.
- The "Rapid Spanning Tree" WBM configuration page is activated.
- The alarm contact only opens in the event of non-redundant power supply.
- The aging time is set to 48 seconds.

2.1.2 Assigning IP parameters

When the supply voltage is switched on, the switch sends requests (BootP requests) to assign IP parameters.

The "BootP" function can be deactivated via the management. By default upon delivery, the "BootP" function is activated.

The assignment of valid IP parameters is vital to the management function of the switch.

Options for assigning IP parameters:

- Configuration via the BootP protocol (default upon delivery)
- Static configuration via the management interfaces

The assignment of IP parameters with Factory Manager 2.1 is described on page 3-1.

2.1.2.1 Valid IP parameters

IP parameters comprise the following three elements: "IP address", "subnet mask", and "default gateway/router".

Valid IP addresses are:
000.000.000.001 to 126.255.255.255
128.000.000.000 to 223.255.255.255

Valid multicast addresses are:
224.000.000.001 to 239.255.255.255

Valid subnet masks are:
255.000.000.000 to 255.255.255.252

Default gateway/router:
The IP address of the gateway/router must be in the same subnetwork as the IP address of the switch.

2.1.2.2 Assigning IP addresses

The IP address is a 32-bit address, which consists of a network part and a user part. The network part consists of the network class and the network address.
There are currently five defined network classes; Classes A, B, and C are used in modern applications, while Classes D and E are hardly ever used. It is therefore usually sufficient if a network device only "recognizes" Classes A, B, and C.

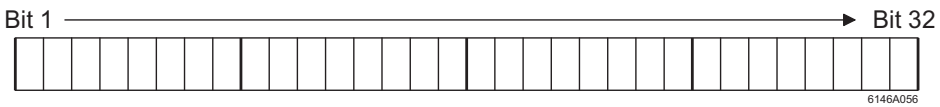


Figure 2-1 Location of the bits within the IP address

With binary representation of the IP address the network class is represented by the first bits. The key factor is the number of “ones” before the first “zero.” The assignment of classes is shown in the table below. The empty cells in the table are not relevant to the network class and are already used for the network address.

	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5
Class A	0				
Class B	1	0			
Class C	1	1	0		
Class D	1	1	1	0	
Class E	1	1	1	1	0

The bits for the network class are followed by those for the network address and the user address. Depending on the network class, a different number of bits are available, both for the network address (network ID) and the user address (host ID).

	Network ID	Host ID
Class A	7 bits	24 bits
Class B	14 bits	16 bits
Class C	21 bits	8 bits
Class D	28-bit multicast identifier	
Class E	27 bits (reserved)	

IP addresses can be represented in decimal or hexadecimal form. In decimal notation, bytes are separated by dots (dotted decimal notation) to show the logical grouping of the individual bytes.

The decimal points do not divide the address into a network and user address. Only the value of the first bits (before the first “zero”) specifies the network class and the number of remaining bits in the address.

Possible address combinations

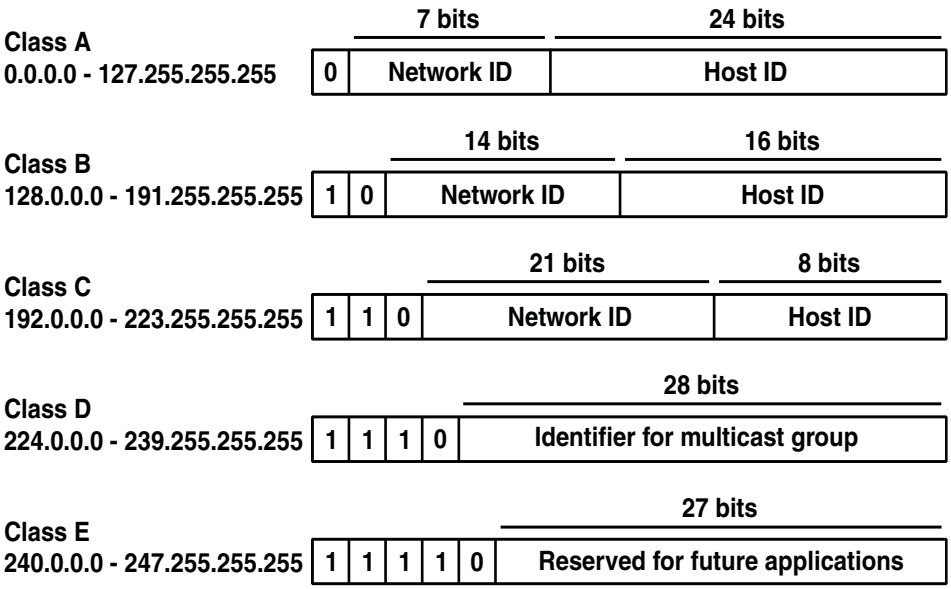


Figure 2-2 Structure of IP addresses

2.1.2.3 Special IP addresses for special applications

Certain IP addresses are reserved for special functions. The following addresses should not be used as standard IP addresses.

127.x.x.x addresses

The Class A network address "127" is reserved for a loopback function on all computers, regardless of the network class. This loopback function may only be used on networked computers for internal test purposes.

If a telegram is addressed to a computer with the value 127 in the first byte, the receiver immediately sends the telegram back to the transmitter.

The correct installation and configuration of the TCP/IP software, for example, can be checked in this way.

As Layers 1 and 2 of the ISO/OSI reference model are not included in the test they should be tested separately using the ping function.

Value 255 in the byte

Value 255 is defined as a broadcast address. The telegram is sent to all the computers that are in the same part of the network. Examples: 004.255.255.255, 198.2.7.255 or 255.255.255.255 (all the computers in all the networks). If the network is divided into subnetworks, the subnet masks must be observed during calculation, otherwise some devices may be omitted. In other words, the last address of an area is reserved as the broadcast address.

0.x.x.x addresses

Value 0 is the ID of the specific network. If the IP address starts with a zero, the receiver is in the same network. Example: 0.2.1.1, refers to device 2.1.1 in this network.

The zero previously signified the broadcast address. If older devices are used, unauthorized broadcast and complete overload of the entire network (broadcast storm) may occur when using IP address 0.x.x.x.

2.1.2.4 Subnet masks

Routers and gateways divide large networks into several subnetworks. The subnet mask is used to assign the IP addresses of individual devices to specific subnetworks. The **network part** of an IP address is **not** modified by the subnet mask. An extended IP address is generated from the user address and subnet mask. Because the masked subnetwork is only recognized by the local computers, this extended IP address appears as a standard IP address to all the other devices.

Structure of the subnet mask

The subnet mask always contains the same number of bits as an IP address. The subnet mask has the same number of bits (in the same position) set to "one", which is reflected in the IP address for the network class.

Example: A Class A IP address contains a 1-byte network address and a 3-byte computer address. Therefore, the first byte of the subnet mask may only contain "ones".

The remaining bits (three bytes) then contain the address of the subnetwork and the computer. The extended IP address is created when the bits of the IP address and the bits of the subnet mask are ANDed. Because the subnetwork is only recognized by local devices, the corresponding IP address appears as a "normal" IP address to all the other devices.

Application

If the ANDing of the address bits gives the local network address and the local subnetwork address, the device is located in the local network. If the ANDing gives a different result, the data telegram is sent to the subnetwork router.

Example for a Class B subnet mask:

Decimal representation: 255.255.192.0

Binary representation: 1111 1111.1111 1111.1100 0000.0000 0000

Using this subnet mask, the TCP/IP protocol software differentiates between the devices that are connected to the local subnetwork and the devices that are located in other subnetworks.

Example: Device 1 wants to establish a connection with device 2 using the above subnet mask. Device 2 has IP address 59.EA.55.32.

Representation of the IP address for device 2:

Hexadecimal representation: 59.EA.55.32

Decimal representation: 0101 1001.1110 1010.0101 0101.0011 0010
61462011

The individual subnet mask and the IP address for device 2 are then ANDed bit-by-bit by the software to determine whether device 2 is located in the local subnetwork.

ANDing the subnet mask and IP address for device 2:

Subnet mask:		1111 1111.1111 1111.1100 0000.0000 0000
	AND	
IP address:		0101 1001.1110 1010.0101 0101.0011 0010
Result:		0101 1001.1110 1010.0100 0000.0000 0000

61462012

Subnetwork

After ANDing, the software determines that the relevant subnetwork (01) does not correspond to the local subnetwork (11) and forwards the data telegram to a subnetwork router.

2.1.3 Flowchart after a restart

2.1.3.1 Loading the configuration data

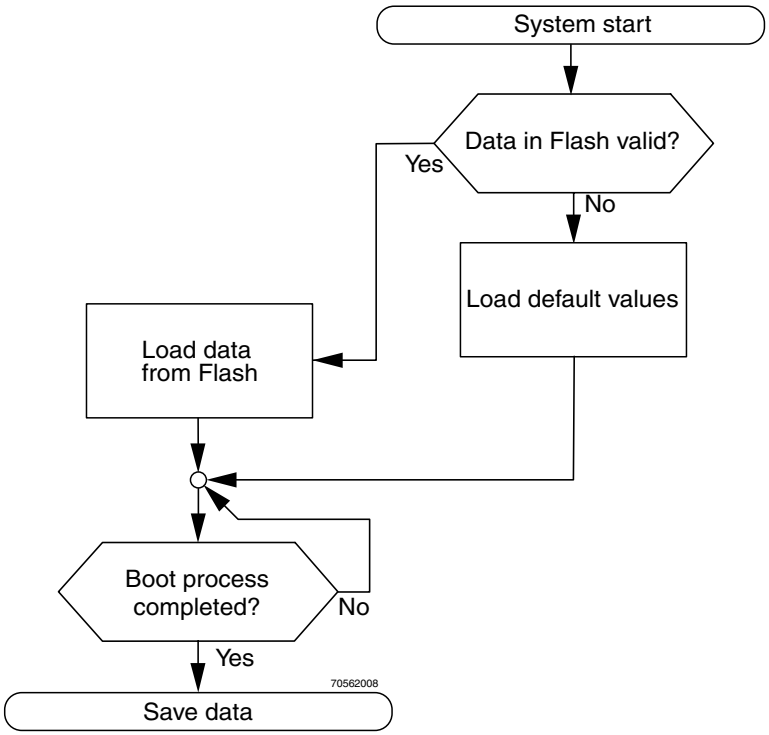


Figure 2-3 Flowchart: Loading the configuration data

2.1.3.2 Assigning IP parameters

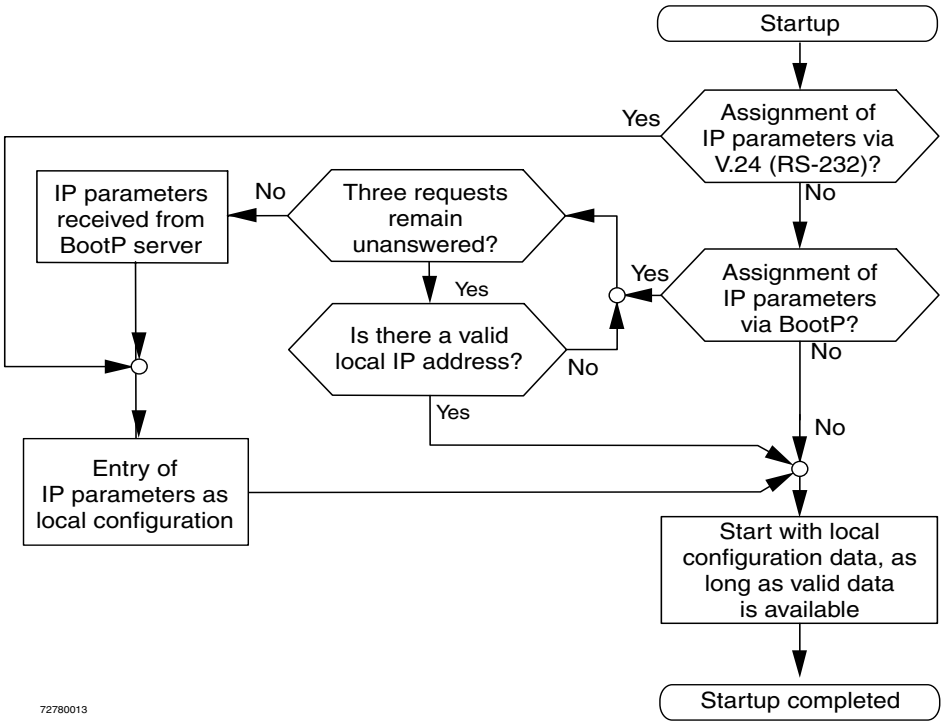


Figure 2-4 Flowchart: Assigning IP parameters

2.2 Frame switching

The Managed 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 1023 MAC addresses with an aging time of 48 seconds in its address table.

2.2.1 Store-and-forward

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

2.2.2 Multi-address function

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

– unknown source addresses
– a source address for this port
– a multicast/broadcast address

in the destination address field are forwarded via the relevant port. The switch can learn up to 1023 addresses. This is important when more than one termination device is connected to one or more ports. In this way, several independent subnetworks can be connected to one switch.

2.2.3 Learning addresses

The LMS independently learns the addresses for termination devices, which are connected via a port, by evaluating the source addresses in the data telegram. When the LMS 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 LMS can learn up to 1023 addresses and store them in its table. The switch monitors the age of the learned addresses. The switch automatically deletes address entries from its address table that have exceeded a specific age (48 seconds, aging time).

All learned entries are deleted on a restart.

Flowchart for "learning addresses" using the example of unicast addresses

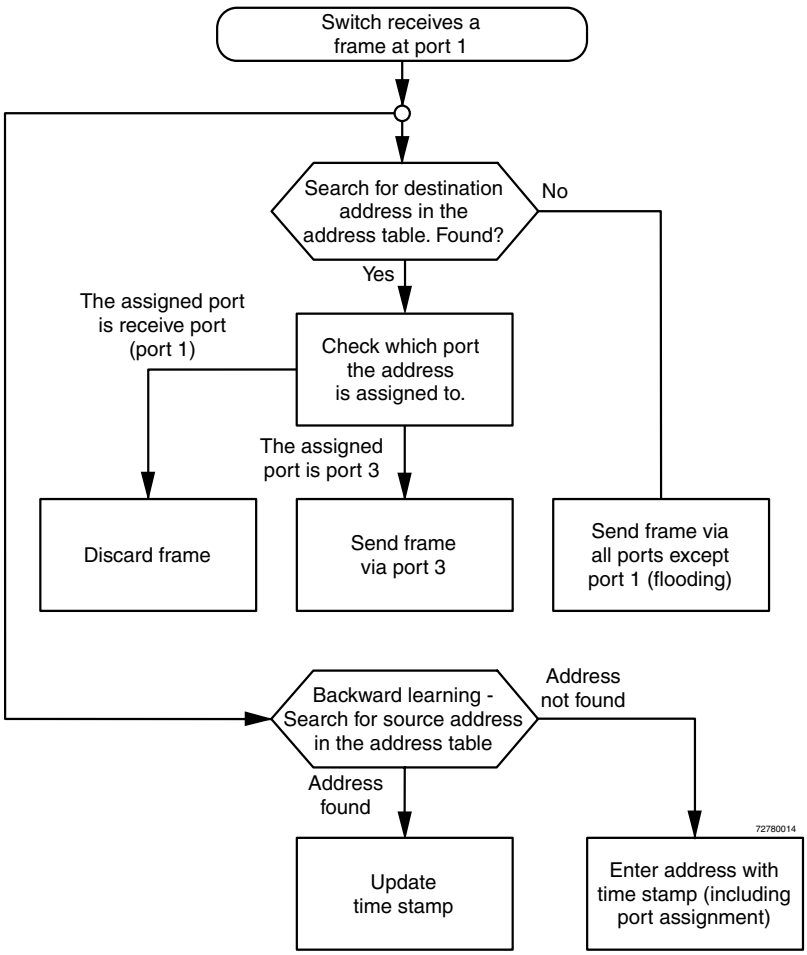


Figure 2-5 Flowchart for "learning addresses"

2.2.4 Prioritization (Quality of Service)

The switch supports two 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:

– Data packets with values between "0" and "3" in the priority field are low (default) priority
– Data packets with values between "4" and "7" in the priority field are transmitted with high priority by the switch

2.2.4.1 VLAN/prioritization tag

The LMS processes incoming data packets in accordance with the prioritization information contained in the Ethernet packet (VLAN/prioritization tag).
The tag enables the specification of a priority level from 0 to 7, which the LMS assigns to one of its two internal queues. By default upon delivery, the packets with priorities from 0 to 3 are treated as low-priority packets whereas packets with priorities from 4 to 7 are high-priority Ethernet packets.

Processing rules

The switch controller in the LMS forwards received packets to one of the receive queues according to the following decisions:

- BPDU packets are always assigned to the high-priority queue.
- Packets with unknown unicast addresses are always assigned to the low-priority queue.
- Packets are assigned to the high-priority queue if the priority from the VLAN/prioritization tag is mapped to the "high" level (default priority 4 to 7).
- The internal port priority "high" results in priority level 7 handling, i.e., the basic settings for data packet assignment to the high-priority queue are made.
- All residual data is assigned to the low-priority queue.

2.2.4.2 Strict priority

The switch supports two priority queues for adjusting the packet processing sequence (traffic classes according to IEEE 802.1D). The switches therefore support the QoS functions required by PROFINET RT and meet conformance class A. Data telegrams that are received are assigned to these classes according to their priority, which is specified in the VLAN/prioritization tag:

- Data packets with values between "0" and "3" in the priority field are low priority (default).
- Data packets with values between "4" and "7" in the priority field are transmitted with high priority by the switch.

The LMS uses "strict priority" for transmitting data telegrams. First, **all** high-priority data packets are transmitted. Once these are forwarded, low-priority telegrams are transmitted.

This function prevents delays in high-priority data transmission due to large volumes of low-priority data traffic. Low-priority traffic is rejected when the memory or data channel is overloaded.

3 Configuration and diagnostics

Lean Managed Switches offer several user interfaces for accessing configuration and diagnostic data. The preferred interfaces are the web interface and SNMP interface. These two interfaces can be used to make all the necessary settings and request all information. Access via Telnet/RS-232 interface only enables access to basic information. However, the RS-232 interface also enables firmware update via XMODEM in the event of faulty firmware.

Settings are not automatically saved permanently. The active configuration can be saved permanently by selecting "Save current configuration" on the "Configuration Management" web page, the "SAVE" button in the terminal interface or the "flWorkFWCtrlConfSave" SNMP object.

3.1 Factory Manager

3.1.1 General function

The integration of the LMS in the Factory Manager provides support for configuration and management.

3.1.2 Assigning IP parameters

Only **one** of several options for assigning IP parameters using Factory Manager is described here.

The "**IPAssign.exe**" addressing tool, which is available free of charge, can be used to assign the IP parameters. This program does not have to be installed, as it is an executable exe file. It can be downloaded at www.phoenixcontact.net/download.

Once you have established all the necessary connections and Factory Manager has been started, restart the LMS.

Following the boot phase, the LMS sends the BootP requests, which are received by Factory Manager and displayed in the message window. If you are operating other devices in the same network, messages from these devices may also be displayed. Messages from Phoenix Contact Factoryline components can be easily identified by their MAC address, which starts with 00.A0.45... and is provided on the devices.

Please check the MAC address in the messages to ensure the correct device is addressed.

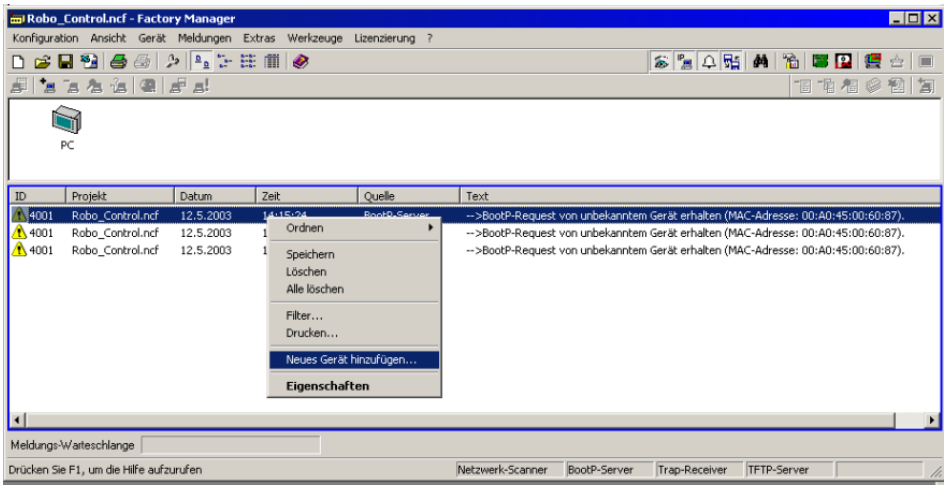


Figure 3-1 Messages from the LMS in Factory Manager

Right-click on one of the LMS messages and select the "Add new device..." menu item. Under "Description" select an icon and enter a device name.

Specify the desired IP parameters under "TCP/IP" (see also Section "Assigning IP parameters" on page 3-1).

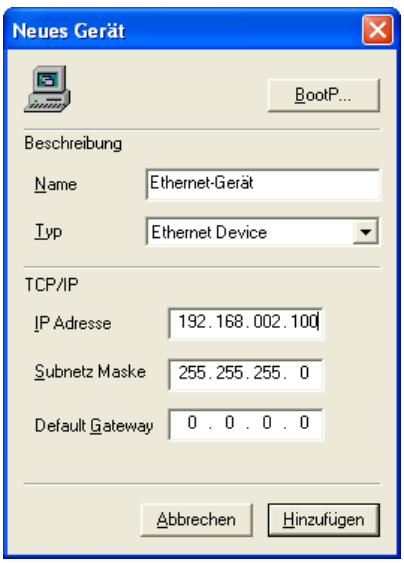


Figure 3-2 Input mask for IP parameters

Make sure that the assignment of IP parameters via BootP is also activated.

Once you have clicked on "Add", the device is added to the project and is indicated as **unavailable**. You must now restart or reset the LMS. After a restart, the LMS resends the BootP requests and receives the corresponding BootP reply from Factory Manager. Once the boot process has been completed the LMS is indicated as available.

If the LMS is still indicated as "unavailable", check your network card settings. Please note that both devices must be located in the same network/subnetwork. If Factory Manager receives the BootP requests this does not mean that the devices are located in the same subnetwork, as the BootP requests are sent as a broadcast across subnetwork boundaries.

3.1.3 Configuration and diagnostics

Numerous options for configuring and diagnosing the LMS can be found in the "Device" menu under "Properties".

