



User manual

UM EN FL SWITCH 30..., 40... and 48...

Managed industrial switch

User manual

Managed industrial switch

2016-09-12

Designation: UM EN FL SWITCH 30..., 40... and 48...

Revision: L

This user manual is valid for:

Designation	Version	Order No.
FL SWITCH 3005		2891030
FL SWITCH 3008		2891031
FL SWITCH 3005T		2891032
FL SWITCH 3008T		2891035
FL SWITCH 3004T-FX		2891033
FL SWITCH 3004T-FX ST		2891034
FL SWITCH 3006T-2FX		2891036
FL SWITCH 3006T-2FX SM		2891060
FL SWITCH 3006T-2FX ST		2891037
FL SWITCH 3012E-2FX		2891120
FL SWITCH 3012E-2FX SM		2891119
FL SWITCH 3016		2891058
FL SWITCH 3016T		2891059
FL SWITCH 4008T-2GT-4FX SM		2891061

Designation	Version	Order No.
FL SWITCH 4008T-2SFP		2891062
FL SWITCH 4012T-2GT-2FX		2891063
FL SWITCH 3012E-2SFX		2891067
FL SWITCH 3016E		2891066
FL SWITCH 4824E-4GC		2891072
FL SWITCH 4808E-16FX LC-4GC		2891073
FL SWITCH 4808E-16FX SM LC-4GC		2891074
FL SWITCH 4808E-16FX-4GC		2891079
FL SWITCH 4808E-16FX SM-4GC		2891080
FL SWITCH 4012T-2GT-2FX ST		2891161
FL SWITCH 4008T-2GT-3FX SM		2891160
FL SWITCH 4808E-16FX ST-4GC		2891085
FL SWITCH 4808E-16FX SM ST-4GC		2891086
FL SWITCH 4800E-24FX-4GC		2891102
FL SWITCH 4800E-24FX SM-4GC		2891104

Please observe the following notes

User group of this manual

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

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

Explanation of symbols used and signal words



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

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

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

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

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



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



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

How to contact us

Internet

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

phoenixcontact.com

Make sure you always use the latest documentation.

It can be downloaded at:

phoenixcontact.net/products

Subsidiaries

If there are any problems that cannot be solved using the documentation, please contact your Phoenix Contact subsidiary.

Subsidiary contact information is available at phoenixcontact.com.

Published by

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

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

tecdoc@phoenixcontact.com

Please observe the following notes

General terms and conditions of use for technical documentation

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

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

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

This manual, including all illustrations contained herein, is copyright protected. Any changes to the contents or the publication of extracts of this document is prohibited.

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

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

Table of contents

1	Overview.....	5
1.1	Models.....	6
1.2	Structure.....	8
1.2.1	FL SWITCH 3006T-2FX	8
1.2.2	16-port FL SWITCH 30... switches	9
1.2.3	14- and 16-port FL SWITCH 40... switches	11
1.2.4	FL SWITCH 4824E-4GC switch	13
1.2.5	FL SWITCH 4808E-16FX...4GC switch	14
1.3	Installation notes	15
2	Installation	17
2.1	Mounting	17
2.1.1	FL SWITCH 30... and FL SWITCH 40...	17
2.1.2	FL SWITCH 48...E...	18
2.2	Removal	20
2.3	Connections	20
2.3.1	Power (FL SWITCH 30... and FL SWITCH 40...)	21
2.3.2	Power (FL SWITCH 48...E...)	22
2.3.3	Alarm contacts	23
2.3.4	RS-232 (V.24) interface	23
2.3.5	Use of SFP slots (FL SWITCH 40... SFP and FL SWITCH 48...E...) ..	24
3	Initial setup.....	27
3.1	Web-based management	27
3.2	Simple Network Management Protocol (SNMP).....	28
3.2.1	Private MIBs	30
3.3	Management via RS-232 (V.24)	30
3.3.1	Login	30
3.4	Telnet interface functions	33
3.5	IP addressing.....	34
3.5.1	Valid IP parameters	34
3.5.2	Assigning IP addresses	34
3.5.3	Subnet masks	36
3.5.4	Application	37
3.5.5	Factory default settings	37
3.5.6	Assigning IP parameters	38
3.5.7	Log in using web-based management	41
3.5.8	Modifying existing IP parameters	42
3.6	Device information.....	45
3.7	System identification	46
3.8	Login session	47
3.9	Log out	47