General

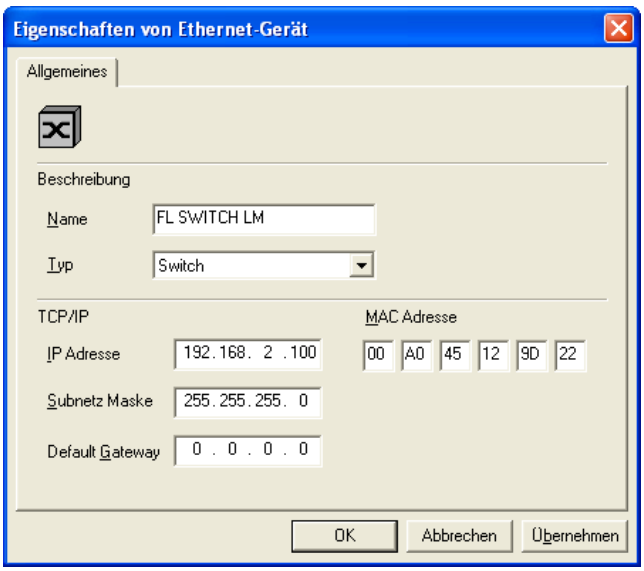


Figure 3-3 "General" menu

Here you can check or modify device names and types as well as IP parameters.

If you modify the IP address and/or the other IP parameters using Factory Manager, once you click "OK" you will no longer have access via Factory Manager. Restarting the LMS activates the modified parameters and restores access.

To activate the new addresses following a restart, BootP must be activated in the LMS.

3.2 Web-based management (WBM)

3.2.1 General function

Online diagnostics

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

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

For security reasons, we recommend you enter a new, unique password.

3.2.2 Requirements for the use of WBM

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

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

Settings are not automatically saved permanently. The active configuration can be saved permanently by selecting "Save current configuration" on the "Configuration Management" web page.

3.2.2.1 Structure of the web pages

The web pages are divided into four areas:

– Device type and device logo.
– Device name (assigned by the user) and loading time, to prevent mix-ups.
– Navigation tree on the left-hand side.
– Information tables, which contain current device information during runtime.

3.2.2.2 Password concept

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

The period of time can be set using the "flWorkFWCtrlLoginExpire" SNMP object within a range of 30 s to 3600 s (default 300 s).

The concept is valid for the first ten users. All further users must confirm each modification of the configuration with the password.

3.2.3 Functions/information in WBM

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

- **General Instructions**
  Basic information about WBM.
- **Device Information**
  General device information.
- **General Configuration**
  General device configuration.
- **Switch Station**
  Device-specific configuration and diagnostics.

3.2.3.1 General Instructions

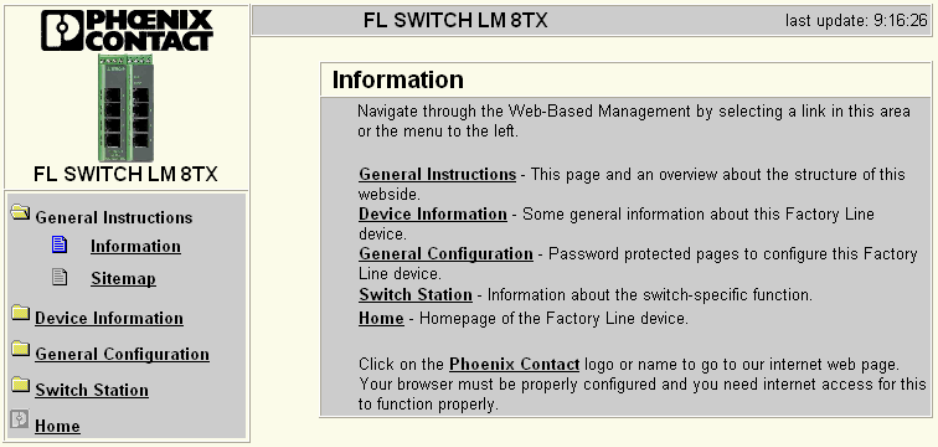


Figure 3-4 "Information" web page

Contains a brief description of WBM and a navigation tree (site map), which is linked to every page of WBM.

3.2.3.2 Device Information

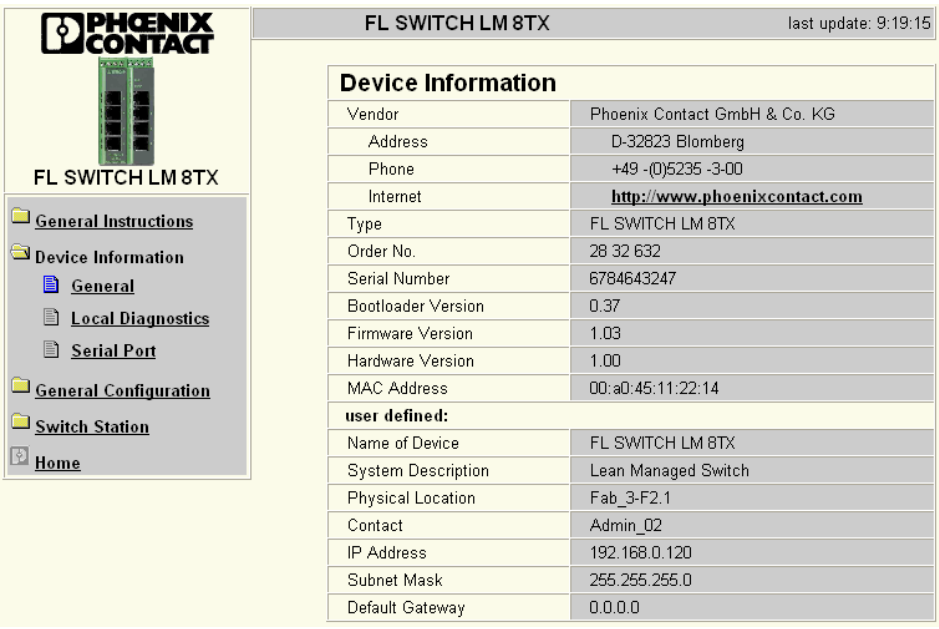


Figure 3-5 "Device Information" web page

"General" menu
This page contains a range of static information about the device and the manufacturer.

"Local Diagnostics" menu

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

Local Diagnostics	
Power Supply	
US1	Supply Voltage 1 (green LED)
US2	Supply Voltage 2 (green LED)
Green LED	
On	Link Up
Off	Link Down
Blink	Send or Receive Activity
Yellow LED	
On	Full Duplex Mode
Off	Half Duplex Mode
Blink	Collision Detection

Figure 3-6 "Local Diagnostics" web page

"Serial Port" menu

This page lists the transmission parameters for serial communication.

Serial Port	
Baud Rate	38400
Character Size	8
Parity	None
Stop Bits	1
Flow Control	None

Figure 3-7 "Serial Port" menu

3.2.3.3 General Configuration

"IP Configuration" menu

This page displays the set IP parameters and addressing mechanism. To change the IP parameters via WBM, "Static" assignment must be selected.

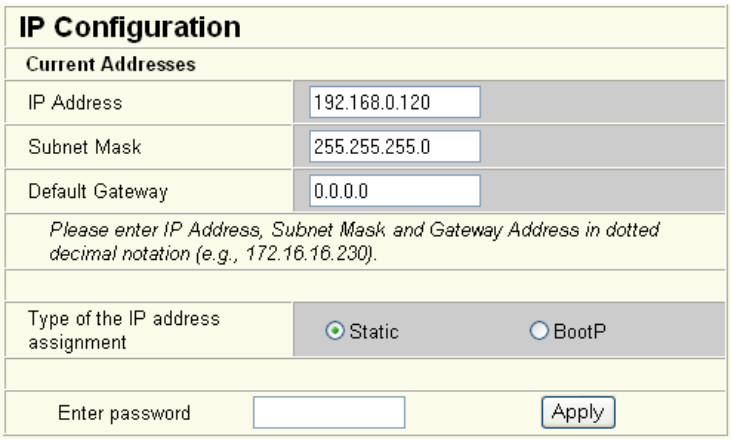


Figure 3-8 "IP Configuration" web page

If you modify the IP address and/or the other IP parameters via WBM, once you click "Apply" you will no longer have access via the IP address set in the browser.

"SNMP Configuration" menu

System Information

This part of the table is used to display or modify user-specific device data, e.g., location, device name or function.

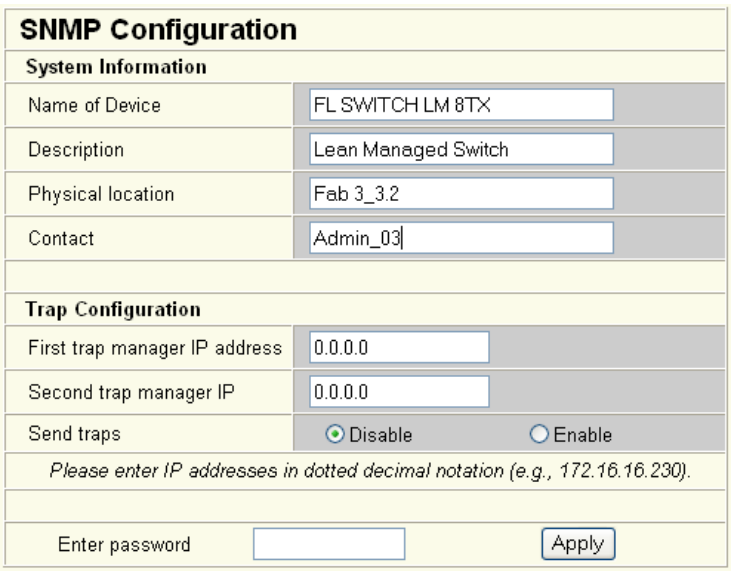


Figure 3-9 "SNMP Configuration" web page

Trap Configuration

This part of the table is used to view or modify the IP addresses of the two trap receivers. It is also used to activate/deactivate the "send traps" function.

"Software Update" menu

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

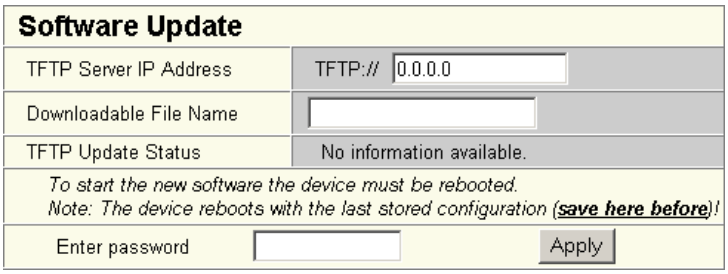


Figure 3-10 "Software Update" web page

3.2.4 Carrying out the firmware/software update

Requirements

The device **must** have **valid** IP parameters so that the firmware can be updated. A functional Factory Manager or another TFTP server are also required.

A suitable version of Factory Manager can be downloaded at www.phoenixcontact.net/download.

Proceed as follows to update the software:

- Save the desired firmware/software in the download directory of your TFTP server. If using Factory Manager, the path for standard installation is as follows: "C:\Program Files\Phoenix Contact\Factory Manager\Version 2.3\download".
- Start Factory Manager and check whether the TFTP server is activated.

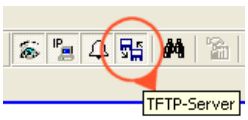


Figure 3-11 Factory Manager with activated TFTP server

- Start WBM for the switch and call the "Software Update" page (...General Configuration/Software Update).
- Enter the IP address of the computer on which Factory Manager is installed in the "TFTP Server IP Address" field.
- Then enter the complete file name of the firmware file in the "Downloadable File Name" field, but do not enter the path (i.e., no drive, no folder).

- Enter the device password (default: "private") and click on "Apply".

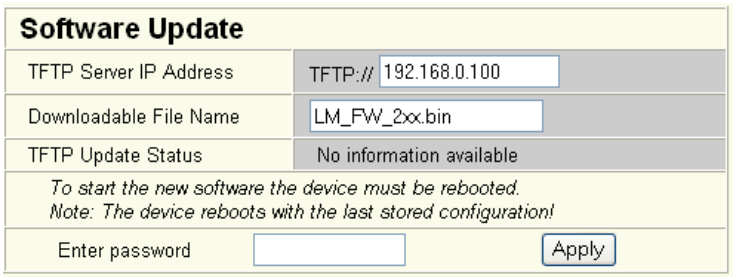


Figure 3-12 Web interface with the update parameters

The following window appears after a few moments.

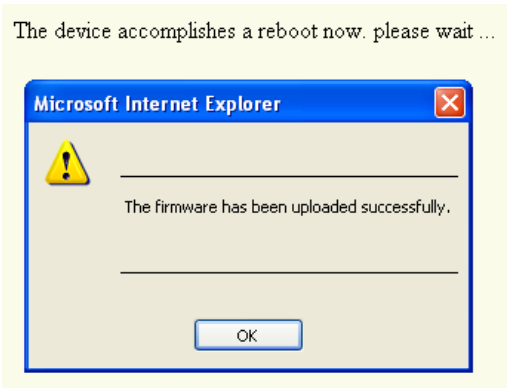


Figure 3-13 Message following successful update

- Close and restart WBM.

Firmware update can take several minutes. You can monitor the download progress in the Factory Manager message window (25%, 50%, 75%, 100%). Always wait approximately two minutes until all the LEDs have lit up and the device is available again after booting.

There are no assurances that all existing configuration data will be retained after a firmware update/downgrade. Therefore, please check the configuration settings or reset the device to the settings default upon delivery.

NOTE: A voltage failure during a firmware update results in the destruction of the firmware on the LMS. An update via XMODEM is required, see "Starting with faulty software" on page 3-56.

"Change Password" menu

This option can be used to specify the current password and then enter a new, unique password. 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.

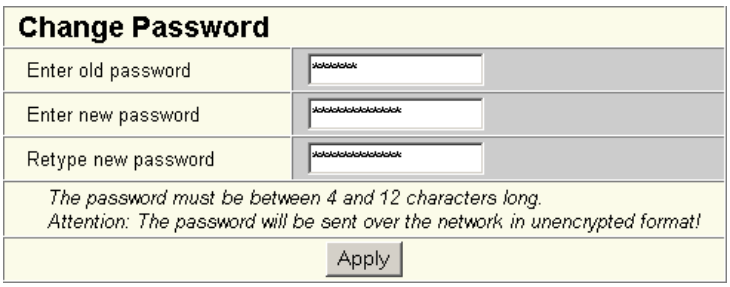


Figure 3-14 "Change Password" web page

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

Forgotten your password?
Call the Phoenix Contact phone number listed in the Appendix, making sure you have the device serial number and MAC address to hand.

"User Interfaces" menu

The following actions can be performed here:

– Activation/deactivation of the web server.
– Activation/deactivation of the SNMP agent.
– Activation/deactivation of the configuration pages for redundancy.

With the activation/deactivation of the configuration pages under "User Interfaces", only the web pages for configuring the selected functions are enabled/disabled in the WBM menu.

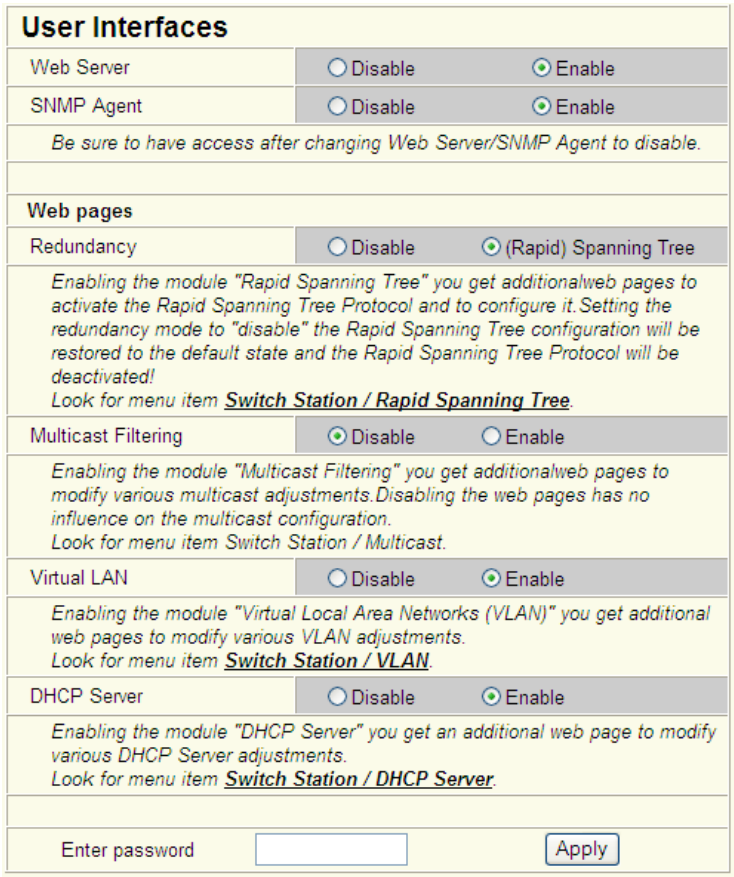


Figure 3-15 "User Interfaces" web page

"General Configuration\Config. Management" menu

This table is used to view all parameters that are required to save the active configuration or load a new configuration, and to modify them (by entering a valid password). It can also be used to restart the system with the relevant configuration.

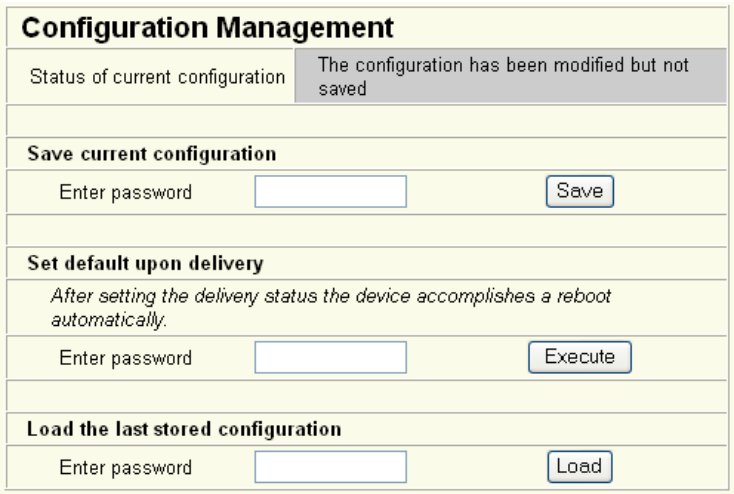


Figure 3-16 "Configuration Management" web page

Possible states for "Status of current configuration":

- The configuration has been modified but not saved.
- Saving the current configuration.
- The current configuration is equal to the saved one in the non volatile memory of the switch.
- The current configuration was saved.

If the new configuration is not activated by a reset after a configuration download, the "Save current configuration" command overwrites the previously loaded configuration and instead saves the active configuration of the LMS.

Set default upon delivery

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

Figure 3-17 "Set default upon delivery" web page

WBM can only be called using a valid IP address. Once the switch has been reset to its default settings, it has **no** valid IP address.

Load the last stored configuration

This option can be used to reload the last configuration stored on either the device or the PC. All modifications made to the configuration since it was last saved are lost.

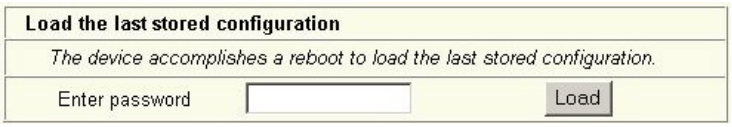


Figure 3-18 "Load the last stored configuration" web page

"File Transfer" menu

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

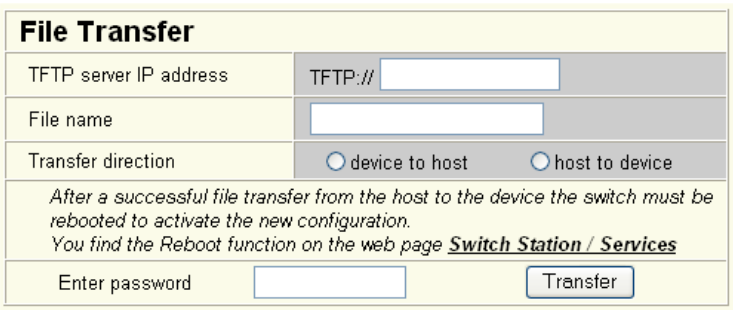


Figure 3-19 "File Transfer" web page

When a configuration is uploaded from the switch to a PC, the last saved version is transmitted. If you want to transmit the active configuration, first save it again ("Save current configuration" function).

When a configuration is downloaded from the PC to a switch, the new configuration is only activated once the switch has been reset.

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

Device replacement

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

– Create a point-to-point connection between a switch and the management station.
– Load the configuration file on the switch.
– Reset the switch.
– Adjust the IP parameters.
– Save the configuration ("Save current configuration" function).

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

3.2.4.1 Switch Station

Services

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

"DHCP Server" menu

On this page, activate/deactivate the DHCP server and configure the settings accordingly.

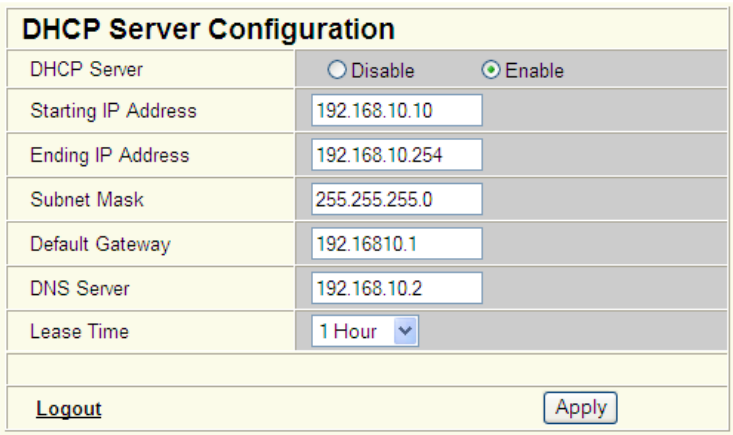


Figure 3-20 "DHCP Server" web page

As a DHCP server, the switch can use the Dynamic Host Configuration Protocol (DHCP) to assign the network configuration to the connected clients.

The IP address area of the DHCP server may include a maximum of 254 clients.

Starting/Ending IP Address

Specifies the area from which the DHCP server/switch assigns IP addresses.

Subnet Mask

Specifies the subnet mask for the network segment.

Default Gateway

Specifies the default gateway/router for switching to other network segments.

DNS Server

Specifies the address of the Domain Name Server.

Lease Time

The lease time is a period of time during which the client may use the assigned IP configuration.

The options are as follows:

– 1 hour
– 1 day
– 1 week
– 1 month

"Ports" menu

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

Port Table

Port	Type	Port Status	Link State
1	TX 10/100	enable	100 MBit FD
2	TX 10/100	enable	100 MBit FD
3	TX 10/100	enable	100 MBit FD
4	TX 10/100	enable	100 MBit FD

Figure 3-21 "Port Table" web page

"Port Cfg. Table" menu

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

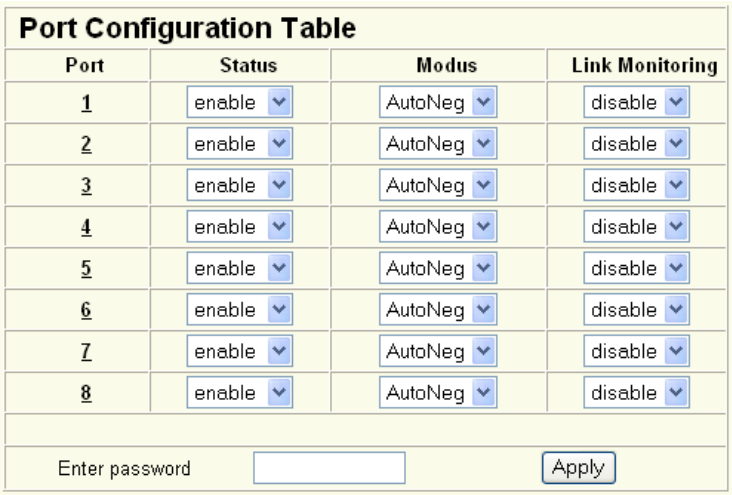


Figure 3-22 "Port Configuration Table" web page

Port Configuration

Individual configuration option for each port. To view detailed data traffic statistics for the selected port, click on "Port Statistics".

Even if the port is switched off, the Link LED for the port remains active.

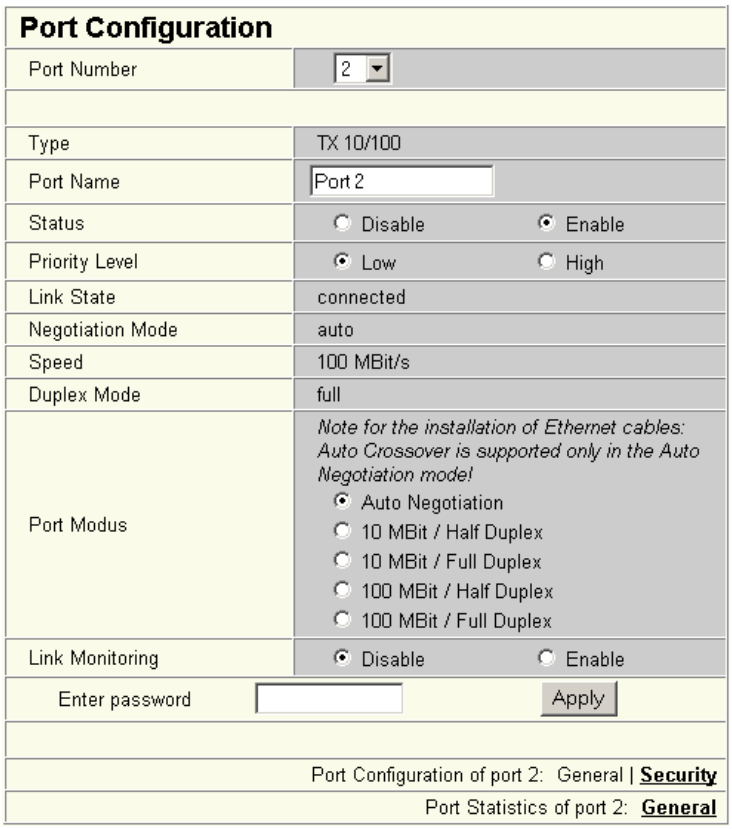
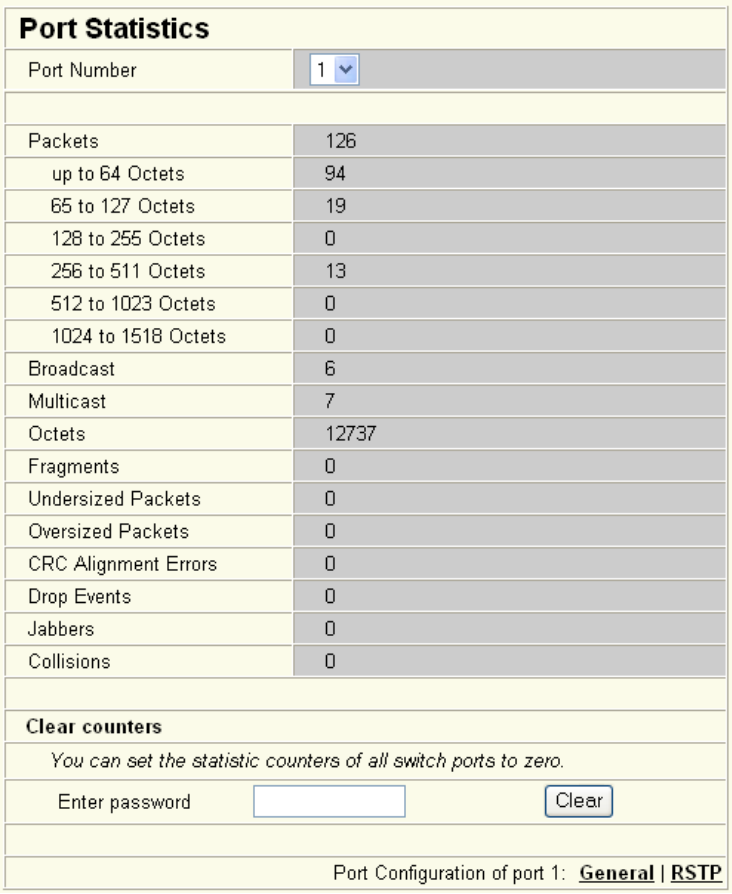


Figure 3-23 "Port Configuration" web page

"Port Statistics" menu

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



Port Statistics

Port Number	1
Packets	126
up to 64 Octets	94
65 to 127 Octets	19
128 to 255 Octets	0
256 to 511 Octets	13
512 to 1023 Octets	0
1024 to 1518 Octets	0
Broadcast	6
Multicast	7
Octets	12737
Fragments	0
Undersized Packets	0
Oversized Packets	0
CRC Alignment Errors	0
Drop Events	0
Jabbers	0
Collisions	0

Clear counters

You can set the statistic counters of all switch ports to zero.

Enter password [ ] Clear

Port Configuration of port 1: General | RSTP

Figure 3-24 "Port Statistics" web page

"Port Mirroring" menu

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

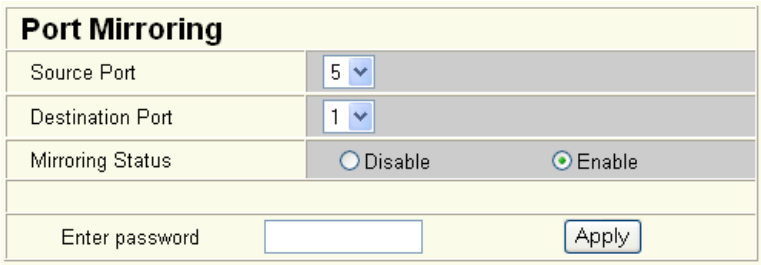


Figure 3-25 "Port Mirroring" web page

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

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

"Diagnostics/Display" menu

The "Display" menu contains some status information about the switch.

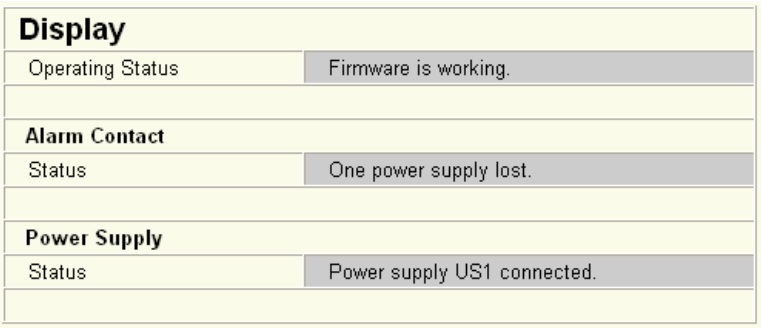


Figure 3-26 "Display" menu

"Diagnostics\Alarm Contact" menu

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

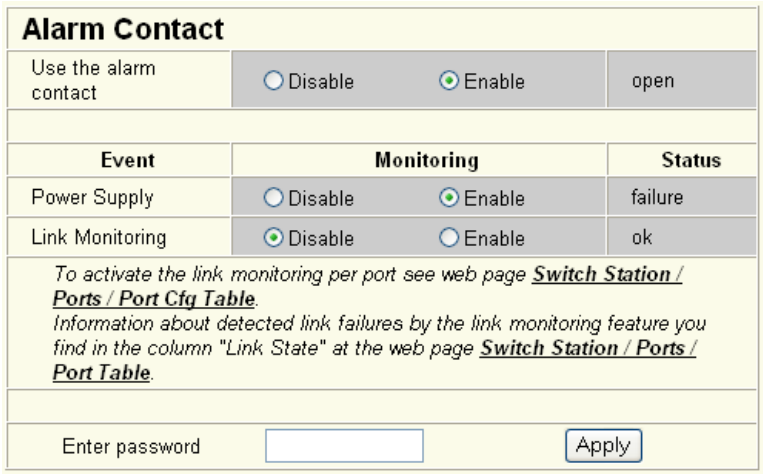


Figure 3-27 "Alarm Contact" web page

Click on the "Switch Station / Ports / Port Table" link (on the "Alarm Contact" page in WBM) to access the port configuration page. Here, the ports to be monitored must be explicitly enabled for link monitoring.

"Utilization" menu

Here, the network capacity of each individual port is displayed as a bar graph. The display is automatically updated according to the refresh interval.

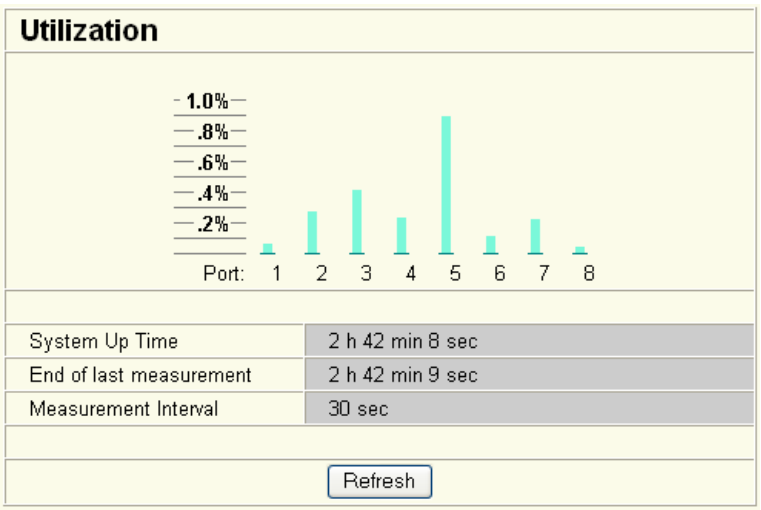


Figure 3-28 "Utilization" web page

Please note that the % scale is spread according to the capacity utilization.

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

3.2.4.2 Rapid Spanning Tree

For information about (Rapid) Spanning Tree, please refer to Section 4 "Rapid Spanning Tree".

3.3 Simple Network Management Protocol (SNMP)

3.3.1 General function

SNMP is a manufacturer-independent standard for Ethernet management and defines commands for reading and writing error and status message information and formats. SNMP is also a structured model, which comprises agents and their relevant MIB (Management Information Base) and a manager. The manager is a software tool, which is executed on a network management station.

The agents are located inside switches, bus terminal modules, routers, and other devices that support SNMP. The task of the agents is to collect and provide data in the MIB. The manager regularly requests and displays this information. The devices can be configured by writing data from the manager to the MIB. In the event of an emergency, the agents can also send messages (traps) directly to the manager.

All configuration modifications, which are to take effect after an LMS restart, must be saved permanently using the "flWorkFWCtrlConfSave" object.

SNMP interface

All managed Factoryline components have an SNMP agent. This agent manages Management Information Base II (MIB 2) according to RFC1213 MIB, Bridge MIB, IANAifType MIB, RSTP MIB, RFC1907 MIB, and private SNMP objects from Phoenix Contact.

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 (SNMP). In addition, any SNMP tools or network management tools can be used to access Factoryline products via SNMP. 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 private SNMP objects, which are then assigned to a private manufacturer area in the large SNMP object tree. Manufacturers are then responsible for their own private (enterprise) areas, i.e., they must ensure that only one object is assigned to an object ID (object name and parameters) and can be published. If an object is no longer needed, it can be labeled as "expired", but it cannot be reused with other parameters under any circumstances.

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

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

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

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

Management Information Base (MIB)

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

Agent

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

Traps

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

trapColdStart

OID	1.3.6.1.6.3.1.1.5.1
Description	Sent when the switch is started

trapPortUp/Down

OID	1.3.6.1.6.3.1.5.3/4
Description	Sent when a port is enabled or disabled.

3.3.2 Schematic view of SNMP management

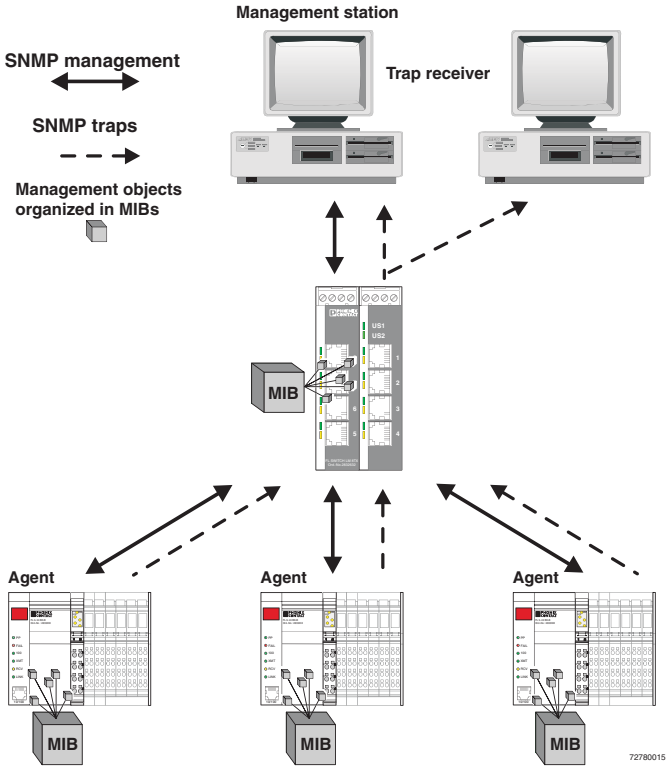


Figure 3-29 Schematic view of SNMP

3.3.2.1 Tree structure of the MIB

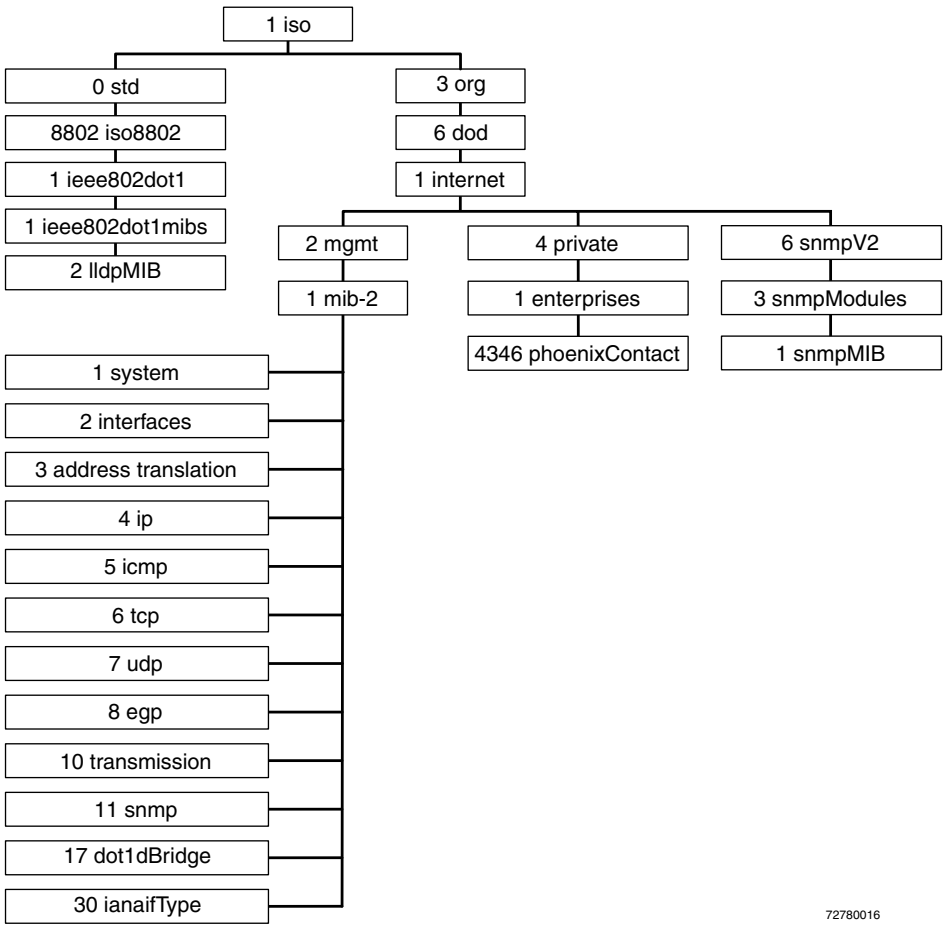


Figure 3-30 Tree structure of the MIB

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.

3.3.3 RFC1213 MIB - MIB II

3.3.3.1 System group (1.3.6.1.2.1.1)

The system group has mandatory characters for all systems. It contains system-specific objects. If an agent does not have a value for a variable, the response is a string with length 0.

(1) system

- (1) sysDescr
- (2) sysObjectID
- (3) sysUpTime
- (4) sysContact
- (5) sysName
- (6) sysLocation
- (7) syswitch sta
-
- (8) sysORLastChange

sysDescr

OID	1.3.6.1.2.1.1.1.0
Syntax	Octet string (size: 0 - 255)
Access	Read
Description	A textual description of the entry. The value should contain the full name and version number of: - Type of system hardware - Operation system software - Network software The description may only consist of ASCII characters that can be printed.

sysObjectID

OID	1.3.6.1.2.1.1.2.0
Syntax	Object identifier
Access	Read
Description	The authorization identification for the manufacturer of the network management subsystem, which is integrated in this device. This value is located in the SMI enterprises subtree (1.3.6.1.4.1) and describes which type of device is being managed. For example, if the manufacturer "Phoenix Contact GmbH" is assigned subtree 1.3.6.1.4.1.4346, it can then assign its bridge the identifier 1.3.6.1.4.1.4346.2.1.

sysUpTime

OID	1.3.6.1.2.1.1.3.0
Syntax	TimeTicks
Access	Read
Description	The time in hundredths of seconds since the last network management unit reset.

sysContact

OID	1.3.6.1.2.1.1.4.0
Syntax	Octet string (size: 0 - 255)
Access	Read and write
Description	The textual identification of the contact person for these managed nodes and information on how this person can be contacted.

sysName

OID	1.3.6.1.2.1.1.5.0
Syntax	Octet string (size: 0 - 255)
Access	Read and write
Description	A name for this node assigned by the administrator. According to the agreement, this is the fully qualifying name in the domain.

sysLocation

OID	1.3.6.1.2.1.1.6.0
Syntax	Octet string (size: 0 - 255)
Access	Read and write
Description	The physical location of this node (e.g., "Hall 1, 3rd floor").

sysServices

OID	1.3.6.1.2.1.1.7.0
Syntax	Integer (0 - 127)
Access	Read
Description	This value indicates a number of services that this device offers. It is the sum of several calculations. For every layer of the OSI reference model, there is a calculation in the form of (2^{L-1}), where L indicates the layer. For example: A node which primarily executes line routing functions has the value $(2^{3-1}) = 4$. A node which is a host and provides application services has the value $(2^{4-1}) + (2^{7-1}) = 72$.

sysORLastChange

OID	1.3.6.1.2.1.1.8
Syntax	TimeTicks
Access	Read
Description	Indicates the value of the sysUpTime during the last system modification.

3.3.3.2 Interface group (1.3.6.1.2.1.2)

The interface group contains information about device interfaces.

(2) interfaces
-- (1) ifNumber
-- (2) ifTable
-- (1) if Entry
-- (1) ifIndex
-- (2) ifDescr
-- (3) ifType
-- (4) ifMtu
-- (5) ifSpeed
-- (6) ifPhysAddress
-- (7) ifAdminStatus
-- (8) ifOperStatus
-- (9) ifLastChange
-- (10) ifInOctets
-- (11) ifInUcastPkts
-- (12) ifInNUcastPkts
-- (13) ifInDiscards
-- (14) ifInErrors
-- (15) ifInUnknownProtos
-- (16) ifOutOctets
-- (17) ifOutUcastPkts
-- (18) ifOutNUcastPkts
-- (19) ifOutDiscards
-- (20) ifOutErrors
-- (21) ifOutQLen
-- (22) ifSpecific

3.3.4 Bridge MIB (1.3.6.1.2.1.17)

3.3.4.1 dot1dBase (1.3.6.1.2.1.17.1)

The dot1dBase group contains bridge-specific information.

(1) dot1dBaseBridgeAddress
(2) dot1dBaseNumPorts
(3) dot1dBasePortType
(4) dot1dBasePortTable
-- dot1dBasePortEntry
-- (1) dot1dBasePort
-- (2) dot1dBasePortIfIndex
-- (3) dot1dBasePortPortCircuit
-- (4) dot1dBasePortDelayExceededDiscards
-- (5) dot1dBasePortMtuExceededDiscards

3.3.4.2 dot1dStp (1.3.6.1.2.1.17.2)

-- (1) dot1dStpProtocolSpecification
-- (2) dot1dStpPriority
-- (3) dot1dStpTimeSinceTopologyChange
-- (4) dot1dStpTopChanges
-- (5) dot1dStpDesignateRoot
-- (6) dot1dStpRootCost
-- (7) dot1dStpRootPort
-- (8) dot1dStpMaxAge
-- (9) dot1dStpHelloTime
-- (10) dot1dStpHoldTime
-- (11) dot1dStpForwardDelay
-- (12) dot1dStpBridgeMaxAge
-- (13) dot1dStpBridgeHelloTime
-- (14) dot1dStpBridgeForwardDelay
-- (15) dot1dStpPortTable
    -- (1) dot1dStpPortEntry
        -- (1) dot1dStpPort
        -- (2) dot1dStpPortPriority
        -- (3) dot1dStpPortState
        -- (4) dot1dStpPortEnable
        -- (5) dot1dStpPortPathCost
        -- (6) dot1dStpPortDesignatedRoot
        -- (7) dot1dStpPortDesignatedCost
        -- (8) dot1dStpPortDesignatedBridge
        -- (9) dot1dStpPortDesignatedPort
        -- (10) dot1dStpPortForwardTransitions
        -- (11) dot1sStpPortProtocolMigration
        -- (12) dot1dStpPortAdminEdgePort
        -- (13) dot1dStpPortOperEdgePort
        -- (14) dot1dStpPortAdminPointToPoint
        -- (15) dot1dStpPortOperPointToPoint
        -- (16) dot1dStpPortAdminPathCost

3.3.4.3 dot1dTp (1.3.6.1.2.1.17.4)

The dot1dTp group contains bridge-specific information.