3.10	Software update	48
3.10.1	Software update	48
3.11	SNTP configuration	49
3.11.1	Configuring SNTP	50
3.12	Changing the user password	51
4	User accounts and web management.....	53
4.1	Web access modes	53
4.1.1	Login	53
4.1.2	Login and user accounts	54
4.2	User account management	57
4.3	Configuration management	59
4.3.1	Saving the configuration	59
4.3.2	Configuration file transfer	60
5	Switch station functions	63
5.1	Services.....	63
5.2	Port configuration	64
5.2.1	Port configuration table	64
5.2.2	Individual port configuration	65
5.3	Management interfaces	66
5.3.1	Web server protocol	66
5.3.2	Activating SNMP	68
5.4	Security	70
5.4.1	Port security and IEEE 802.1x	70
5.4.2	RADIUS authentication (IEEE 802.1x)	71
5.4.3	802.1x configuration table	73
5.4.4	Configuring the RADIUS server	73
5.4.5	MAC-based security overview	75
5.4.6	MAC-based security per port	75
5.4.7	MAC-based security global discard	77
5.5	Diagnostics.....	78
5.5.1	Trap configuration	78
5.5.2	Querying port states	79
5.5.3	Using port statistics	80
5.5.4	Configuring port mirroring	81
5.5.5	Display	83
5.5.6	Configuring alarm contacts	84
5.5.7	Utilization	85
5.5.8	Event table	86
5.5.9	Displaying the MAC address table	87
5.5.10	Link layer discovery protocol	87
5.5.11	LLDP topology	90

5.6	Redundancy	92
5.6.1	Spanning tree general	93
5.6.2	Configuring RSTP	94
5.6.3	Spanning tree port table	95
5.6.4	Spanning tree port configuration table	96
5.6.5	STP port configuration	97
5.6.6	MST	99
5.6.7	MST Global Config	100
5.6.8	MST Config	101
5.6.9	MST Port Config	102
5.6.10	Extended ring redundancy	103
5.6.11	Path control	117
5.7	Quality of service	119
5.7.1	Configuring quality of service	119
5.7.2	Priority mapping	122
5.7.3	Differentiated services	123
5.7.4	Flow control	124
5.7.5	Storm control	125
5.7.6	Traffic shaping	126
5.8	Multicast control	127
5.8.1	Procedure for creating a multicast group	127
5.8.2	General multicast configuration	128
5.8.3	Static multicast groups	129
5.8.4	Dynamic multicast groups	132
5.8.5	“General Multicast Configuration” page	133
5.8.6	Current multicast groups	134
5.9	VLAN	135
5.9.1	VLAN ID management	137
5.9.2	General VLAN configuration	138
5.9.3	Port-based VLAN configuration	140
5.9.4	Current VLANs	141
5.9.5	Tagging-based VLANs: Static VLANs	141
5.9.6	Native VLAN configuration	145
5.9.7	Tagging-based VLANs: Dynamic GVRP configuration	147
5.9.8	VLAN and RSTP	147
5.10	Link aggregation	148
5.10.1	Configuring link aggregation	148
A	Technical appendix – MIB objects	151
A 1	SNMP MIB objects	151
B	Technical appendix	161
B 1	Ordering data	161
B 2	Technical data	163

C	Appendices.....	171
	C 1	List of figures 171
	C 2	List of tables 175
	C 3	Index..... 177

1 Overview

The FL SWITCH 30..., 40... and 48... managed switches provide scalable power for application flexibility and ease of use. The switches are industrially hardened and offer a complete range of 10/100 connections and IEEE functions.

The FL SWITCH 30... range consists of managed switches with up to 16 ports that provide maximum redundancy, message filtering and security functions with both wide and normal industrial temperature ranges. The large IEEE function set meets application and IT department requirements, while retaining the ease of use needed by supporting plant floor personnel. Versions with 10/100 TX and TX/Fiber port combinations are available.

The FL SWITCH 30...E... range consists of managed switches with up to 16 ports that provide maximum redundancy, message filtering and security functions with wide industrial temperature ranges and IEC 61850 extended electrical noise immunity.

The FL SWITCH 40... range consists of managed switches with up to 16 ports and various combinations of RJ45 and fiber optic connections. FL SWITCH 40... switches contain the same large IEEE function set as the FL SWITCH 30... switches. The unique mix of 1000 Mbps, 10/100 Mbps and fiber optic ports allows a wide range of distributed and supervisory applications.

The FL SWITCH 48...E... range consists of rack-mounted managed switches with up to 28 ports with different port formats:

- Switches with 24 TX ports with 4 SFP/TX combo ports (“combo – means, “combination port”, where the user may use one of two interfaces – either a copper RJ45 or fiber media module.
- Switches with eight TX RJ45 ports with 16 FX-MM or SM fiber optic ports as well as the 4 SFP/TX combo ports that provide maximum redundancy, message filtering and security functions with wide, industrial temperature ranges and IEC 61850-3/IEEE 1613 substation hardened extended electrical noise immunity. The switch is compatible with DNP3 protocol-based devices.