(1) dot1dTpLearnedEntryDiscards
(2) dot1dTpAgingTime
(3) dot1dTpFdbTable
    -- (1) dot1dTpFdbEntry
        -- (1) dot1dTpFdbAddress
        -- (2) dot1dTpFdbPort
        -- (3) dot1dTpFdbStatus
(4) dot1dTpPortTable
    -- dot1dTpPortEntry

```
-- (1) dot1dTpPort
-- (2) dot1dTpPortMaxInfo
-- (3) dot1dTpPortInFrames
-- (4) dot1dTpPortOutFrames
-- (5) dot1dTpPortInDiscards
```

3.3.5 Private MIBs

The private MIBs for the LMS from Phoenix Contact can be found under object ID 1.3.6.1.4.1.4346. The LMS MIB contains the following groups:

– pxcModules (OID = 1.3.6.1.4.1.4346.1)
– pxcGlobal (OID = 1.3.6.1.4.1.4346.2)
– pxcFactoryLine (OID = 1.3.6.1.4.1.4346.11)

All configuration modifications, which are to take effect after an LMS restart, must be saved permanently using the "flWorkFWCtrlConfSave" object.

MIB tree

The private MIB from Phoenix Contact is integrated in the MIB tree as follows (see red arrow).

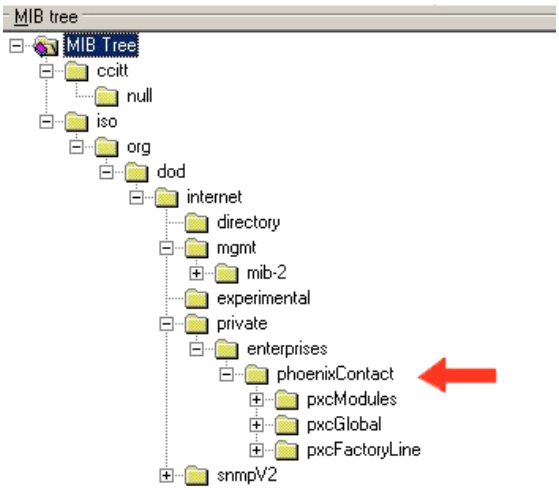


Figure 3-31 MIB tree

3.3.5.1 pxcModules OID = 1.3.6.1.4.1.4346.1

flMSwitchMModule

OID 1.3.6.1.4.1.4346.1.8

The object contains information about the manufacturer (address, phone number, etc.).

3.3.5.2 pxcGlobal OID = 1.3.6.1.4.1.4346.2

pxcBasic

OID 1.3.6.1.4.1.4346.2.1

	pxcBasicName
OID	1.3.6.1.4.1.4346.2.1.1
Syntax	Display string
Access	Read
Description	Contains the manufacturer's name: Phoenix Contact GmbH & Co. KG.
	pxcBasicDescr
OID	1.3.6.1.4.1.4346.2.1.2
Syntax	Display string
Access	Read
Description	Contains the manufacturer's name and address: Phoenix Contact GmbH & Co. KG, D-32823 Blomberg.
	pxcBasicURL
OID	1.3.6.1.4.1.4346.2.1.3
Syntax	Display string
Access	Read
Description	Contains the manufacturer's web address: http://www.phoenixcontact.com.

3.3.5.3 pxcFactoryLine OID = 1.3.6.1.4.1.4346.11

	flGlobal
OID	1.3.6.1.4.1.4346.11.1
	flBasic
OID	1.3.6.1.4.1.4346.11.1.1
	flBasicName
OID	1.3.6.1.4.1.4346.11.1.1.1
Syntax	Display string
Access	Read
Description	Contains the name of the product group: Factoryline.
	flBasicDescr
OID	1.3.6.1.4.1.4346.11.1.1.2

Syntax	Display string
Access	Read
Description	Contains a brief description of the product group: Ethernet Installation System.
	flBasicURL
OID	1.3.6.1.4.1.4346.11.1.1.3
Syntax	Display string
Access	Read
Description	Contains a specific URL for the product group: www.factoryline.de.
	flBasicCompCapacity
OID	1.3.6.1.4.1.4346.11.1.1.4
Syntax	Integer32 (1 ... 1024)
Access	Read
Description	Contains the number of different components that can be managed with this device.
	flComponents
OID	1.3.6.1.4.1.4346.11.1.2
	flComponentsTable
OID	1.3.6.1.4.1.4346.11.1.2.1
	flComponentsTableEntry

OID	1.3.6.1.4.1.4346.11.1.2.1.1
Syntax	
Access	
Description	Generates a table containing information about a Factoryline component.
flComponentsIndex	
OID	1.3.6.1.4.1.4346.11.1.2.1.1.1
Syntax	Integer32 (1 ... 1024)
Access	Read
Description	Identifies the components for which this entry contains information.
flComponentsName	
OID	1.3.6.1.4.1.4346.11.1.2.1.1.2
Syntax	Display string
Access	Read
Description	Indicates the device designation of the component.
flComponentsDescr	

OID	1.3.6.1.4.1.4346.11.1.2.1.1.3
Syntax	Display string
Access	Read
Description	Contains a brief description of the component.
flComponentsURL	
OID	1.3.6.1.4.1.4346.11.1.2.1.1.4
Syntax	Display string
Access	Read
Description	Contains the URL of a Phoenix Contact website with additional information.
flComponentsOrderNumber	
OID	1.3.6.1.4.1.4346.11.1.2.1.1.5
Syntax	Display string
Access	Read
Description	Contains the order number of the component.

flWorkDevice

OID 1.3.6.1.4.1.4346.11.11

flWorkBasic

OID 1.3.6.1.4.1.4346.11.11.1

flWorkBasicName

OID	1.3.6.1.4.1.4346.11.11.1.1
Syntax	Display string
Access	Read/write
Description	Contains the device name (corresponds to "sysName" from MIB2), which the user assigned to the device.

Check this entry following a firmware update, it may have been overwritten with default values.

flWorkBasicDescr

OID	1.3.6.1.4.1.4346.11.11.1.2
Syntax	Display string
Access	Read/write
Description	Contains a short description (corresponds to "sysDescr" from MIB2), which the user assigned to the device.

Check this entry following a firmware update, it may have been overwritten with default values.

flWorkBasicURL

OID	1.3.6.1.4.1.4346.11.11.1.3
Syntax	Display string
Access	Read
Description	Contains the URL of the device-specific web page for WBM in the form of the currently set IP address.

flWorkBasicSerialNumber

OID	1.3.6.1.4.1.4346.11.11.1.4
Syntax	Octet string (12)
Access	Read
Description	Contains the serial number of the device.

flWorkBasicHWRevision

OID	1.3.6.1.4.1.4346.11.11.1.5
Syntax	Octet string (4)
Access	Read
Description	Contains the hardware version of the device.

flWorkBasicPowerStat

OID	1.3.6.1.4.1.4346.11.11.1.6
Syntax	Integer32 (1 ... 1024)
Access	Read
Description	Contains status information about the connected supply voltages: - Unknown 1 - Supply voltage 1 OK 3 - Supply voltage 2 OK 4 - Supply voltage 1 and 2 OK 5

flWorkBasicCompMaxCapacity

OID	1.3.6.1.4.1.4346.11.11.1.11
Syntax	Integer 32
Access	Read
Description	Contains the maximum number of interfaces that can be connected in theory.

flWorkBasicCompCapacity

OID	1.3.6.1.4.1.4346.11.11.1.12
Syntax	Integer 32
Access	Read
Description	Contains the number of interfaces actually connected.

flWorkComponentsGroup

OID	1.3.6.1.4.1.4346.11.11.2

flWorkComponentsEntry

OID	1.3.6.1.4.1.4346.11.11.2.1.1
Syntax	
Access	
Description	Generates a table containing information about this component.
flComponentsIndex	
OID	1.3.6.1.4.1.4346.11.11.2.1.1.1
Syntax	Integer32 (1 ... 1024)
Access	Read
Description	Identifies the components for which this entry contains information.
flWorkComponentsOID	
OID	1.3.6.1.4.1.4346.11.11.2.1.1.2
Syntax	Object identifier
Access	Read
Description	Indicates the corresponding component in the "flComponents" group.
flWorkComponentsURL	
OID	1.3.6.1.4.1.4346.11.11.2.1.1.3
Syntax	Display string
Access	Read
Description	Contains the IP address that can be used to access the web server for this device.
flWorkComponentsDevSign	
OID	1.3.6.1.4.1.4346.11.11.2.1.1.4
Syntax	Integer (0 ... 255)
Access	Read
Description	Contains the interface designation assigned by the manufacturer.

flWorkNet

OID 1.3.6.1.4.1.4346.11.11.4

flWorkNetIfParameter

OID 1.3.6.1.4.1.4346.11.11.4.1

flWorkNetIfParamPhyAddress

OID	1.3.6.1.4.1.4346.11.11.4.1.1
Syntax	MAC address
Access	Read
Description	Contains the MAC address of the switch.

flWorkNetIfParamIPAddress

OID	1.3.6.1.4.1.4346.11.11.4.1.2
Syntax	IP address
Access	Read/write
Description	Contains the current IP address of the LMS. Changes only take effect once the "flWorkNetIfParamSave" object has been executed.

The "flWorkNetIfParamAssignment" object must be set to static (1), otherwise objects cannot be written.

flWorkNetIfParamSubnetmask

OID	1.3.6.1.4.1.4346.11.11.4.1.3
Syntax	IP address
Access	Read/write
Description	Contains the current subnet mask of the LMS. Changes only take effect once the "flWorkNetIfParamSave" object has been executed.

The "flWorkNetIfParamAssignment" object must be set to static (1), otherwise objects cannot be written.

flWorkNetIfParamGWIpAddress

OID	1.3.6.1.4.1.4346.11.11.4.1.4
Syntax	IP address
Access	Read/write
Description	Contains the IP address of the current default gateway/router of the LMS. Changes only take effect once the "flWorkNetIfParamSave" object has been executed.

The "flWorkNetIfParamAssignment" object must be set to static (1), otherwise objects cannot be written.

flWorkNetIfParamStatus

OID	1.3.6.1.4.1.4346.11.11.4.1.5
Syntax	Integer32 (1 ... 1024)
Access	Read
Description	Indicates whether the IP parameters have been modified but not saved:

- No change 1
- Address setting modified, but not yet activated 2

Address settings must be saved permanently using the "flWorkFWCtrlConfSave" object.

flWorkNetIfParamSave

OID	1.3.6.1.4.1.4346.11.11.4.1.6
Syntax	Integer
Access	Read/write
Description	Provides the option of saving modified IP parameters or undoing the modifications: - Undo modification 1 - Activate modification 2

Address settings must be saved permanently using the "flWorkFWCtrlConfSave" object.

flWorkNetIfParamAssignment

OID	1.3.6.1.4.1.4346.11.11.4.1.7
Syntax	Integer
Access	Read/write
Description	Provides the option of modifying the assignment mechanism for IP parameters. Takes effect after an LMS restart: - Static IP address 1 - Assignment via BootP (default) 2

Modifications to the assignment mechanism also affect the management functions via the web interface and via RS-232.

Address settings must be saved permanently using the "flWorkFWCtrlConfSave" object.

flWorkNetPort

OID 1.3.6.1.4.1.4346.11.11.4.2

flWorkNetPortCapacity

OID	1.3.6.1.4.1.4346.11.11.4.2.1
Syntax	Integer32 (1 ... 1024)
Access	Read
Description	Contains the number of available ports depending on the configuration of the LMS.

flWorkNetPortTable

OID 1.3.6.1.4.1.4346.11.11.4.2.2

flWorkNetPortEntry

OID	1.3.6.1.4.1.4346.11.11.4.2.2.1
Description	Generates a table with a detailed description of the port configuration.
flWorkNetPortIndex	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.1
Syntax	Integer32 (1 ... 1024)
Access	Read

Description	Specifies the port number of the selected port.
flWorkNetPortLinkState	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.2
Syntax	Integer
Access	Read
Description	Indicates the port status: Connected 1 Not connected 2
flWorkNetPortSpeed	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.3
Syntax	Gauge32
Access	Read
Description	Contains the data transmission speed of the selected port in bps.
flWorkNetPortDuplexMode	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.4
Syntax	INTEGER
Access	Read
Description	Contains the duplex mode of the selected port: No link 0 Full duplex 1 Half duplex 2
flWorkNetPortNegotiation	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.5
Syntax	INTEGER
Access	Read
Description	Contains information indicating whether auto negotiation is active: Active 1 Manual 2
flWorkNetPortName	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.6
Syntax	Octet string (0 ... 16)
Access	Read/write
Description	Contains the "name" of the port assigned by the user, e.g., "Robot 1".
flWorkNetPortEnable	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.7
Syntax	Integer
Access	Read/write
Description	Here you can disable the port: Port disabled 1 Port enabled 2
flWorkNetPortModus	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.9

Syntax	Integer32 (0 ... 1024)
Access	Read/write
Description	This object can be used to set the transmission mode for the relevant port: Auto negotiation 1 10 Mbps half duplex 2 10 Mbps full duplex 3 100 Mbps half duplex 4 100 Mbps full duplex 5

Fiberglass FX ports only support operation at 100 Mbps full duplex (5).

The autocrossing function is only active when auto negotiation is enabled. If the transmission speed or transmission mode is set to a fixed value, the autocrossing function is disabled.

flWorkNetPortIfIndex	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.11
Syntax	Integer32 (0 ... 1024)
Access	Read
Description	Specifies the index of the port according to IEEE 802.3ad.

flWorkNetPortType	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.13
Syntax	Octet string
Access	Read
Description	Specifies the medium of this port.

flWorkNetPortModuleName	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.14
Syntax	Octet string
Access	Read
Description	Specifies the "name" of the module.

flWorkNetPortInterfaceName	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.15
Syntax	Octet string
Access	Read
Description	Specifies the "name" of the interface.

flWorkNetPortStpMode	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.18
Syntax	Integer
Access	Read
Description	Specifies the port mode during redundancy operation: Spanning Tree 1 Rapid Spanning Tree 2

flWorkFirmware

OID	**1.3.6.1.4.1.4346.11.11.11**
	flWorkFWInfo
OID	1.3.6.1.4.1.4346.11.11.11.1

flWorkFWInfoVersion

OID	1.3.6.1.4.1.4346.11.11.11.1.1
Syntax	Octet string
Access	Read
Description	Contains the firmware version as a string. Example for Version "3.97": 0x33, 0x2e, 0x39, 0x37.

flWorkFWInfoState

OID	1.3.6.1.4.1.4346.11.11.11.1.2
Syntax	Octet string (6)
Access	Read
Description	Contains the firmware release as a string. Example for "beta": 0x62, 0x65, 0x64, 0x61.

flWorkFWInfoDate

OID	1.3.6.1.4.1.4346.11.11.11.1.3
Syntax	Octet string (6)
Access	Read
Description	Contains the creation date of the firmware version as a string. Example for "21.05.2001": 0x32, 0x31, 0x30, 0x35, 0x30, 0x31.

flWorkFWInfoTime

OID	1.3.6.1.4.1.4346.11.11.11.1.4
Syntax	Octet string
Access	Read
Description	Contains the creation time of the firmware version as a string. Example for "14:10:20": 0x31, 0x34, 0x31, 0x30, 0x32, 0x30.

flWorkFWInfoCopyright

OID	1.3.6.1.4.1.4346.11.11.11.1.5
Syntax	Display string
Access	Read
Description	Contains the owner of the firmware copyright. Copyright by Phoenix Contact GmbH & Co., 2003.

flWorkFWInfoBootVersion

OID	1.3.6.1.4.1.4346.11.11.11.1.6
Syntax	Octet string
Access	Read
Description	Contains the version of the boot loader as a string. Example for Version "2.65": 0x32, 0x2e, 0x36, 0x35.

flWorkFWInfoBootState

OID	1.3.6.1.4.1.4346.11.11.11.1.7
Syntax	Octet string
Access	Read
Description	Contains the boot loader release as a string. Example for "beta": 0x62, 0x65, 0x64, 0x61.

flWorkFWInfoBootDate

OID	1.3.6.1.4.1.4346.11.11.11.1.8
Syntax	Octet string
Access	Read
Description	Contains the creation date of the boot loader version as a string. Example for "09.03.01": 0x30, 0x39, 0x30, 0x33, 0x30, 0x31.

flWorkFWInfoBootTime

OID	1.3.6.1.4.1.4346.11.11.11.1.9
Syntax	Octet string
Access	Read
Description	Contains the creation time of the boot loader version as a string. Example for "14:10:20": 0x31, 0x34, 0x31, 0x30, 0x32, 0x30.

flWorkFWCtrl

OID 1.3.6.1.4.1.4346.11.11.11.2

flWorkFWCtrlBasic

OID 1.3.6.1.4.1.4346.11.11.11.2.1

flWorkFWCtrlReset

OID	1.3.6.1.4.1.4346.11.11.11.2.1.1
Syntax	Integer
Access	Read/write
Description	With write access, a reset can be executed with "2". With read access, the value is always "1".

flWorkFWCtrlHttp

OID	1.3.6.1.4.1.4346.11.11.11.2.1.6
Syntax	Integer
Access	Read/write
Description	This object can be used to disable the web server for the switch. The change only takes effect after a restart: Web server enabled: 2 Web server disabled: 1

flWorkFWCtrlSNMP

OID	1.3.6.1.4.1.4346.11.11.11.2.1.9
Syntax	Integer
Access	Read/write
Description	Here you can activate or deactivate the SNMP agent. The changes take effect after a restart. SNMP agent deactivated 1 SNMP agent activated 2

flWorkFWCtrlTrapDest

1.3.6.1.4.1.4346.11.11.11.2.2

flWorkFWCtrlTrapDestTable

1.3.6.1.4.1.4346.11.11.11.2.2.1

flWorkFWCtrlTrapDestEntry	
OID	1.3.6.1.4.1.4346.11.11.11.2.2.1.1
Syntax	
Access	
Description	Generates a table with the IP addresses of the trap managers.
flWorkFWCtrlTrapDestIndex	
OID	1.3.6.1.4.1.4346.11.11.11.2.2.1.1.1
Syntax	Integer32 (1 ... 1024)
Access	Read
Description	Indicates the index of the target component, which should receive the traps.

flWorkFWCtrlTrapDestIPAddr	
OID	1.3.6.1.4.1.4346.11.11.11.2.2.1.1.2
Syntax	IP address
Access	Read/write
Description	Indicates the IP address of the target component, which should receive the traps.
flWorkFWCtrlTrapDestCapacityMax	
OID	1.3.6.1.4.1.4346.11.11.11.2.2.1.1.2.3
Syntax	Integer32 (1 ... 1024)
Access	Read
Description	Specifies the maximum permissible number of trap receivers.
flWorkFWCtrlTrapDestEnable	
OID	1.3.6.1.4.1.4346.11.11.11.2.2.1.1.2.3
Syntax	Integer
Access	Read/write
Description	Activates/deactivates the sending of traps: Sending of traps deactivated: 1 Sending of traps activated: 2

flWorkFWCtrlTrapDestCapacityMax

OID	1.3.6.1.4.1.4346.11.11.11.2.2.2
Syntax	Integer32
Access	Read
Description	Specifies the maximum permissible number of trap receivers.

flWorkFWCtrlTrapDestEnable

OID	1.3.6.1.4.1.4346.11.11.11.2.2.3
Syntax	Integer
Access	Read/write
Description	This object can be used to disable the "send SNMP traps" function: Sending permitted 2 Sending not permitted 1

flWorkFWCtrlPasswd

OID	1.3.6.1.4.1.4346.11.11.11.2.3

flWorkFWCtrlPasswdSet

OID	1.3.6.1.4.1.4346.11.11.11.2.3.1
Syntax	Octet string (2 ... 24)
Access	Read/write

For security reasons the response is always "******" with read access.

Description

A new password, with a maximum of 12 characters, can be assigned here. Example:
- Your new password is to be "*factory3*".
- The password must be entered a second time for confirmation.
- You enter "*factory3factory3*".
- Your password for write access is now: "*factory3*".

flWorkFWCtrlPasswdSuccess

OID	1.3.6.1.4.1.4346.11.11.11.2.3.2
Syntax	Integer
Access	Read

Description

A message is displayed, which informs you whether the last change of password was successful:

- Not changed	1
- Failed	2
- Successful	3

flWorkFWCtrlLoginExpire

OID	1.3.6.1.4.1.4346.11.11.11.2.3.3
Syntax	Integer32 (30 ... 3600)
Access	Read/write

Description

Here, the number of seconds between two password entries is specified. After the time has elapsed, the password must be re-entered, if required.

Default	300
Range	30 - 3600

flWorkFWCtrlUpdate

OID 1.3.6.1.4.1.4346.11.11.11.2.4

flWorkFWCtrlTftpIpAddr

OID	1.3.6.1.4.1.4346.11.11.11.2.4.2
Syntax	IP address
Access	Read/write

Description

This object can be used to set the IP address of the TFTP server.

flWorkFWCtrlTftpFile

OID	1.3.6.1.4.1.4346.11.11.11.2.4.3
Syntax	Octet string (0 ... 64)
Access	Read/write
Description	This object can be used to set the name of the firmware file for TFTP download.

flWorkFWCtrlUpdateStatus

OID	1.3.6.1.4.1.4346.11.11.11.2.4.4
Syntax	Integer
Access	Read
Description	This object can be used to request the status of the firmware update:

Update successful	1
Update not successful	2
No update completed	3
Unknown	4

flWorkFWCtrlUpdateExecute

OID	1.3.6.1.4.1.4346.11.11.11.2.4.5
Syntax	Integer
Access	Read/write
Description	This object can be used to trigger the firmware update.

No firmware update	1
Execute firmware update	2

After a firmware update, a reset is required to activate the new firmware.

flWorkFWCtrlRunningUpdate

OID	1.3.6.1.4.1.4346.11.11.11.2.4.6
Syntax	Integer
Access	Read
Description	This object can be used to request the status of the firmware update:

Firmware update not started	1
Executing firmware update	2
Firmware update successful	3
Connection error	4
Incorrect path/file name	5
Error	6

flWorkFWCtrlAutoUpdate

OID	1.3.6.1.4.1.4346.11.11.11.2.4.7
Syntax	Integer
Access	Read/write
Description	This object can be used to trigger the firmware update with subsequent restart:

No firmware update	1
Execute firmware update	2

flWorkFWCtrlConf

OID 1.3.6.1.4.1.4346.11.11.11.2.5

flWorkFWCtrlConfStatus

OID	1.3.6.1.4.1.4346.11.11.11.2.5.1
Syntax	Integer
Access	Read
Description	This object can be used to request the status of the active device configuration:

Configuration OK	1
Configuration faulty	2
Configuration saved	3
Saving configuration	4

flWorkFWCtrlConfSave

OID	1.3.6.1.4.1.4346.11.11.11.2.5.2
Syntax	Integer
Access	Read/write
Description	This object can be used to save the device configuration:

Do not save configuration	1
Save configuration	2

flWorkFWCtrlDefaultUponDelivery

OID	1.3.6.1.4.1.4346.11.11.11.2.5.3
Syntax	Integer
Access	Read/write
Description	This object can be used to set the device to the default settings (basic settings - see 2.1.1 on page 2-1). It also triggers a restart:

Do not reset to default settings	1
Reset to default settings	2

flWorkFWCtrlSerial

OID 1.3.6.1.4.1.4346.11.11.11.2.6

flWorkFWCtrlSerialBaud

OID	1.3.6.1.4.1.4346.11.11.11.2.6.1
Syntax	Integer
Access	Read
Description	This object can be used to request the set data transmission speed of the serial interface: 2400 baud 1 9600 baud 2 19200 baud 3 38400 baud 4 57600 baud 5 115200 baud 6

flWorkFWCtrlSerialDataBits

OID	1.3.6.1.4.1.4346.11.11.11.2.6.2
Syntax	Integer
Access	Read
Description	Indicates the number of data bits in the serial interface: 8 bits 1

flWorkFWCtrlSerialStopBits

OID	1.3.6.1.4.1.4346.11.11.11.2.6.3
Syntax	Integer
Access	Read
Description	Indicates the number of stop bits in the serial interface: 1 bit 1 2 bits 2

flWorkFWCtrlSerialParity

OID	1.3.6.1.4.1.4346.11.11.11.2.6.4
Syntax	Integer
Access	Read
Description	Indicates the parity mode for the serial interface: None 1 Odd 2 Even 3

flWorkFWCtrlSerialFlowControl

OID	1.3.6.1.4.1.4346.11.11.11.2.6.5
Syntax	Integer
Access	Read
Description	Indicates the selected flow control for the serial interface: None 1 Hardware 2

flSwitch

OID	1.3.6.1.4.1.4346.15.11.11

flSwitchCtrl

OID	1.3.6.1.4.1.4346.15.11.11.1

flSwitchCtrlSpanTree

OID	1.3.6.1.4.1.4346.15.11.11.1.1
Syntax	Integer
Access	Read/write
Description	Activates/deactivates STP for the switch. RSTP deactivated 1 RSTP activated 2

To enable RSTP activation, the "flSwitchCtrlRedundancy" object must be set to RSTP.

flSwitchCtrlRedundancy

OID	1.3.6.1.4.1.4346.15.11.11.1.2
Syntax	Integer
Access	Read/write
Description	Indicates the selected redundancy mechanism for the switch. If "No redundancy" is selected, all redundancy mechanisms and the corresponding web pages are disabled. No redundancy 1 RSTP activated 2

flSwitchCtrlMacTableErase

OID	1.3.6.1.4.1.4346.15.11.11.1.11
Syntax	Integer
Access	Read/write
Description	This object controls the deletion of the unicast table. If this object is set to "2", the switch immediately deletes its unicast table. The switch then relearns and creates a new table. The object is always set to "1". Default 1 Delete unicast table 2

flSwitchCtrlLinkStatusMirroring

OID	1.3.6.1.4.1.4346.15.11.11.1.12
Syntax	Integer
Access	Read/write
Description	The "Port Link Status Mirroring" function can be used to mirror the link status of a port to one or more other ports. The function can then be activated and configured via SNMP, as the function is deactivated by default upon delivery. If the function is enabled when the switch is started, it is only activated once the switch has been fully booted. Deactivated (default) 1 Activated 2 The "flSwitchControlLinkStatusMirroring" object enables/disables the "Port Link Status Mirroring" function. The "flWorkNetPortLinkStatusMirrorMap" object writes the bit mask of the mirrored ports, where bit 0 stands for port 1, bit 1 for port 2, etc. If the bit equals 1, this port mirrors the master port. The object is assigned 0 by default.

flWorkNetPortLinkStatusMirrorMap

OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.19.X*
Syntax	Integer32 (0 - 255)
Access	Read/write
Description	X* = The port number of the master port to be mirrored Example 1: The status of port 6 should be mirrored to port 1. Set the "flWorkNetPortLinkStatusMirrorMap" object for port 6 to 1. (OID 1.3.6.1.4.1.4346.11.11.4.2.2.1.19.6 = 1) Then enable the function with the "flSwitchCtrlLinkStatusMirroring" object. 2 (OID 1.3.6.1.4.1.4346.11.11.15.1.12.0 = 2) Example 2: The status of port 5 should be mirrored to port 1, 3, and 4. Port status mapping must be calculated for port 1, 3, and 4: Mapping = (binary) 00001101 = 13 Set the "flWorkNetPortLinkStatusMirrorMap" object for port 5 to 13. (OID 1.3.6.1.4.1.4346.11.11.4.2.2.1.19.5 = 13) Then enable the function with the "flSwitchCtrlLinkStatusMirroring" object. (OID 1.3.6.1.4.1.4346.11.11.15.1.12.0 = 2)

flSwitchIgmpTableErase

OID	1.3.6.1.4.1.4346.15.11.11.3.3
Syntax	Integer
Access	Read/write
Description	This object controls the deletion of the multicast table. If this object is set to "2", the switch immediately deletes its multicast table. The switch then relearns and creates a new table. The object is always set to "1". Default 1 Delete multicast table 2

3.4 Management via local RS-232 communication interface

3.4.1 General function

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

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

3.4.1.1 Interface configuration

Make the following settings on your Windows PC.

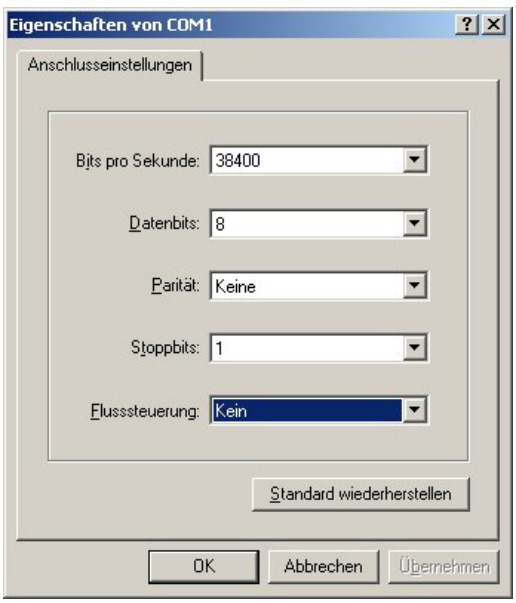


Figure 3-32 HyperTerminal configuration

3.4.1.2 Calling the user interface

Connect the PC and the switch using a suitable RS-232 cable (PRG CAB MINI DIN, Order No. 2730611). After establishing the connection, press the keyboard shortcut Ctrl + L on the PC. The switch then requests the screen contents.

3.4.2 User interface functions

3.4.2.1 Functions during the boot process after a restart

If you open the user interface in the first five seconds directly after an LMS restart, you have the option of triggering a firmware update. Since the actual switch firmware is not yet started at this stage, even in the event of an error, e.g., if the firmware on the device is faulty, this firmware can still be updated (see Section "Starting with faulty software" on page 3-56).

3.4.2.2 Functions during operation

The following functions are available in the user interface:

– Setting IP parameters
– Selecting the addressing mechanism
– Resetting to the default settings
– Activating/deactivating the web server, Rapid Spanning Tree, and the SNMP interface.

The activation/deactivation of the web server only takes effect after a "SAVE" and subsequent restart.

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

3.4.2.3 Structure of the user interface screens

Login screen

Figure 3-33 User interface login screen

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

Basic switch configuration

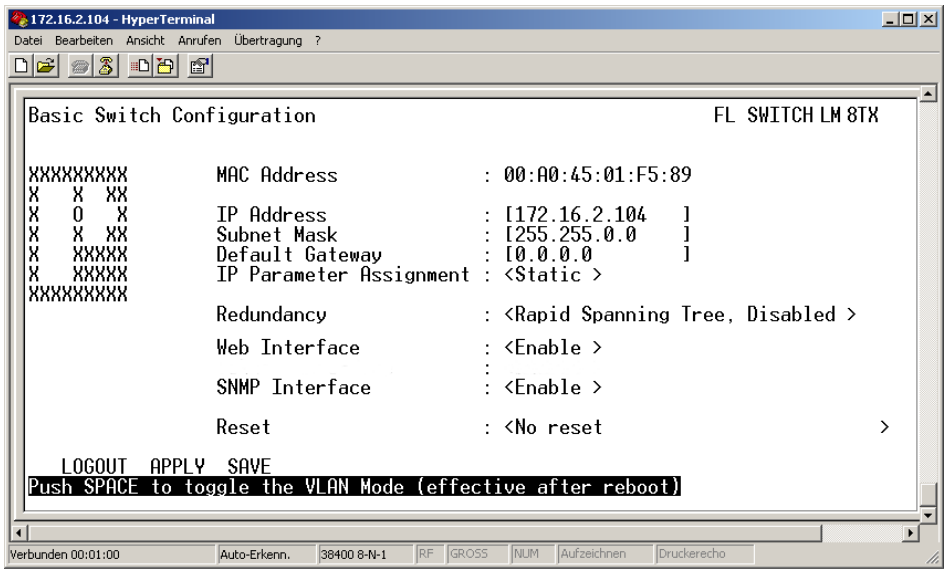


Figure 3-34 IP configuration in the user interface

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

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

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

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

Resetting to the default settings

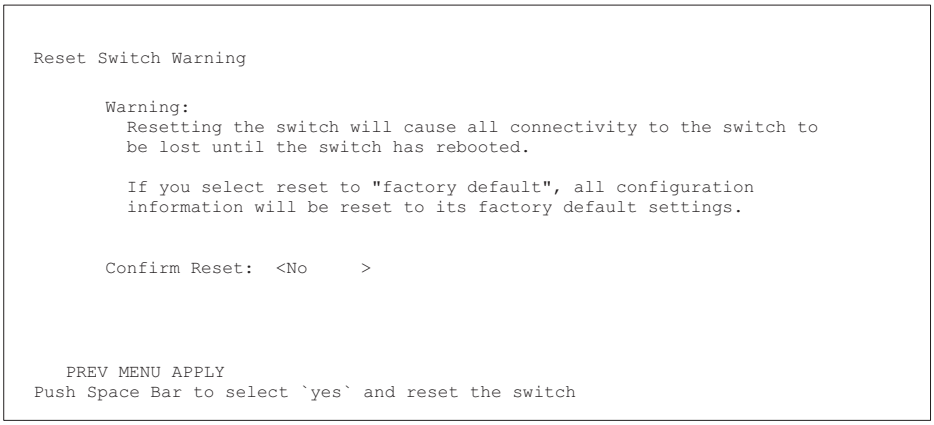


Figure 3-35 Resetting to the default settings

This screen can be used to reset the switch to the settings default upon delivery or to restart it. This screen can be opened by first setting the "Reset Switch" option or the "Reset Switch to factory defaults" option in the "Basic Switch Configuration" screen, and then selecting "Apply" or "Save". This undoes any changes to the configuration and resets all IP parameters to the settings default upon delivery (see Section 2.1.1 on page 2-1).

Resetting to the default settings also resets the password to "private". For security reasons, we recommend you enter a new, unique password.

3.4.3 Starting with faulty software

If the software installed on the LMS (firmware) is faulty, you can restore or update the firmware by means of an update.

Procedure:

– Connect the switch to your PC via the serial RS-232 interface. Make sure that your HyperTerminal is configured correctly (see configuration on page 3-52).

```
- - - > Phoenix Contact Lean Managed Switch < - - -

Phoenix Contact GmbH & Co. KG
www.phoenixcontact.com
BIOS version: X.XX


Press any key to stop booting ...
1

ENTER ´a´  TO DOWNLOAD SWITCH SOFTWARE USING XMODEM PROTOCOL
ENTER ´c´  TO CONTINUE BOOTING

PxC LMS systemprompt
```

Figure 3-36 Screen displayed on HyperTerminal when booting

If the device firmware is faulty, the following message appears:

```
        - - - > Phoenix Contact Lean Managed Switch < - - -
                    Phoenix Contact GmbH & Co. KG
                        www.phoenixcontact.com


Press any key to stop booting ...
 0
booting continues ...

SOFTWARE IMAGE CORRUPTED

YOU HAVE TO UPDATE THE SOFTWARE USING XMODEM PROTOCOL:

ENTER ´a´ TO DOWNLOAD SWITCH SOFTWARE USING XMODEM PROTOCOL
ENTER ´c´ TO CONTINUE BOOTING

PxC LMS systemprompt>
```

Figure 3-37 Selection menu for faulty firmware

Press "a" to download the new software. The following message then appears:

```
        - - - > Phoenix Contact Lean Managed Switch < - - -
                    Phoenix Contact GmbH & Co. KG
                       www.phoenixcontact.com



ENTER ´a´ TO DOWNLOAD SWITCH SOFTWARE USING XMODEM PROTOCOL
ENTER ´c´ TO CONTINUE BOOTING

PxC LMS systemprompt> a

Downloading firmware image with XMODEM over serial port ...

XMODEM Receive: Waiting for Sender ...

-_
```

Figure 3-38 XMODEM ready

The switch is now ready for the new firmware. In HyperTerminal, select "Send File" from the "Transmission" menu.

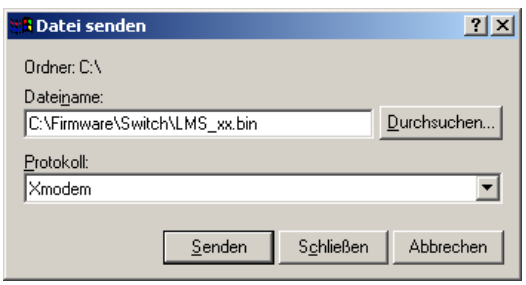


Figure 3-39 Xmodem - Send File option

Make sure that the protocol is set to "Xmodem", otherwise the transmission will fail.

Clicking "Send" starts the file transfer. The following screen shows the progress of the file transfer.

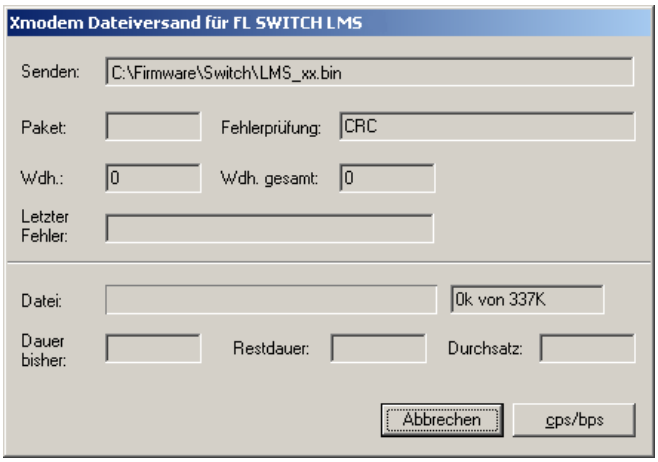


Figure 3-40 File transfer with Xmodem

File transfer may take a few minutes. Do not perform any other actions while the box is open.

Once the box has closed, a message appears in HyperTerminal. Enter "c" to continue with the boot process or trigger a reset using the reset button.

4 Rapid Spanning Tree

4.1 General function

4.1.1 General function

Loops

The Rapid/Spanning Tree Protocol (RSTP) is a standardized method (IEEE 802.1w/IEEE 802.1d) that enables the use of Ethernet networks with redundant data paths. Ethernet networks with redundant data paths form a meshed topology with initially impermissible loops. Due to these loops, data packets can circulate endlessly within the network and can also be duplicated. As a consequence, the network is usually overloaded due to circulating data packets and thus communication is interrupted. The meshed structure is therefore replaced by a logical, deterministic path with a tree structure without loops using the Rapid Spanning Tree algorithm. In the event of data path failure, some of the previously disconnected connections are reconnected to ensure uninterrupted network operation.

IEEE 802.1w

The Rapid Reconfiguration Spanning Tree Protocol (RSTP) is a standardized method (IEEE 802.1w) that enables the use of Ethernet networks with redundant data paths and prevents the long timer-controlled switch-over times of STP. Usually, the formal term "Rapid Reconfiguration Spanning Tree" is not used, rather just "Rapid Spanning Tree Protocol (RSTP)".

Example:

In the following network topology (six) redundant paths have been created to ensure access to all network devices in the event of a data path failure. These redundant paths are impermissible loops. The RSTP protocol automatically converts this topology into a tree by disabling selected ports. In this context, one of the switches is assigned the role of the root of the tree. From this root, all other switches can be accessed via a single data path.

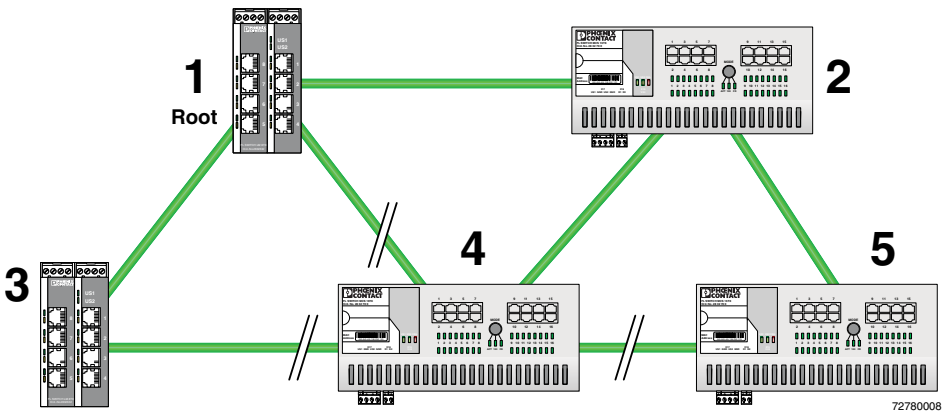


Figure 4-1 Possible tree structure with Rapid Spanning Tree

4.2 RSTP startup

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

1 Enable RSTP on all switches that are to be operated as active RSTP components in the network.

2 Connect the switches to form a meshed topology.

NOTE: Only create the meshed topology after activating RSTP.

4.2.1 Enabling RSTP on all switches involved

RSTP can be activated via web-based management, via the SNMP interface or via the serial interface.

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

4.2.1.1 Enabling using web-based management

Start web-based management for the switches, e.g., using Factory Manager, switch to the "General Configuration" menu, then the "User Interfaces" page. Activate the "Rapid Spanning Tree" function under "Redundancy" and confirm by entering your password.

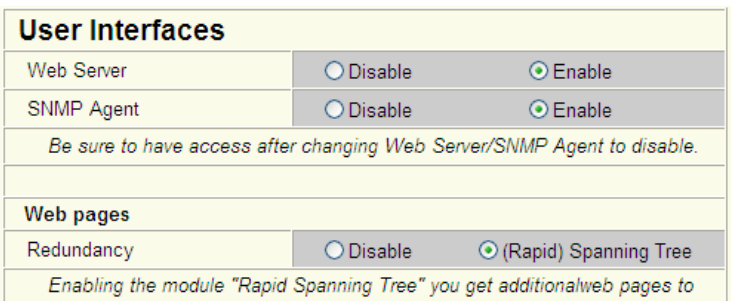


Figure 4-2 "User Interfaces" menu

The previously created configuration is lost if "No redundancy" is selected in the WBM menu following RSTP configuration.

Now switch to the "RSTP General" menu. Here, you will find various information about the Rapid Spanning Tree configuration.

RSTP General	
(Rapid) Spanning Tree Status	This bridge is the **root** bridge!
System Up Time	1 days 18 hours 36 minutes 9 seconds
Last Topology Change	1 days 18 hours 36 minutes 3 seconds ago
Topology Changes	1
Designated Root	8000 00:A0:45:00:9A:1F
Root Port	0
Root Cost	0
Maximum Age of STP Information	20s
Hello Time	2s
Forward Delay	15s
Note: This web page will be refreshed in 1 sec automatically (change the interval at the web page 'Services')!	

Figure 4-3 "RSTP General" web page

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

Port roles

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

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

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

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

RSTP Configuration

It is sufficient to set the Rapid Spanning Tree status to "Enable" in order to start RSTP using default settings. Priority values can be specified for the switch. The root and alternate ports can be specified via these priority values.

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

Redundant connections can now be created.

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

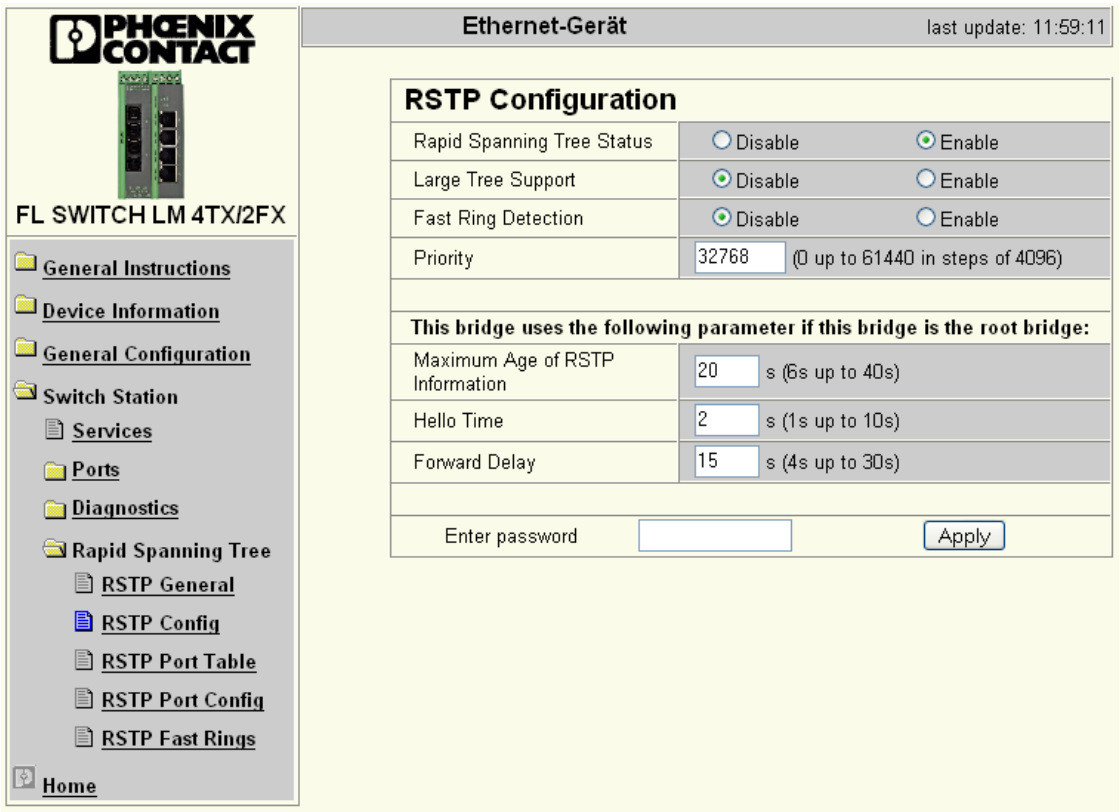


Figure 4-4 "RSTP Configuration" web page

Maximum Age of RSTP Information
RSTP information (BPDU) is sent by the root switch at an age of "0" and at hello time intervals. If a BPDU was received, all other switches send their own configuration message via the ports for which the switch itself is the designated switch. The age of the information (BPDU) is increased by one second every time the information passes a switch.