The unique web simplification approach allows users to choose from extensive redundancy, message filtering and security functions, while reducing overall system complexity. It allows maintenance personnel complete access to read diagnostic information without login requirements.

Maximum network availability is ensured through redundant power supply, rapid spanning tree (RST) and extended ring protocols. Browser-based configuration pages make configuration simple. For further simplification, unused configuration pages can be hidden from less experienced personnel, such as those on the plant floor.

1.1 Models

The FL SWITCH 30... switch is available with five or eight ports and fiber optic ports in either SC or ST format. The FL SWITCH 40... provides 10, 14 or 16 ports and SC or LC (SFP) fiber optic ports. Each switch has two 1000 Mbps uplink ports. The FL SWITCH 48...E... provides 28 ports with different port formats, such as RJ45, LC and SFP.

The available models are:

Table 1-1 Models

	No. of RJ45 ports: 10/100	No. of RJ45 ports: 10/100/1000	No. of fiber optic ports	No. of GC ports ¹
FL SWITCH 3005	5	-	-	
FL SWITCH 3005T	5	-	-	
FL SWITCH 3008	8	-	-	
FL SWITCH 3008T	8	-	-	
FL SWITCH 3016	16	-	-	
FL SWITCH 3016T	16	-	-	
FL SWITCH 3004T-FX	4	-	1 (SC, Multimode, 100 Mbps)	
FL SWITCH 3004T-FX ST	4	-	1 (ST, Multimode, 100 Mbps)	
FL SWITCH 3006T-2FX	6	-	2 (SC, Multimode, 100 Mbps)	
FL SWITCH 3006T-2FX ST	6	-	2 (ST, Multimode, 100 Mbps)	
FL SWITCH 3006T-2FX SM	6	-	2 (SC, Single mode, 100 Mbps)	
FL SWITCH 3012E-2SFX	12	-	2 (SFP slots - LC, 100 Mbps)	
FL SWITCH 3012E-2FX	12	-	2 (SC, Multimode, 100 Mbps)	
FL SWITCH 3012E-2FX SM	12	-	2 (SC, Single mode, 100 Mbps)	
FL SWITCH 3016E	16	-	-	
FL SWITCH 4008T-2SFP ³	8	-	2 (SFP slots - LC, 1000 Mbps)	
FL SWITCH 4012T-2GT-2FX	12	2	2 (SC, Multimode, 100 Mbps)	
FL SWITCH 4012T-2GT-2FX ST	12	2	2 (ST, Multimode, 100 Mbps)	
FL SWITCH 4008T-2GT-3FX SM	8	2	3 (SC, Single mode, 100 Mbps)	
FL SWITCH 4008T-2GT-4FX SM	8	2	4 (SC, Single mode, 100 Mbps)	

Table 1-1 Models

	No. of RJ45 ports: 10/100	No. of RJ45 ports: 10/100/1000	No. of fiber optic ports	No. of GC ports ¹
FL SWITCH 4824E-4GC ³	24			4
FL SWITCH 4808E-16FX LC-4GC ³	8		16 (LC, Multimode, 100 Mbps)	4
FL SWITCH 4808E-16FX SM LC-4GC ³	8		16 (LC, Single mode, 100 Mbps)	4
FL SWITCH 4808E-16FX LC-4GC ³	8		16 (SC, Multimode, 100 Mbps)	4
FL SWITCH 4808E-16FX LC-4GC ³	8		16 (SC, Single mode, 100 Mbps)	4
FL SWITCH 4808E-16FX ST-4GC ³	8		16 (ST, Multimode, 100 Mbps)	4
FL SWITCH 4808E-16FX SM ST-4GC ³	8		16 (ST, Single mode, 100 Mbps)	4
FL SWITCH 4800E-24FX-4GC ³			24 (SC, Multimode, 100 Mbps)	4
FL SWITCH 4800E-24FX SM-4GC ³			24 (SC, Single mode, 100 Mbps)	4

¹ GC ports are combination ports that allow connection through either RJ45 or fiber optic connection. The RJ45 ports connect at 10/100/1000 Mbps and the fiber optic ports connect at 1000 Mbps via an SFP module. The RJ45 and fiber optic connection for a single port cannot be used at the same time.