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

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

RSTP Port Table

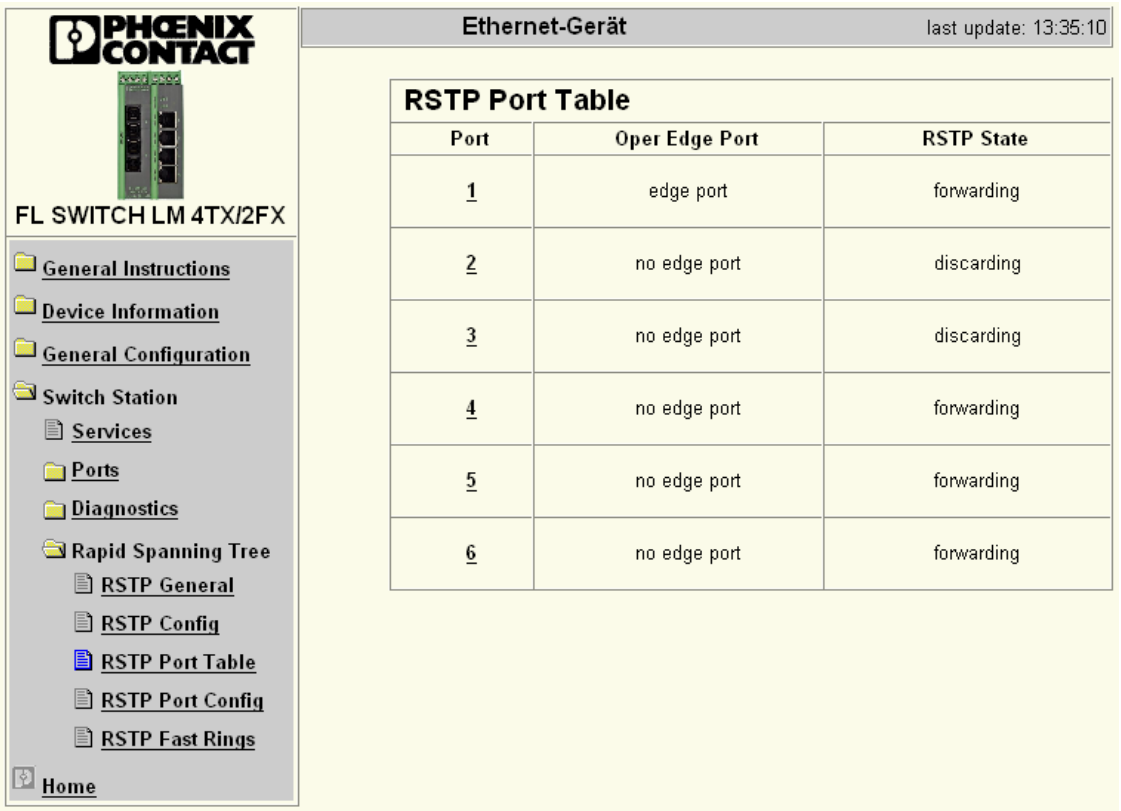


Figure 4-5 "RSTP Port Table" web page

Oper Edge Port
All ports that do not receive any RSTP BPDUs become edge ports, i.e., ports that switch to the "Forwarding" state immediately after restart.

RSTP State
Indicates the current RSTP state of the relevant port.

Possible states:

– "Forwarding"
The port is integrated in the active topology and forwards data.
– "Discarding"
The port does not take part in data transmission.
– "Learning"
The port does not take part in data transmission of the active topology, however, MAC addresses are learned.

4.2.1.2 RSTP Port Configuration

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

This page displays the valid RSTP configuration settings for the selected port.

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

4.2.1.3 Switch/port ID

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

Bridge identifier

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

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

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

Port identifier

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

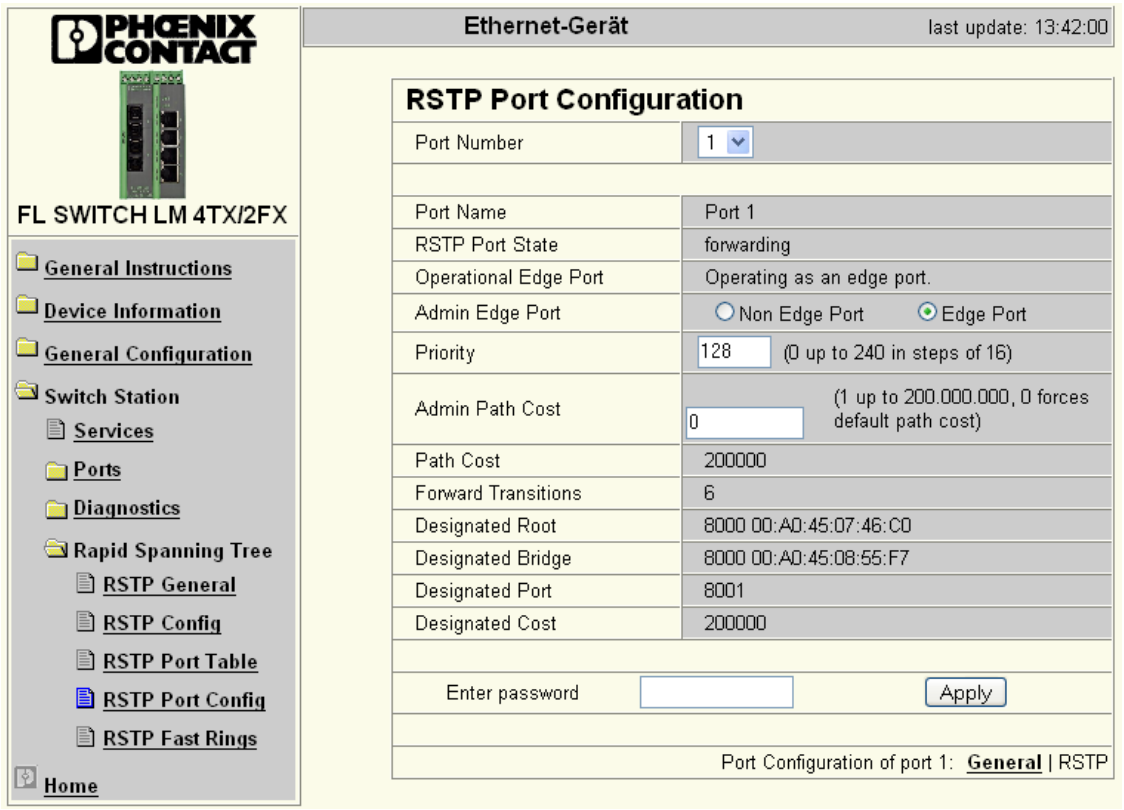


Figure 4-6 "RSTP Port Configuration" web page

Port Number
Indicates the number of the port currently selected.

Port Name
Indicates the name of the port.

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

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

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

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

Admin Path Cost
Indicates the path cost set for this port. A path cost equal to "0" activates the cost calculation according to the transmission speed (10 Mbps = 100; 100 Mbps = 19).

Path Cost
Indicates the path cost used for this port.

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

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

Designated Root
Root bridge for this Rapid Spanning Tree.

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

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

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

Common features/differences with regard to STP

As with STP, a device is also selected as the root for RSTP and every port is assigned a role according to its participation within the topology.

Port states

The number of port states is also reduced in RSTP. Only the "Forwarding", "Discarding", and "Learning" states are still available if the network is operated in mixed operation of STP and RSTP.

Frame duplication

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

4.2.1.4 Enabling via serial interface

Establish a connection to the switch as described in Section "Management via local RS-232 communication interface" on page 3-52. Set "Rapid Spanning Tree, Enabled" on the following page in the "Redundancy" field and select "Save".

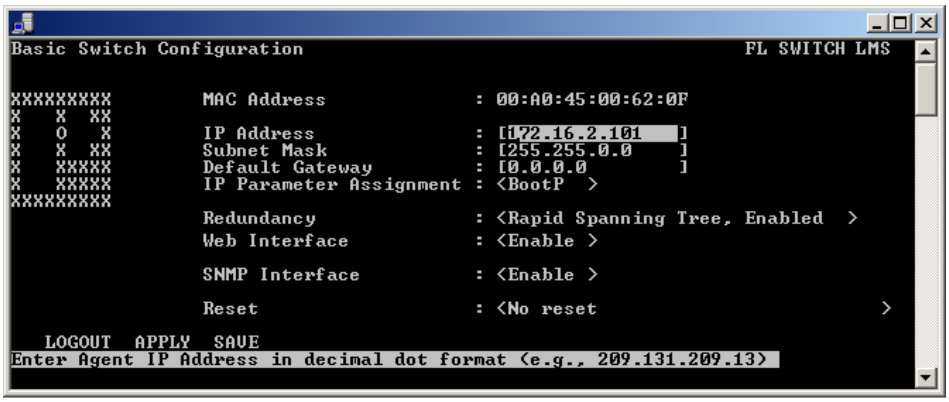


Figure 4-7 Activating Rapid Spanning Tree

4.2.1.5 Connecting the switches to form a meshed topology

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

A data path between Rapid Spanning Tree switches can be:

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

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

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

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

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

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

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

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

Example:

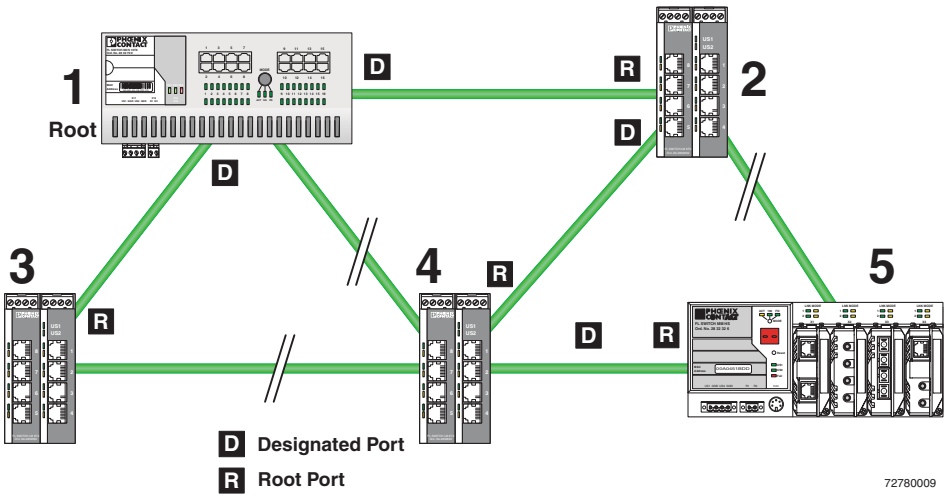


Figure 4-8 Example topology

There are six loops in the example topology shown above. Each of these loops contains active STP components, e.g. device 4 and device 2. In this way, all loops are broken by STP.

– **Rule 3: No more than ten active Spanning Tree components in the topology when using Spanning Tree default settings**
  The ability to disintegrate any topology to form a tree without loops requires a complex protocol that works with several variable timers. These variable timers are dimensioned using the default values recommended by the IEEE standard so that a topology with a maximum of ten active Spanning Tree components always results in a stable network.

4.2.2 RSTP fast ring detection

The "RSTP Fast Ring Detection" function can be activated on the "RSTP Configuration" web page.

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

Structure of the ring ID

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

– Easier to identify redundant paths and locate blocking ports.

– Possible to check whether the desired topology corresponds to the actual topology.

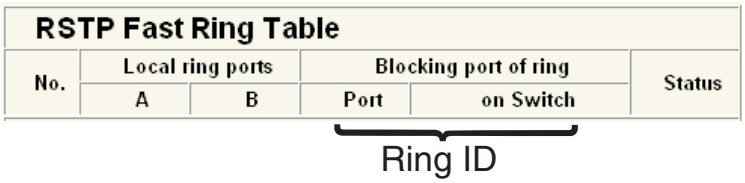


Figure 4-9 RSTP ring table

Information in WBM

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

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

Blocking port
This port deliberately breaks the loop.

Ring detection states

The following states can occur for ring detection:

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

In the event of a link failure in the ring, the "trapRstpRingFailure" trap is sent.

If "Broken" or "Failed" status lasts for longer than 60 seconds, it is no longer displayed after the next topology modification, since these rings no longer exist.

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

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

4.2.2.1 Fast ring detection switch-over times

With the maximum permissible number of 57 switches in a ring, typical switch-over times range from 100 to 500 ms with fast ring detection.

4.2.3 Connection failure - Example

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

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

Switch 3 - Failed on Port A

Switch 4 - Broken

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

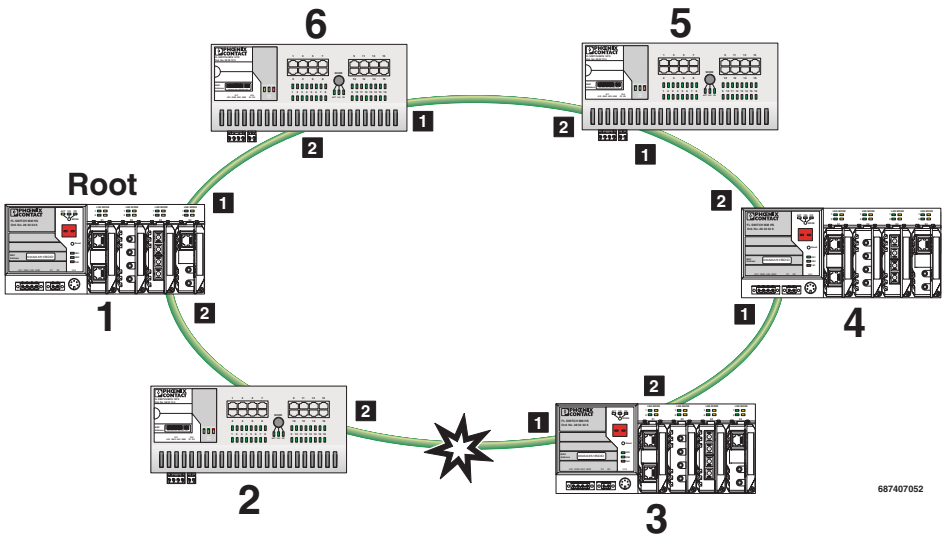


Figure 4-10 Connection failure with RSTP ring detection

4.2.4 Example topologies

4.2.4.1 Redundant coupling of network segments

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

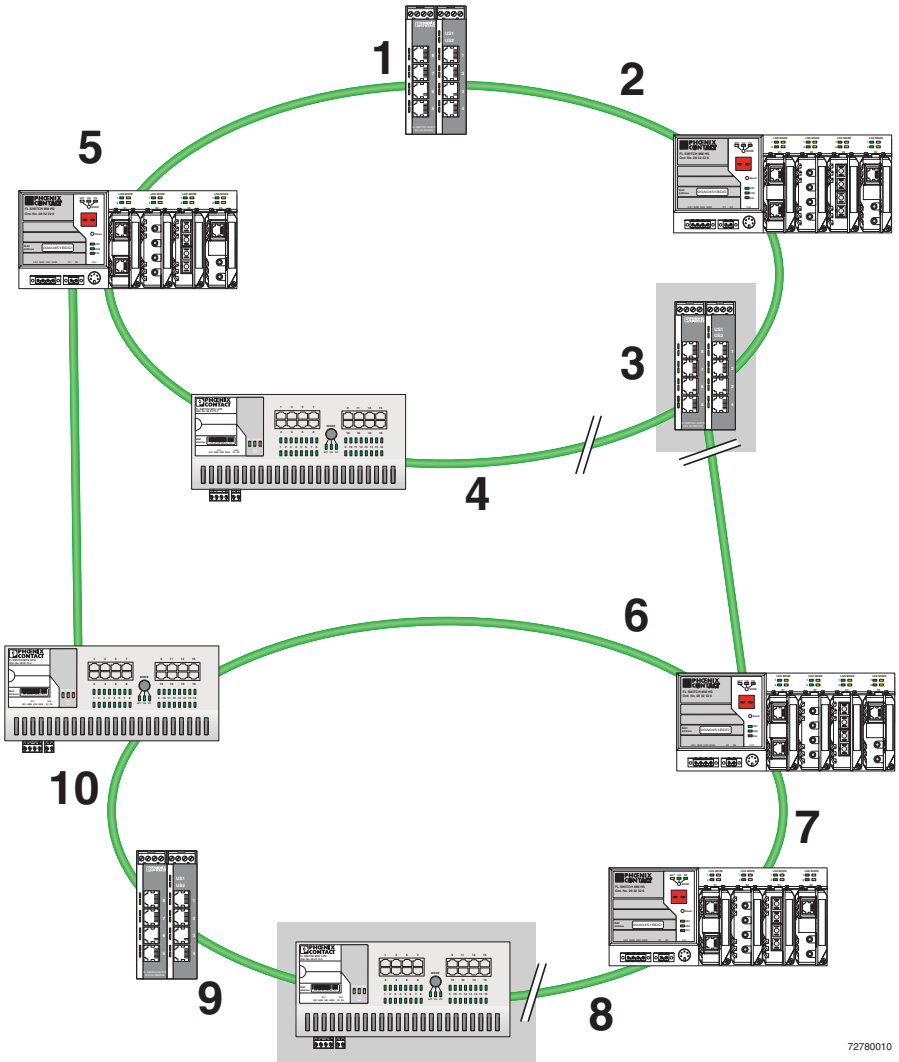


Figure 4-11 Redundant coupling of network segments

4.2.4.2 Flowchart for specifying the root path

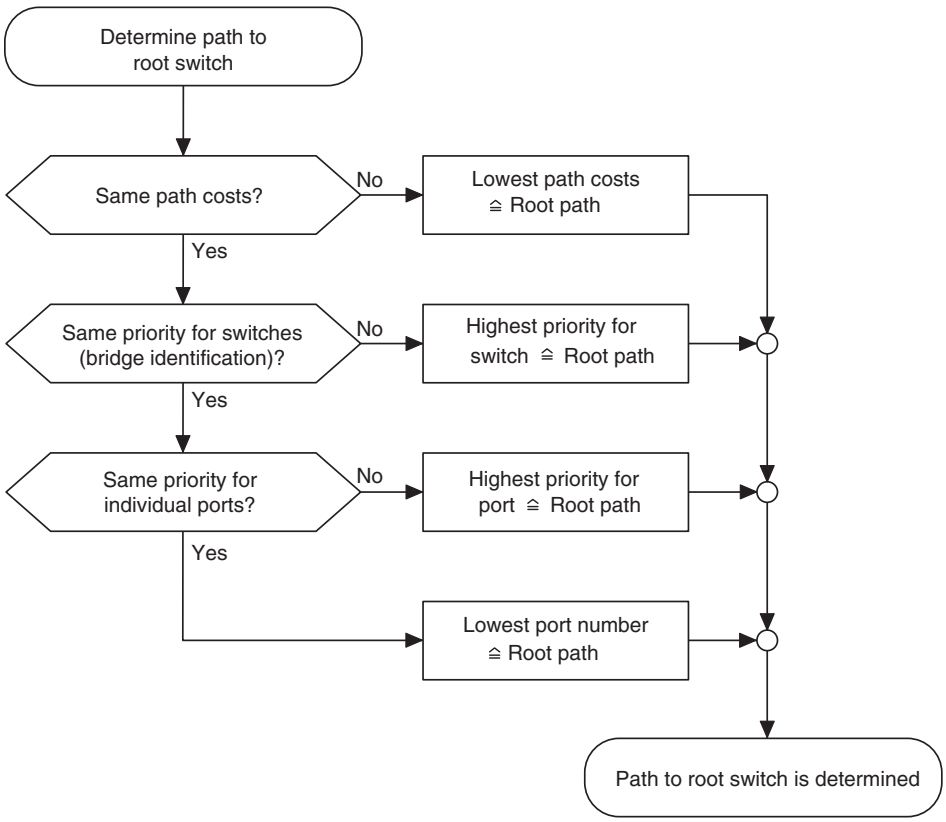


Figure 4-12 Flowchart for specifying the root path

4.2.4.3 Extended configuration

It may be useful to actively specify the topology that is formed due to the Rapid Spanning Tree Protocol and to not leave it to the random MAC addresses of the switches involved. Non-blocking/blocking data paths can thus be influenced and a load distribution specified. It may also be useful to explicitly disable the Rapid Spanning Tree Protocol at ports that do not participate in Rapid Spanning Tree so as to benefit from the fast forwarding function. The Rapid Spanning Tree Protocol must also be disabled at individual ports if two different network segments - both using Rapid Spanning Tree - are to be coupled via these ports without the two tree structures merging into a large Spanning Tree.

Specifying the root switch

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

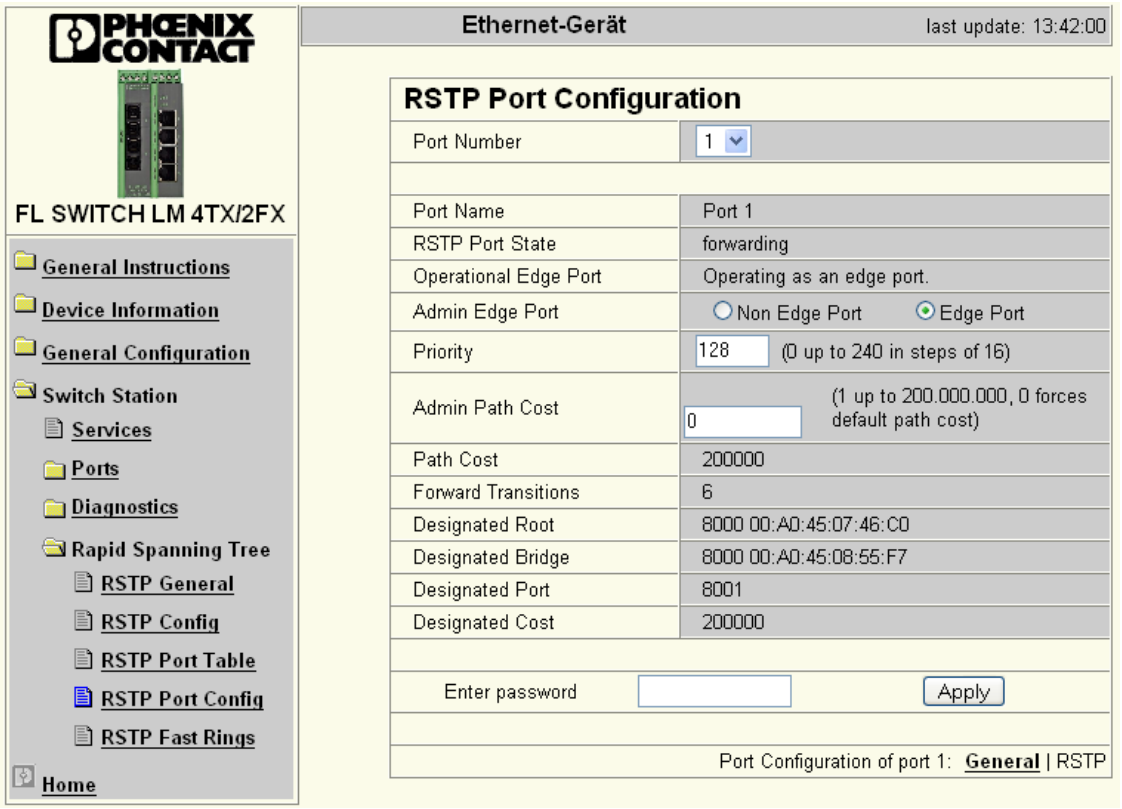


Figure 4-13 Specifying the root switch priority

Specifying the root port and designated port

The root port and designated port are always the ports with the lowest path costs. If the costs are the same, the priority is the decisive criterion. If the priorities are also the same, the port number is the decisive criterion. Specify an appropriate combination of costs and priority on the "RSTP Port Configuration" page in WBM for the port specified as the root port or designated port. Make sure that all the other network switches either have higher costs or a lower priority (higher value).

4.2.4.4 Disabling the Rapid Spanning Tree Protocol/using the fast forwarding function

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

– A termination device is connected to the port.

– Additional infrastructure components are connected to the port. The corresponding network segment does not contain any loops.

Additional infrastructure components are connected to the port, forming a Rapid Spanning Tree of their own. No additional redundant connections to this network segment are permitted.

4.2.4.5 Modifying the protocol timers

NOTE: Modifying the protocol timers may result in unstable networks.

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

Specifying the timer values

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

– 2 x Forward Delay - 1 s ≥ MaxAge

– MaxAge ≥ 2 × Hello Time + 1 s

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

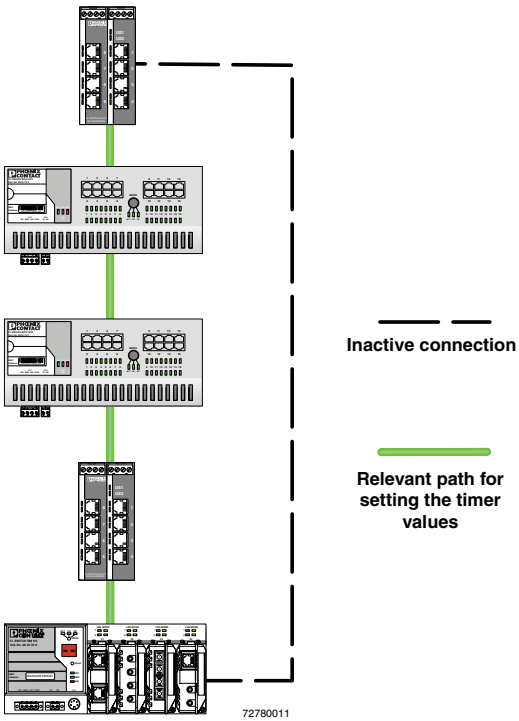


Figure 4-14 Example 1 for the "relevant path"

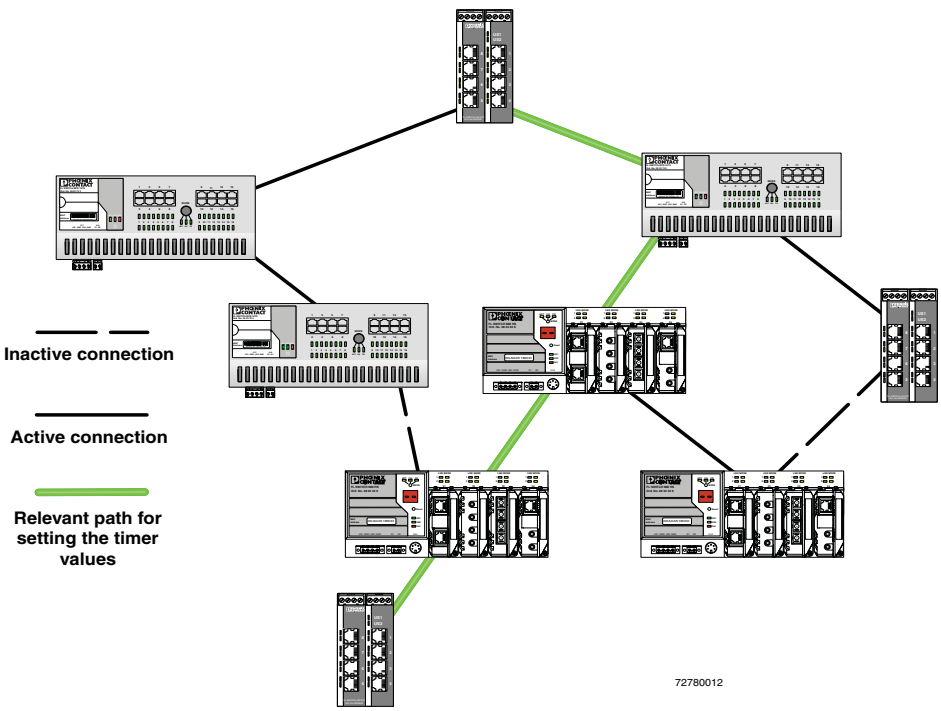


Figure 4-15 Example 2 for the "relevant path"

4.2.4.6 Reconfiguration times

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

The minimum reconfiguration time is:
2 × Forward Delay

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

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

Switch-over time response to be expected for Rapid Spanning Tree

Overview of the switch-over time response to be expected for the maximum number of switches within a Spanning Tree segment.

MaxAge	Hello Time	Forward Delay	Maximum number of active RSTP switches	Switch-over time
10 s	1 s	≥ 6 s	5	22 s
20 s	1 s	≥ 11 s	10	42 s
30 s	1 s	≥ 16 s	15	62 s
40 s	1 s	≥ 21 s	20	82 s
20 s	***2 s***	***15 s***	***9***	***50 s***

Bold/italic **= Default**

4.2.5 Configuration notes for Rapid Spanning Tree

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

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

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

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

- For short switch-over times, structure your network in such a way that a maximum of seven switches are located in a cascade up to the root switch. The switch-over times can range from 2 to 8 s.
- Use priority assignment to specify a central switch as the root.
- It is also recommended to assign a switch as the backup root.
- For short switch-over times, all switches should support the Rapid Spanning Tree Protocol.

4.3 Large Tree support

4.3.1 Large Tree support

If RSTP is operated using the default values, it is suitable for up to seven switches along the relevant path (see Figure 4-14 on page 4-17 and Figure 4-15 on page 4-17 as an example for the relevant path). The RSTP protocol would therefore be possible in a ring topology for up to 15 switches.

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

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

4.3.2 Properties of Large Tree support

– 28 switches below the root
– Rings with a total of 57 switches

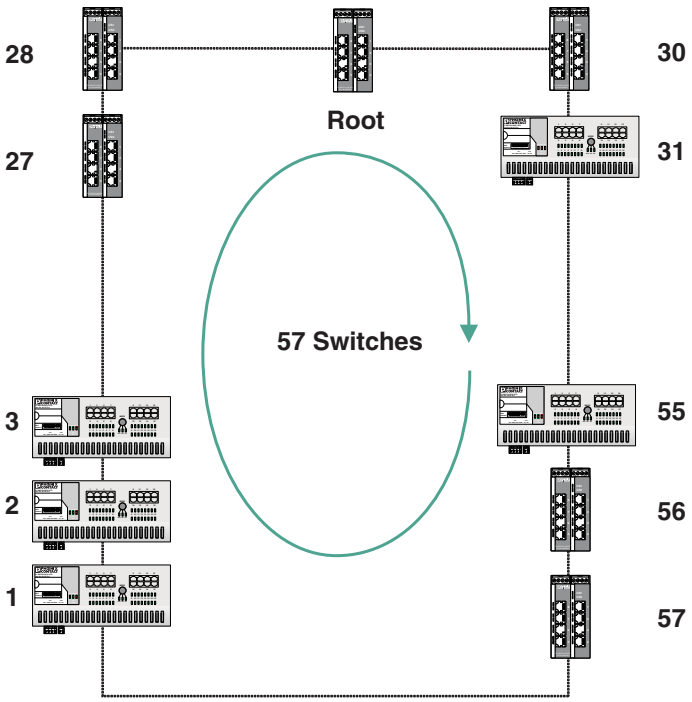


Figure 4-16 Topology example for Large Tree support

5 Multicast filtering

5.1 Basics

Multicast

Multicast applications, unlike unicast applications with point-to-point communication, do not transmit their data with the MAC address of the destination, but with an independent multicast group address. Always using wireless communication, a station transmits **one** data packet that is received by one or more receiving stations.

Advantages:

1 If, for example, a data packet of a transmitter is to be transmitted to eight receivers, the same packet does not have to be sent eight times to the addresses of all eight devices. Instead it only needs to be sent once to the address of the multicast group that includes the eight devices.

2 When using multicast communication and filtering, the bandwidth requirement for data transmission is reduced because each packet is only transmitted once.

5.2 Dynamic multicast groups

5.2.1 Internet Group Management Protocol (IGMP)

IGMP on Layer 3

The Internet Group Management Protocol describes a method for distributing information via multicast applications between routers and termination devices at IP level (Layer 3).

When starting a multicast application, a network device transmits an IGMP membership report and thus announces its membership of a specific multicast group. A router collects these membership reports and thus maintains the multicast groups of its subnetwork.

Query

At regular intervals, the router sends IGMP queries. This prompts the devices with multicast receiver applications to send another membership report.

The "IGMP Query" function only transmits in the management VLAN and only stops if there is a better querier in the management VLAN.

The router enters the IP multicast group address from the report message in its routing table. This means that frames with this IP multicast group address in the destination address field are only transferred according to the routing table. Devices that are no longer members of a multicast group log out with a leave message (IGMP Version 2 or later) and no longer send report messages.
The router also removes the routing table entry if it does not receive a report message within a specific time (aging time). If several routers with active IGMP query function are connected to the network, they determine among themselves which router performs the query function. This depends on the IP addresses, as the router with the lowest IP address continues to operate as the querier and all the other routers no longer send query messages. If these routers do not receive a new query telegram within a specific period of time, they themselves become queriers again. If there are no routers in the network, a suitably equipped switch can be used for the query function.

IGMP snooping

A switch which connects a multicast receiver with a router can read and evaluate IGMP information using the IGMP snooping method. IGMP snooping translates IP multicast group addresses into multicast MAC addresses, so that the IGMP function can also be detected by Layer 2 switches. The switch enters the MAC addresses of the multicast receivers, which were obtained from the IP addresses by IGMP snooping, in its own multicast filter table. Thus the switch filters multicast packets of known multicast groups and only forwards packets to those ports to which corresponding multicast receivers are connected.

IGMP snooping can only be used on Layer 2 if all termination devices send IGMP messages. The IP stack of multicast-compatible termination devices with applications linked to a multicast address automatically sends the relevant membership reports.

IGMP snooping operates independently of the Internet Group Management Protocol (IGMP).

5.2.1.1 Extended multicast filtering

If IGMP snooping is active, multicast data streams are also detected for which no membership reports of possible recipients are registered. For these multicasts, groups are created dynamically. These multicasts are forwarded to the querier, i.e., the querier port is entered in the group.

If the switch itself is the querier, these multicasts are blocked.

5.2.1.2 "General Multicast Configuration" web page

This web page provides global settings for multicast support. Here, IGMP snooping can be activated and an aging time can be specified for IGMP snooping information.

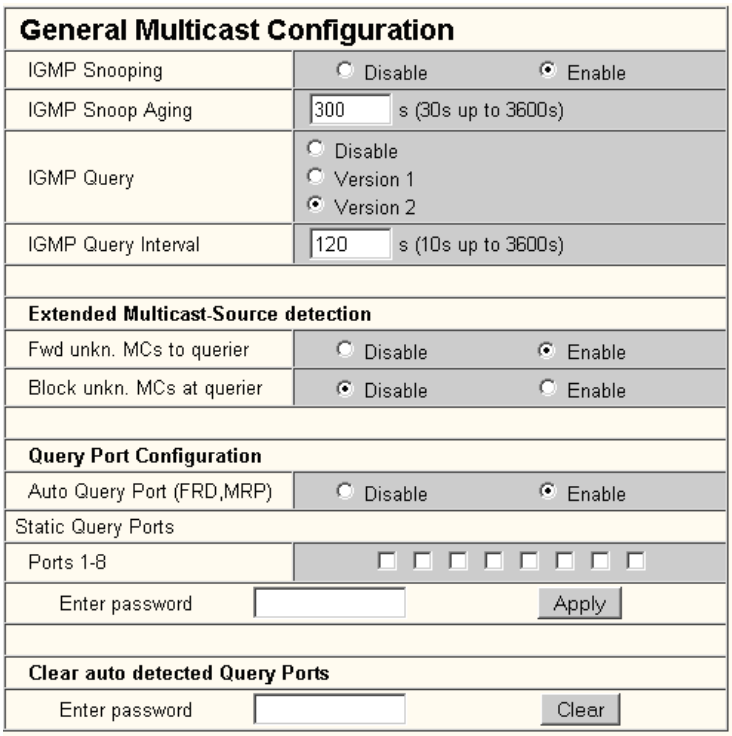


Figure 5-1 "General Multicast Configuration" web page

Please note that the switch supports 50 multicast groups at any given time.

IGMP Snooping
In IGMP snooping, the switch passively listens in on the IGMP messages that are sent over the network and dynamically creates the appropriate groups. The groups are not saved and will be lost during every power down or when the snooping function is switched off.

IGMP Snoop Aging
IGMP snoop aging is the time period during which membership reports are expected. If this time passes without new membership reports being received, the associated port is deleted from the groups.

IGMP Query
An LMS with activated query function actively sends queries at "query intervals" and evaluates the received reports. The LMS only sends IGMP query reports if IGMP snooping is enabled and only in the management VLAN.

IGMP Query/IGMP Query Interval
A switch with activated query function actively sends queries regarding the version selected under "IGMP Query" at the "IGMP Query Interval" and evaluates the received reports. The switch only sends IGMP query reports if IGMP snooping is enabled and only in the management VLAN.

Extended Multicast Source Detection
(see 5.3 "Multicast source detection" on page 5-5)

Forward unknown Multicasts to querier

Select whether a group which forwards packets to the querier is created for unknown multicast packets.

Block unknown Multicasts at querier

Select whether unknown multicast packets are to be blocked at the querier.

Query Port Configuration

Auto Query Port (FRD, MRP)
Activates the automatic selection of additional query ports by means of fast ring detection and/or MRP. Redundant ports are thereby 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 groups.

If this function is activated, the multicast tables are not deleted on redundancy switch-over. Deletion of the multicast tables is triggered when the auto query ports are deactivated in order to force a new multicast group learning process in the event of redundancy switch-over.

Static Query Ports

Select the ports that are static query ports.

Clear auto detected Query Ports

Deletion of the ports automatically assigned to the groups.

5.3 Multicast source detection

Multicast source detection can be used to create dynamic multicast groups without the multicast receiver/membership report sender in the network being active.

5.3.1 Properties of multicast source detection

The following properties apply if IGMP snooping has previously been activated globally.

a) The switch is not the IGMP querier in the network segment because the querier function is disabled or another device has assumed the querier role.

– If the switch receives an IGMP query packet, it will save the port via which it received the packet for the IGMP query time and add it to each dynamic multicast group.
– If the switch receives a multicast packet and is still able to create new dynamic multicast groups (upper limit not reached) and it has saved one or more ports via which it received queries, the switch will:
  1. Create a new multicast group for this multicast address, provided one does not already exist
  2. Add the port via which it received the multicast packet and all query ports to this new group
– The multicast groups created as described above are deleted in accordance with the timeout rules. For example, if no more membership reports are received, if the associated port is deleted from the groups or if no port, other than the ports receiving queries, is a member of the group, this group is deleted.

b) The switch is the active querier in the network segment

– If the switch receives a multicast packet and is still able to create new dynamic multicast groups (upper limit not reached) and it has saved one or more ports via which it received queries, the switch will:
  1. Create a new multicast group for this multicast address, provided one does not already exist
  2. Add the port via which it received the multicast packet and all query ports to this new group
– The multicast groups created as described above are deleted in accordance with the timeout rules. For example, if no more membership reports are received, if the associated port is deleted from the groups or if no port, other than the ports receiving queries, is a member of the group, this group is deleted.

5.3.1.1 Multicast registration with GMRP

GMRP (GARP Multicast Registration Protocol) enables the distribution of multicast group destination addresses to Layer 2 devices that do not support IGMP snooping. After a multicast device has registered with the switch (e.g., by means of an IGMP report), the switch sends a GMRP broadcast packet to all GARP switches, which contains the multicast group destination address and indicates whether the switch is joining or leaving the group. The other switches can thus create their own multicast groups and add the receive port to the group. By default, GMRP is activated as soon as IGMP snooping is activated. The switches that receive the GMRP packets do not have to support IGMP snooping in order to receive and evaluate the GMRP packets.

6 Virtual Local Area Network (VLAN)

6.1 Basics

VLAN

A VLAN is a closed network, which is separated logically/functionally rather than physically from the other networks. A VLAN creates its own broadcast and multicast domain, which is defined by the user according to specified logical criteria. VLANs are used to separate the physical and the logical network structure.

– Data packets are only forwarded within the relevant VLAN.
– The members of a VLAN can be distributed over a large area.

The reduced propagation of broadcasts and multicasts increases the available bandwidth within a network segment. In addition, the strict separation of the data traffic increases system security.

A router or similar Layer 3 device is required for data traffic between VLANs.

For the switch, the VLANs can be created statically or dynamically. For dynamic configuration, the data frames are equipped with a tag. A tag is an extension within a data frame that indicates the VLAN assignment. If configured correspondingly, this tag can be added during transmission to the first switch in the transmission chain and removed again from the last one. Several different VLANs can thus use the same switches/infrastructure components. Alternatively, termination devices that support VLAN tags can also be used.

6.2 Enabling the VLAN web pages in web-based management

Start web-based management for the switches, e.g., using Factory Manager, switch to the "General Configuration" menu, then the "User Interfaces" page. Activate the "VLAN" function and confirm by entering your password.

When activating "VLAN" under "User Interfaces", the VLAN mechanism is **not** activated. In the WBM menu, the "VLAN" page - under which the function can be configured and activated - is enabled.

When deactivating the VLAN configuration pages under "User Interfaces", the VLAN mechanism is **not** deactivated. The saved VLAN configuration is retained.

6.2.1 Management VLAN ID

The management of the switch is assigned to VLAN 1 by default upon delivery. In addition, all ports are assigned to VLAN 1 by default upon delivery. This ensures that the network-supported management functions can be accessed via all ports.

Make sure that the LM switch is always managed in a VLAN that you can also access.

VLAN ID 1 cannot be deleted and is thus always created on the switch.

If you delete the VLAN in which the LM switch is managed, management is automatically switched to VLAN 1.

The "IGMP Query" function only transmits in the management VLAN and only stops if there is a better querier in the management VLAN.

6.2.2 Changing the management VLAN ID

6.2.2.1 Configuration in transparent mode

1. In WBM, enable the pages for VLAN configuration (WBM: User Interfaces/Virtual LAN).
2. Create the required VLANs on the "Static VLANs" web page.
3. On the "VLAN Port Cfg. Table" web page, assign the ports for incoming packets to individual VLANs using the VLAN ID.
4. On the "IP Configuration" web page, the desired management VLAN ID can now be set.
5. On the "General VLAN Configuration" web page, set the switch to "Tagging" VLAN mode.
6. Save the configuration on the "General Configuration/Configuration Management" web page and restart the switch.

6.2.2.2 Configuration in tagging mode (usually used to change the management VLAN ID in the event of an existing VLAN configuration)

1. Connect the PC directly to the switch to be configured via a port (A) whose VLAN ID is set to "1".
2. Update the firmware to Version 3.30 or later and restart the switch.
3. Place another port (B) in the desired management VLAN. Port B must be an "untagged member" of the desired management VLAN. Set the corresponding port VLAN ID, if necessary.
4. Set the desired VLAN ID as the management VLAN.
5. Connect your PC to the switch via port B and save the configuration.

6.3 General VLAN Configuration

Basic settings for VLAN operation can be made on the "Switch Station/VLAN/General VLAN Configuration" web page.

Transparent

In "Transparent" mode, the switch processes the incoming data packets as described in the "Frame switching" section (see Section 2.2 on page 2-8). 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.

Tagging

In "Tagging" mode, incoming packets are received according to the specified VLAN rules, a VLAN tag is added, if required, and the packet is then processed by the switch and the management level according to the information in the tag. When transmitting Ethernet packets, the switch observes the rules for the relevant VLAN or the relevant output port.

The management VLAN ID specifies in which VLAN the switch can be accessed if it is operating in "Tagging" VLAN mode.

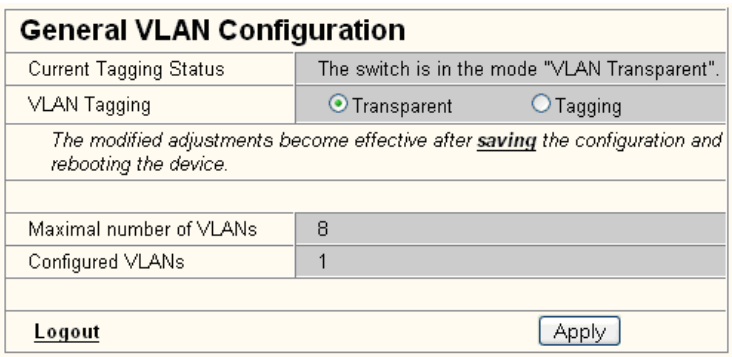


Figure 6-1 "General VLAN Configuration" menu

The switch supports a maximum of 8 different VLANs.

After switching the VLAN mode from "Tagging" to "Transparent" or vice versa, the active configuration must be saved and a device reset triggered so that the modification becomes active. The current valid state can be read in the "Current Tagging Status" line.

6.4 Current VLANs

The "Current VLANs" web page provides an overview of the VLANs currently set up. In addition, refer to the table for the VLAN in which the switch is actually managed. All static and dynamic VLANs are listed here. A distinction is made between tagged (T) and untagged (U) group members, as well as non-members (-) (see possible states on page 6-5).

Current VLANs

VID	Status	Group	Membership
1	static/ **Management Vlan**	Ports 1-8	U U U U U U U U
12	static	Ports 1-8	- T T - - - - -
24	static	Ports 1-8	- - - - T T - -

(T=Tagged, U=Untagged, -=Non Member)

*This table, indicates, out of which ports, each VLAN's data is to be sent, using configuration data entered manually (i.e. web page "**Static VLANs**).*

Figure 6-2 "Current VLANs" web page

When the maximum number of created VLANs (static and/or dynamic) is reached, the following text appears below the key for the member states: "The switch supports only 8 VLANs! Further VLANs will be refused!".

VLAN 1 is always created statically and all ports are added to it as untagged members.