³ SFP slots accept only 1000 Mbps modules

1.2 Structure

1.2.1 FL SWITCH 3006T-2FX

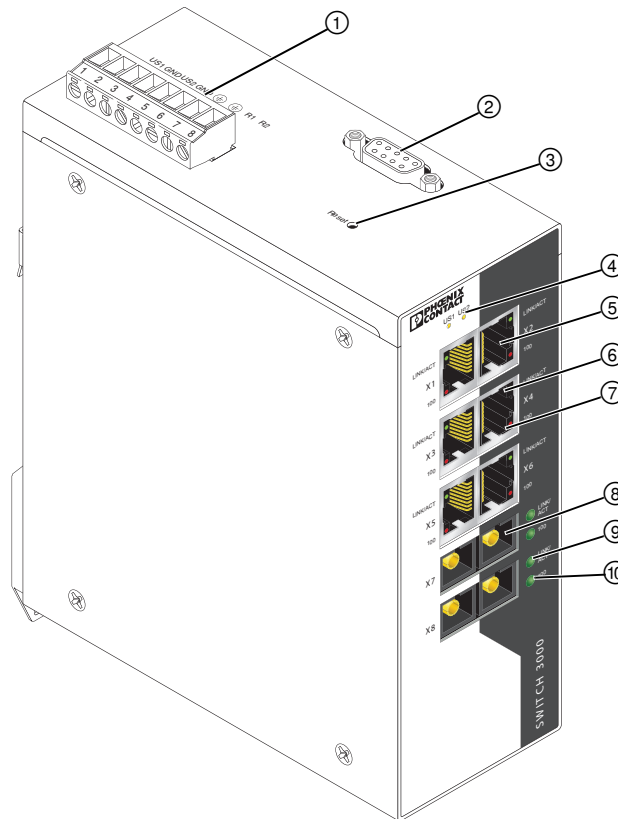


Figure 1-1 Structure of the FL SWITCH 3006T-2FX

Table 1-2 Structure of the FL SWITCH 3006T-2FX

1	Power supply/remote alarm connector	
2	RS-232 serial port (9-pos. D-SUB)	
3	Reset button	<p>Press and hold for less than 10 seconds to reboot with the saved configuration. The IP address is retained. Press and hold until all LEDs flash (approximately 30 seconds) to reboot using the factory defaults. The saved configuration and IP address will be lost.</p> <div style="border: 1px solid black; padding: 5px; display: inline-block;"> <p>i The reset button may be disabled for security purposes (see “Services” on page 63).</p> </div>
4	Power indicator LEDs (US1/US2)	Green indicates voltage supply is within range. Off indicates a voltage supply is below 18 V.

Table 1-2 Structure of the FL SWITCH 3006T-2FX (continued)

5	RJ45 ports	
6	RJ45 port LNK/ACT LED	Green indicates link is active. Off indicates link is not active. Flashing indicates data transfer.
7	RJ45 port 100 LED	Orange indicates 100 Mbps. Off indicates 10 Mbps.
8	Fiber optic port	
9	Fiber optic LNK/ACT LED	Green indicates link is active. Off indicates link is not active. Flashing indicates data transfer.
10	Fiber optic 100 LED	Orange indicates 100 Mbps. Off indicates link is not active.

1.2.2 16-port FL SWITCH 30... switches

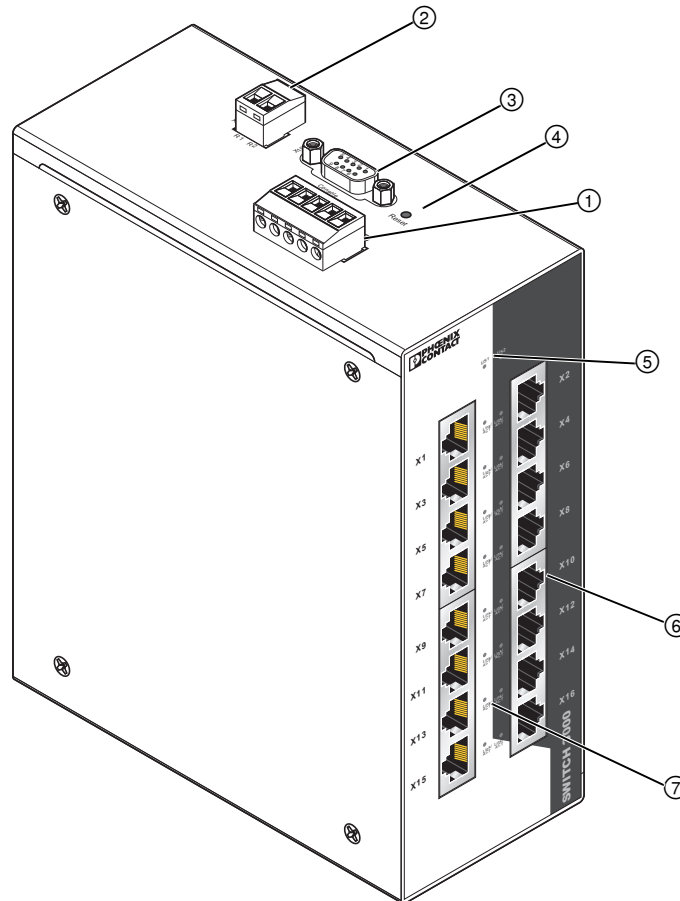



Figure 1-2 Structure of the FL SWITCH 3016

FL SWITCH 30..., 40... and 48...