6.4.1 Static VLANs

Static VLANs can be created on this web page. Up to 7 new VLANs can be created (VLAN 2 to VLAN 8). If more are created, a corresponding message will be displayed.
VLAN 1 is always created statically and all ports are added to it as untagged members. By default upon delivery, with "Tagging" VLAN mode activated, network-based management interfaces (WBM, Telnet, and SNMP) are only available from VLAN 1. This means that in order to access the management interfaces, you must either implement data traffic in tagged mode without VLAN tag, where the switch is accessed via ports using the VLAN ID or you must use data traffic with a VLAN tag with ID 1.

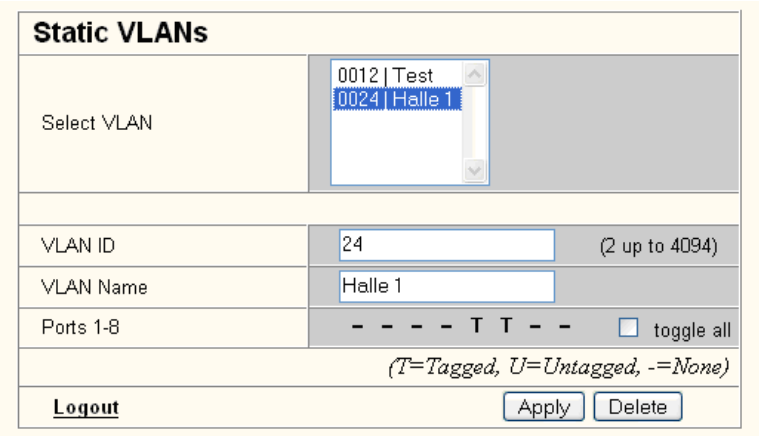


Figure 6-3 "Static VLANs" menu

On this web page you can create static VLANs by assigning a VLAN ID and VLAN name. The ports are then assigned to the individual VLANs by selecting the relevant VLAN and clicking on the character in the "Ports 1-8" line that indicates the current port status. Various options are selected by clicking on the status several times. By clicking on "toggle all", all available ports in the relevant port group change their status.

The possible states are:

T = Tagged

Ports with "Tagged" status belong to the selected VLAN and packets are sent to this port with VLAN tag.

U = Untagged

Ports with "Untagged" status belong to the selected VLAN and packets are sent to this port without VLAN tag. An "Untagged" port cannot belong to multiple VLANs - otherwise there is no logical division (except VLAN 1).

- = None

Ports with "None" status are not integrated into the VLAN.

6.4.2 VLAN Port Configuration

Port-specific VLAN settings can be made on this web page.

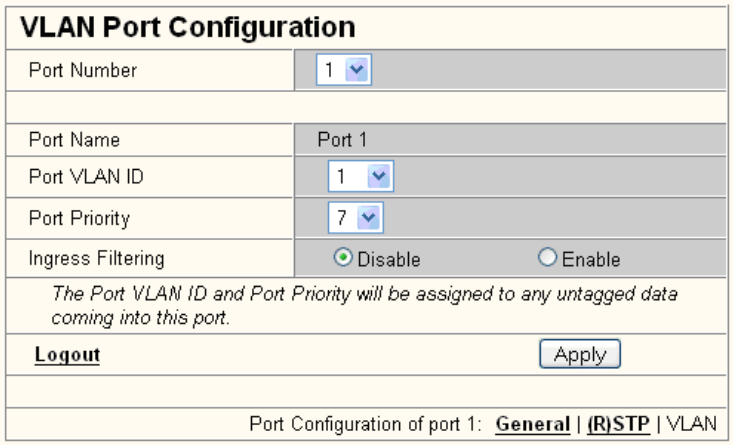


Figure 6-4 "VLAN Port Configuration" menu

If "Ingress Filtering" is set to "Enable", the switch rejects data packets received at this port if the port is not a "tagged member" or "untagged member" of the VLAN with the VLAN ID contained in the tag of the packet.

Port Priority

– A corresponding tag indicating the priority is added to packets without tags.

Port VLAN ID

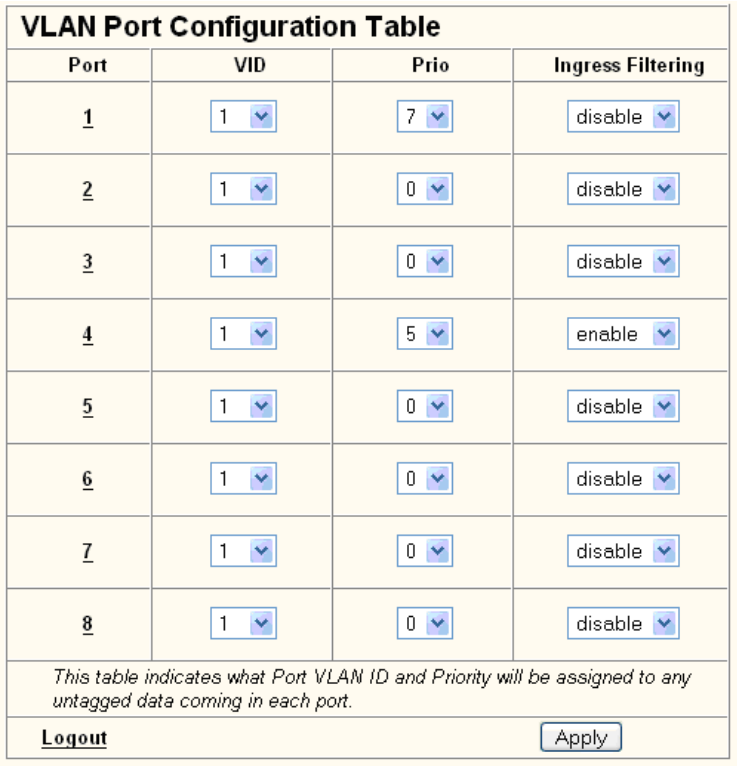
– Assignment of received, untagged packets to a VLAN. The corresponding VLAN ID must be set for the ports that are "untagged members" of a VLAN (see "Example: Communication between termination devices via VLAN" on page 6-8).

Only IDs of existing VLANs can be set as the port VLAN ID. If a VLAN is deleted, all port VLAN IDs that are set to this VLAN are reset to the default VLAN ID "1".

6.4.3 VLAN Port Configuration Table

This web page provides an overview of the main VLAN settings for the ports. Clicking on the relevant port number opens the "VLAN Port Configuration" web page, where the settings can be modified.

This table can be used to assign incoming packets to the created VLANs if the packets reach the port without VLAN tag.



VLAN Port Configuration Table

Port	VID	Prio	Ingress Filtering
1	1	7	disable
2	1	0	disable
3	1	0	disable
4	1	5	enable
5	1	0	disable
6	1	0	disable
7	1	0	disable
8	1	0	disable

This table indicates what Port VLAN ID and Priority will be assigned to any untagged data coming in each port.

Logout Apply

Figure 6-5 "VLAN Port Configuration Table" menu

6.5 Setting up static VLANs

Security recommendation: Instead of using VLAN 1 for management, it is recommended that a new separate VLAN is created for management. Make sure that the administrator has access to this VLAN.

Warnings displayed when setting up/configuring VLANs indicate configuration errors:

– An "untagged" port belongs to **multiple** VLANs.

The port assignment (untagged) and VID do **not** match.

In order to set up a VLAN, the switches involved must be configured accordingly. In the following example, data traffic is to be enabled in VLAN 5 between termination devices A and B.

The type of termination device must be taken into consideration: VLAN-compatible (processes tags) or not VLAN-compatible (does not process tags). In the example, two types of termination device are take into consideration.

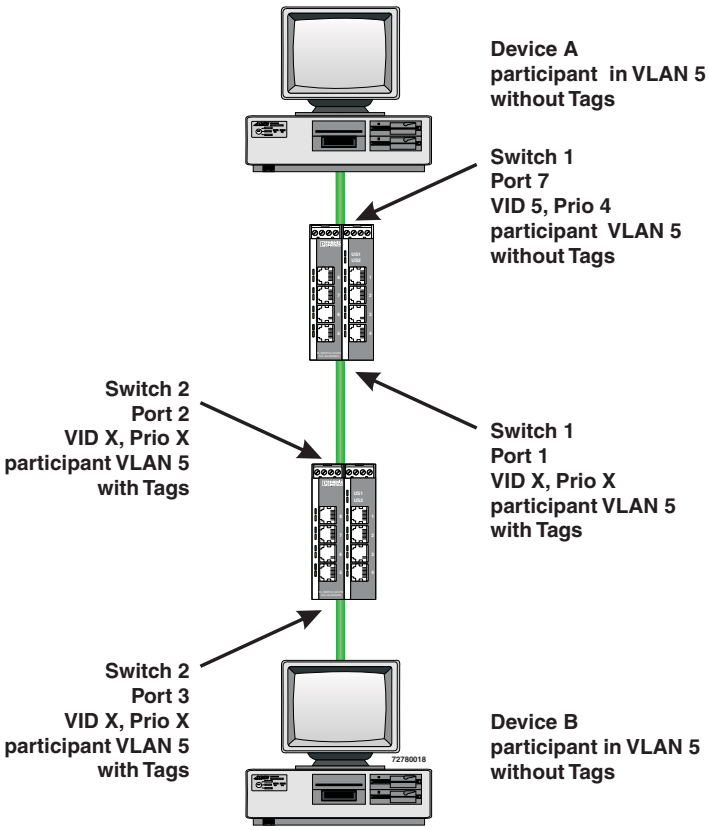


Figure 6-6 Example: Communication between termination devices via VLAN

Switch configuration

1 Set both switches to "VLAN Tagging" mode, save, and restart devices.
2 On switch 1, set up VLAN 5 and specify port 7 as an "untagged" member and port 1 as a "tagged" member.
3 For port 7 at switch 1, set the port VLAN ID to 5 and the port priority to any.
4 On switch 2, set up port 2 and port 3 as "tagged" members of VLAN 5.

Both termination devices now communicate via the network path shown in the example without other switch ports forwarding the broadcast packets for both termination devices, for example.

6.6 VLAN and (R)STP

When using (R)STP and VLAN simultaneously, please note the following:
– (R)STP is **not** based on VLANs
– (R)STP creates a loop-free topology in the form of a tree structure

In the event of static VLAN configuration, all possible redundant data paths must be taken into consideration in the configuration. All possible backbone ports of the network (not the termination device ports) must be inserted in all available VLANs as "tagged" members. This ensures that for every possible tree structure that can be generated by (R)STP, every VLAN can be accessed by every switch.

A typical configuration is illustrated in the following diagram:

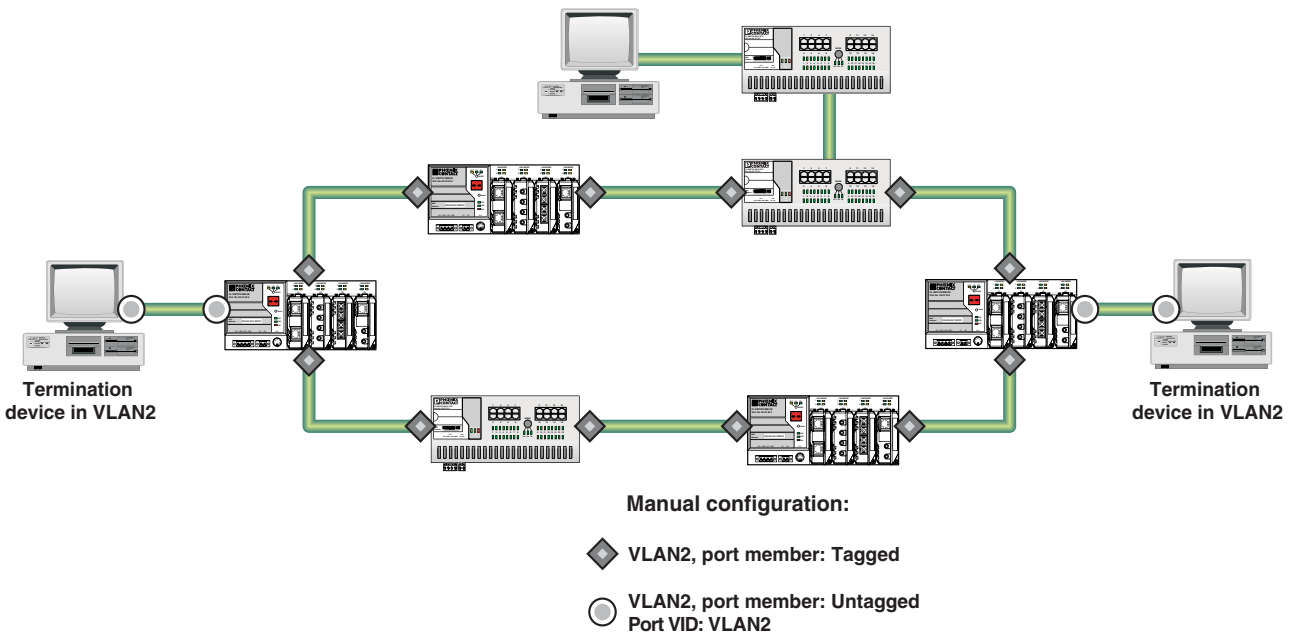


Figure 6-7 Typical configuration for VLAN and (R)STP

7 Technical data

General data	
Function	Lean Managed Ethernet/Fast Ethernet Switch; conforms to standard IEEE 802.3
Switch principle	Store-and-forward
PROFINET conformance	Class A
Data throughput with 100 Mbps full duplex	148,809 packets with 46 (64) byte packet size 8127 packets with 1500 (1518) byte packet size
Address table	For 1023 MAC addresses
SNMP	Version 1 and 2
Supported MIBs	SNMPv2 MIB, RSTP MIB, and private SNMP objects from Phoenix Contact
Housing dimensions (width x height x depth)	45 mm x 99 mm x 112 mm
Permissible operating temperature	-40°C to +70°C
Permissible storage temperature	-40°C to +85°C
Degree of protection	IP20, DIN 40050, IEC 60529
Protection class	Class 3 VDE 0106; IEC 60536
Maximum humidity (operation)	30% to 95%, non-condensing
Maximum humidity (storage/transport)	30% to 95%, non-condensing
Air pressure (operation)	86 kPa to 108 kPa, 1500 m above sea level
Air pressure (storage)	66 kPa to 108 kPa, 3500 m above sea level
Preferred mounting position	Perpendicular to a standard DIN rail
Connection to protective earth ground	Snapped onto a grounded DIN rail/via COMBICON (optional)
Weight	230 g, typical

Supply voltage	
Connection	Via COMBICON; maximum conductor cross section = 2.5 mm^2
Nominal value	24 V DC
Permissible ripple	3.6 V_{PP} within the permissible voltage range
Permissible voltage range	18.5 V DC to 30.5 V DC
Current consumption at U_S at nominal value	170 mA, typical; 250 mA, maximum
Test voltage	500 V DC for one minute
Protection against polarity reversal	Present
Power consumption	4 W, typical; 6 W, maximum

Interfaces	
Ethernet interfaces in RJ45 format	
Number	8 or 4
Connection format	8-pos. RJ45 female connector on the switch
Connection medium	Twisted pair cable with a conductor cross section of 0.14 mm^2 to 0.22 mm^2
Cable impedance	100 ohms
Transmission speed	10/100 Mbps
Ethernet interface (SC)	
Number	0 or 2
Connection format	SC duplex female connector on the switch
Wavelength	1300 nm
Laser protection	Class 1 according to DIN EN 60825-1:2001-11
Minimum transmission length, including 3 dB system reserve, when using **multi**-mode	6.4 km fiberglass with F-G 50/125 0.7 dB/km F1200 2.8 km fiberglass with F-G 50/125 1.6 dB/km F800 11 km fiberglass with F-G 62.5/125 0.7 dB/km F100 3.0 km fiberglass with F-G 62.5/125 2.6 dB/km F1000
Maximum **multi**-mode transmission power	-14 dBm
Minimum **multi**-mode transmission power	-20 dBm at 62.5/125 µm, -23.5 at 50/125 µm

Interfaces (continued)

Minimum **multi**-mode receiver sensitivity	-31 dBm
Multi-mode overrange	-14 dBm
Minimum transmission length, including 3 dB system reserve, when using **single**-mode	36 km fiberglass with F-G 9/125 0.36 dB/km 32 km fiberglass with F-G 9/125 0.4 dB/km 26 km fiberglass with F-G 9/125 0.5 dB/km
Maximum **single**-mode transmission power	-8 dBm
Minimum **single**-mode transmission power	-15 dBm
Minimum **single**-mode receiver sensitivity	-31 dBm
Single mode overrange	-7 dBm
Transmission speed	100 Mbps
RS-232 communication interface	
Number	1
Connection format	Mini-DIN female connector on the switch
Alarm contact	
Voltage	24 V DC
Current carrying capacity	100 mA, maximum

Mechanical tests

Shock test according to IEC 60068-2-27	Operation: 25g, 11 ms period, half-sine shock pulse Storage/transport: 50g, 11 ms period, half-sine shock pulse
Vibration resistance according to IEC 60068-2-6	Operation/storage/transport: 5g, 150 Hz, criterion 3
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 EN 55011:1998 + A1:1999 + A2:2002 (electromagnetic interference)	Class A (industrial applications)
Immunity to interference according to EN 61000-4-2 (IEC 1000-4-2) (ESD)	Requirements according to DIN EN 61000-6-2
Contact discharge:	Test intensity 2, criterion B
Air discharge:	Test intensity 3, criterion B
Indirect discharge:	Test intensity 2, criterion B
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 61000-4-4 (IEC 1000-4-4) (burst)	Requirements according to DIN EN 61000-6-2
Data cables:	Test intensity 2, criterion B
Power supply:	Test intensity 3, criterion B
Immunity to interference 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 B
Power supply:	Test intensity 1, criterion B
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

Differences between this version and previous versions

Rev. 00 - First version
Rev. 01: LM-E switches added and functions of current firmware added
Rev. 02: Extended to include functions for the current firmware
Rev. 03: New device versions added
Rev. 04: Firmware 3.x added
Rev. 05: Firmware 3.40 added

7.1 Ordering data

Products

Description	Order designation	Order No.	Pcs. / Pkt.
Lean Managed Switch with 5 RJ45 ports	FL SWITCH LM 5TX FL SWITCH LM 5TX-E	2989527 2989336	1 1
Lean Managed Switch with 8 RJ45 ports	FL SWITCH LM 8TX FL SWITCH LM 8TX-E	2832632 2891466	1 1
Lean Managed Switch with 4 RJ45 ports and two FX ports in SC-D format for **multi-mode** fibers	FL SWITCH LM 4TX/2FX FL SWITCH LM 4TX/2FX-E	2832658 2891660	1 1
Lean Managed Switch with 4 RJ45 ports and two FX ports in ST format for **multi-mode** fibers	FL SWITCH LM 4TX/2FX ST FL SWITCH LM 4TX/2FX ST	2989132 2989831	1
Lean Managed Switch with 4 RJ45 ports and two FX ports in SC-D format for **single-mode** fibers	FL SWITCH LM 4TX/2FX SM FL SWITCH LM 4TX/2FX SM-E	2891916 2891864	1 1
Lean Managed Switch with 4 RJ45 ports and two FX ports in ST format for **single-mode** fibers	FL SWITCH LM 4TX/2FX SM ST FL SWITCH LM 4TX/2FX SM ST-E	2989239 2989938	1
Lean Managed Switch with 4 RJ45 ports and one FX port in SC-D format for **multi-mode** fibers	FL SWITCH LM 4TX/1FX FL SWITCH LM 4TX/1FX-E	2989624 2989433	1
Lean Managed Switch with 4 RJ45 ports and one FX port in ST format for **multi-mode** fibers	FL SWITCH LM 4TX/1FX ST FL SWITCH LM 4TX/1FX ST-E	2989721 2989530	1
Lean Managed Switch with 4 RJ45 ports and one FX port in SC-D format for **single-mode** fibers	FL SWITCH LM 4TX/1FX SM FL SWITCH LM 4TX/1FX SM	2989828 2989637	1
Lean Managed Switch with 4 RJ45 ports and one FX port in ST format for **single-mode** fibers	FL SWITCH LM 4TX/1FX SM ST FL SWITCH LM 4TX/1FX SM ST-E	2989925 2989734	1

Accessories

Description	Order designation	Order No.	Pcs. / Pkt.
Configuration cable, for connecting the switch to a PC, RS-232	PRG CAB MINI DIN	2730611	1
Universal end clamp	E/NS 35 N	080088 6	1
Factory Manager startup/diagnostics software	FL SWT	2831044	1
Network monitoring with HMI/SCADA systems	FL SNMP OPC SERVER	2832166	1
Angled patch connector with two RJ45 CAT5e network connections	FL PF 2TX CAT5E	2891165	1
Angled patch connector with eight RJ45 CAT5e network connections	FL PF 8TX CAT5E	2891178	1
Angled patch connector with two RJ45 CAT6 network connections	FL PF 2TX CAT 6	2891068	1
Angled patch connector with eight RJ45 CAT6 network connections	FL PF 8TX CAT 6	2891071	1
Patch cable, CAT**6**, pre-assembled, 0.3 m long	FL CAT6 PATCH 0,3	2891181	10
Patch cable, CAT**6**, pre-assembled, 0.5 m long	FL CAT6 PATCH 0,5	2891288	10
Patch cable, CAT**6**, pre-assembled, 1.0 m long	FL CAT6 PATCH 1,0	2891385	10
Patch cable, CAT**6**, pre-assembled, 1.5 m long	FL CAT6 PATCH 1,5	2891482	10
Patch cable, CAT**6**, pre-assembled, 2.0 m long	FL CAT6 PATCH 2,0	2891589	10
Patch cable, CAT**6**, pre-assembled, 3.0 m long	FL CAT6 PATCH 3,0	2891686	10
Patch cable, CAT**6**, pre-assembled, 5.0 m long	FL CAT6 PATCH 5,0	2891783	10
Patch cable, CAT**6**, pre-assembled, 7.5 m long	FL CAT6 PATCH 7,5	2891880	10
Patch cable, CAT**6**, pre-assembled, 10 m long	FL CAT6 PATCH 10	2891887	10
Patch cable, CAT**6**, pre-assembled, 12.5 m long	FL CAT6 PATCH 12,5	2891369	5
Patch cable, CAT**6**, pre-assembled, 15 m long	FL CAT6 PATCH 15	2891372	5
Patch cable, CAT**6**, pre-assembled, 20 m long	FL CAT6 PATCH 20	2891576	5
Patch cable, CAT5, pre-assembled, 0.3 m long	FL CAT5 PATCH 0,3	2832250	10
Patch cable, CAT5, pre-assembled, 0.5 m long	FL CAT5 PATCH 0,5	2832263	10

Description (continued)	Order designation	Order No.	Pcs. / Pkt.
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

Phoenix Contact GmbH & Co. KG
Flachsmarktstr. 8
32825 Blomberg
Germany

+ 49 5235 - 3-00

+ 49 5235 - 3-41200

www.phoenixcontact.com

Worldwide locations:
www.phoenixcontact.com/salesnetwork

HOTLINE:

Should problems occur that cannot be resolved with the help of this documentation, please contact our hotline:

+ 49 5281 9-462888

factoryline-service@phoenixcontact.com