Table 1-3 Structure of the FL SWITCH 3016

1	Power supply	
2	Remote alarm connector	
3	RS-232 serial port (9-pos. D-SUB)	
4	Reset button	<p>Press and hold for less than 10 seconds to reboot with the saved configuration. The IP address is retained. Press and hold until all LEDs flash (approximately 30 seconds) to reboot using the factory defaults. The saved configuration and IP address will be lost.</p> <div style="border: 1px solid black; padding: 5px;"> The reset button may be disabled for security purposes (see "Services" on page 63).</div>
5	Power indicator LEDs (US1/US2)	<p>Green indicates voltage supply is within range. Off indicates a voltage supply is below 18 V.</p>
6	RJ45 ports	
7	RJ45 port LED (LNK/ACT)	<p>Green indicates link is active. Off indicates link is not active. Flashing indicates data transfer.</p>

1.2.3 14- and 16-port FL SWITCH 40... switches

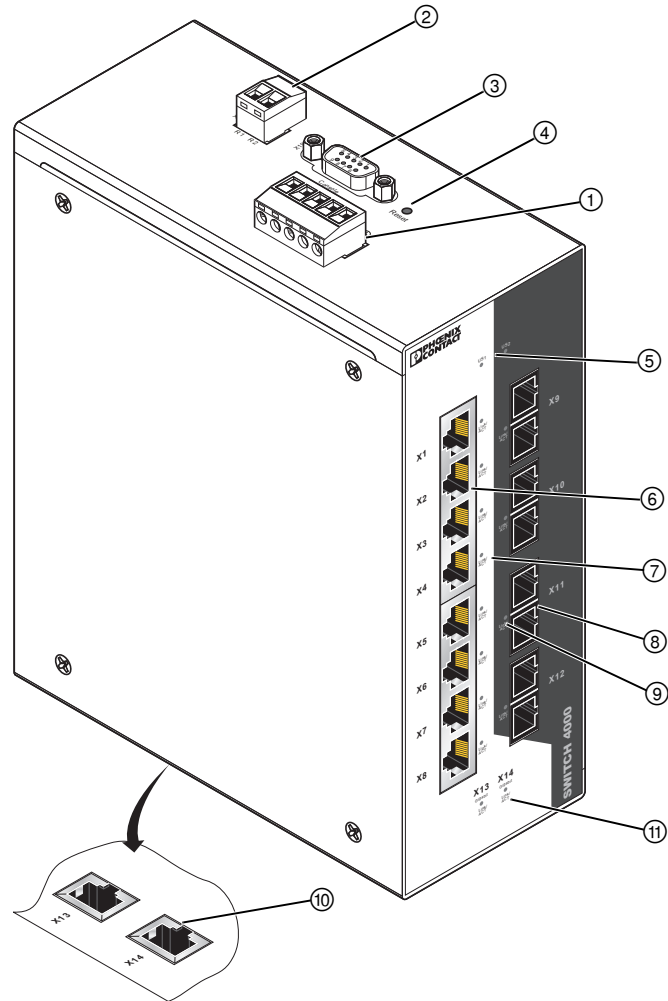



Figure 1-3 Structure of the FL SWITCH 4008T-2GT

FL SWITCH 30..., 40... and 48...

Table 1-4 Structure of the FL SWITCH 4008T-2GT

1	Power supply	
2	Remote alarm connector	
3	RS-232 serial port (9-pos. D-SUB)	
4	Reset button	<p>Press and hold for less than 10 seconds to reboot with the saved configuration. The IP address is retained.</p> <p>Press and hold until all LEDs flash (approximately 30 seconds) to reboot using the factory defaults. The saved configuration and IP address will be lost.</p> <div style="border: 1px solid black; padding: 5px; display: inline-block;">  <p>The reset button may be disabled for security purposes (see “Services” on page 63).</p> </div>
5	Power indicator LEDs (US1/US2)	<p>Green indicates voltage supply is within range.</p> <p>Off indicates a voltage supply is below 18 V.</p>
6	RJ45 ports	
7	RJ45 port LEDs (LNK/ACT)	<p>Green indicates link is active.</p> <p>Off indicates link is not active.</p> <p>Flashing indicates data transfer.</p>
8	Fiber optic ports	
9	Fiber optic LNK/ACT LED	<p>Green indicates link is active.</p> <p>Off indicates link is not active.</p> <p>Flashing indicates data transfer.</p>
10	RJ45 1000 Mbps ports	
11	RJ45 1000 Mbps port LEDs (LNK/ACT)	<p>Orange indicates 1000 Mbps.</p> <p>Off indicates link is not active.</p>

1.2.4 FL SWITCH 4824E-4GC switch

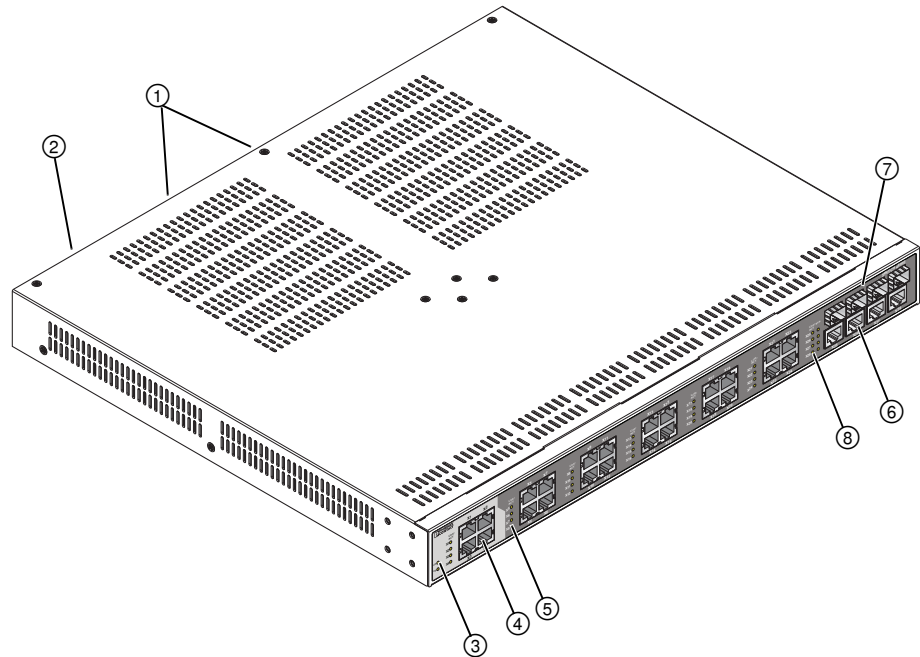


Figure 1-4 Structure of the FL SWITCH 4824E-4GC

Table 1-5 Structure of the FL SWITCH 4824E-4GC

1	Power supply slots	
2	RS-232 serial port (9-pos. D-SUB)	
3	Power indicator LEDs (US1/US2)	Green indicates voltage supply is within range. Off indicates a voltage supply is below 18 V.
4	RJ45 ports (10/100 Mbps)	
5	RJ45 port LEDs (LNK/ACT)	Green indicates link is active. Off indicates link is not active. Flashing indicates data transfer.
6	Gigabit combination ports - RJ45 connection	
7	Gigabit combination ports - Fiber optic connection (1000 Mbps)	
8	Gigabit combination port LEDs	Green indicates link is active. Off indicates link is not active. Flashing indicates data transfer.

1.2.5 FL SWITCH 4808E-16FX...4GC switch

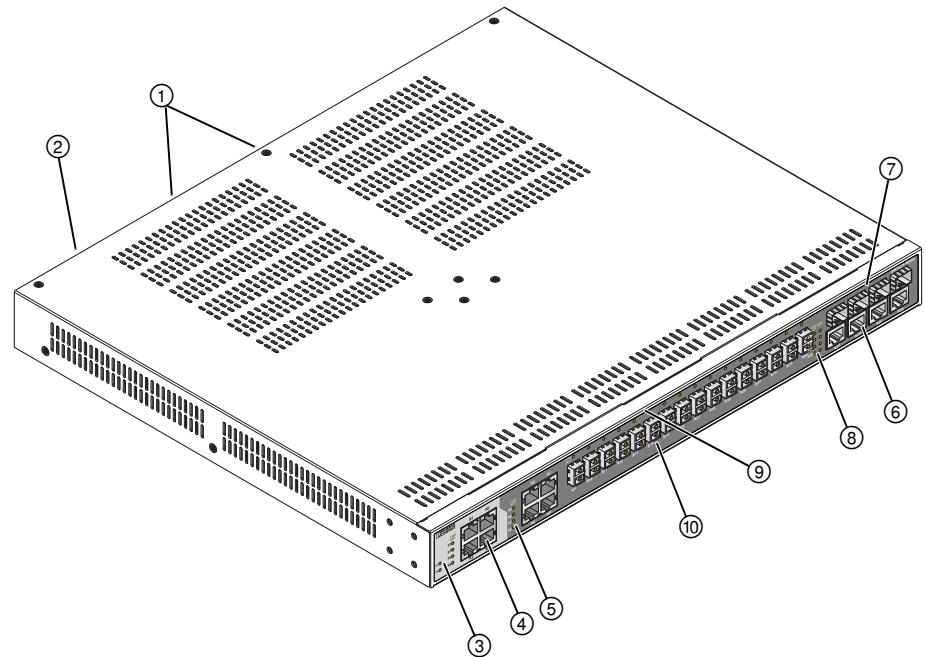


Figure 1-5 Structure of the FL SWITCH 4808E-16FX...4GC

Table 1-6 Structure of the FL SWITCH 4808E-16FX...4GC

1	Power supply slots	
2	RS-232 serial port (9-pos. D-SUB)	
3	Power indicator LEDs (US1/US2)	Green indicates voltage supply is within range. Off indicates a voltage supply is below 18 V.
4	RJ45 ports	
5	RJ45 port LEDs (LNK/ACT)	Green indicates link is active. Off indicates link is not active. Flashing indicates data transfer.
6	Gigabit combination ports - RJ45 connection	
7	Gigabit combination ports - Fiber optic connection	
8	Gigabit combination port LEDs	Green indicates link is active. Off indicates link is not active. Flashing indicates data transfer.
9	Fiber optic ports (100 Mbps)	
10	Fiber optic LNK/ACT LED	Green indicates link is active. Off indicates link is not active. Flashing indicates data transfer.

1.3 Installation notes

**WARNING:**

Do not look directly into the fiber optic ports when operational. The laser lightst can cause blindness or damage vision.

The user shall be responsible for ensuring the integrity of any protective conductor connections before carrying out any other actions. The protective earth connections should not be removed when the equipment is energized.

The user shall be responsible for checking equipment ratings, operating instructions, and installation instructions before commissioning or maintenance. It is the responsibility of the user to ensure that the equipment is installed, operated, and used for it's intended function in a manner specified by the manufacturer. Failure to do to this may impair safety protection mechanisms of the equipment.

The equipment conforms to pollution degree 2 when installed according to the normal position of use.

The FL SWITCH 4800E-P... power supplies contain factory-soldered (not user replaceable) fuses with the values: 400 V, 5 A, T (10 s).

2 Installation

2.1 Mounting

2.1.1 FL SWITCH 30... and FL SWITCH 40...

Mount the FL SWITCH 30... and FL SWITCH 40... on a clean DIN rail according to EN 50022. 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 placed on the left-hand side next to the switch to stop the module from slipping on the DIN rail. After the switch is mounted, install an end clamp on the right-hand side of the switch.

1. Place the module onto the DIN rail from above (1). The upper holding keyway must be hooked onto the top edge of the DIN rail. Push the module from the front toward the mounting surface (2).

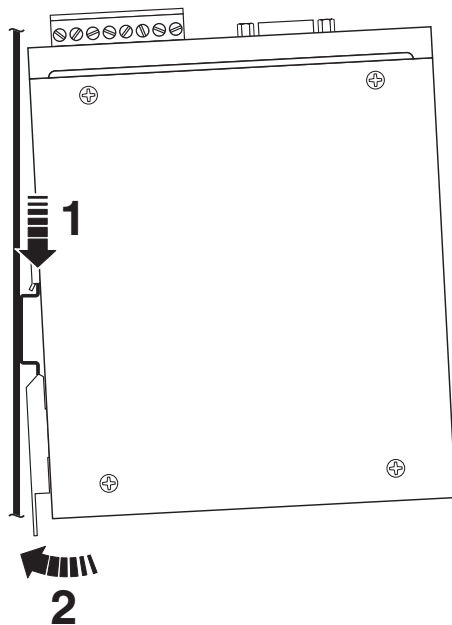


Figure 2-1 DIN rail installation

2. Once the module is snapped on properly, check that it is fixed securely on the DIN rail.
3. To prevent slipping along the DIN rail, install end clamps (E/NS 35N, Order No. 0800886) on each side of the module.

2.1.2 FL SWITCH 48...E...

The FL SWITCH 48...E... switch is for installation in a standard 19-inch rack. The optional FL RMB 4800E (Order No. 2891054) can be purchased separately for high-vibration and shock environments that require a more rugged installation.



It is recommended that 1U (rack unit) of space be kept free above each FL SWITCH 48...E... to allow additional air flow for heat dissipation. While not a requirement, the space will allow the switch to operate at a reduced temperature.



Because of tight spaces in most rack assemblies, connect the cord to the back of the switch before installing. See “Power (FL SWITCH 30... and FL SWITCH 40...)” on page 21 for additional information.

Standard mounting bracket installation

1. Attach the two mounting brackets (1) to the switch using the one M3 screw (2) and three M4 screws (3) provided.

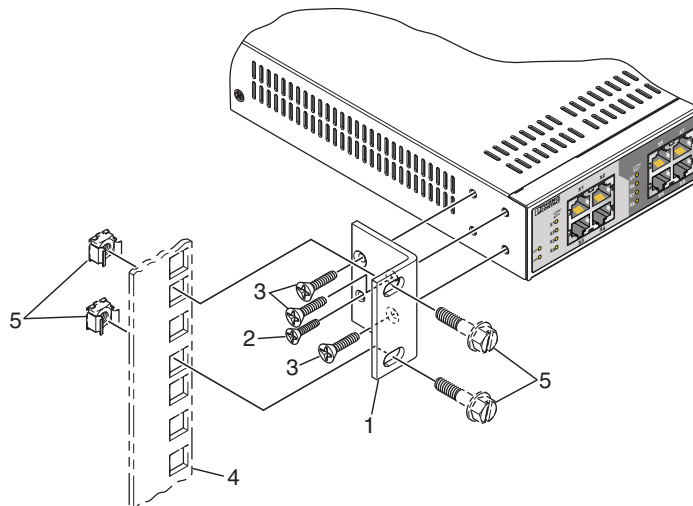


Figure 2-2 19-inch rack mounting with standard mounting brackets

2. Connect the user-supplied power cord into the rear of the switch.
3. Place the switch in the desired location on the rack (4). Use the rack hardware (5) to secure the switch in place on the rack.

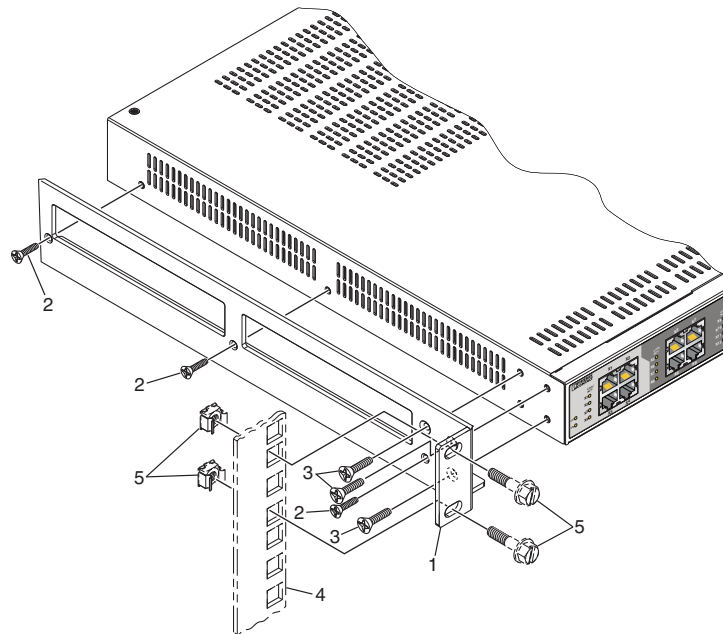
Optional FL RMB 4800E mounting bracket installation

Figure 2-3 19-inch rack mounting with optional FL RMB 4800E mounting brackets

1. Attach one mounting bracket (1) to the side of the switch using the three M3 screws (2) and three M4 screws (3) provided.
2. Repeat for the other side.
3. Place the switch in the desired location on the mounting rack (4). Use the mounting hardware (5) provided with the mounting rack to secure the switch.

2.2 Removal

1. Remove all plug-in connections.
2. Loosen and slide end clamps away from the switch.
3. Release the latch (1) using a suitable tool (screwdriver). Swivel the bottom of the module away from the DIN rail slightly (2). Next, lift the module upward away from the DIN rail (3).

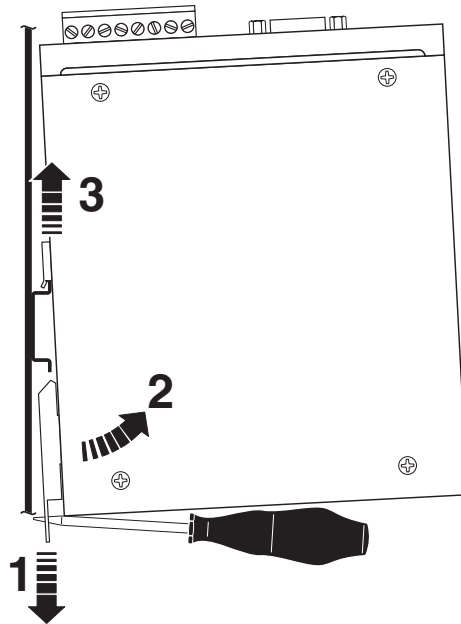


Figure 2-4 Removal from the DIN rail

2.3 Connections



NOTE:

For 24 V DC nominal power switches: 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.

The FL SWITCH 30..., 40... and 48... can be connected to a single power supply or two power supplies for redundancy.

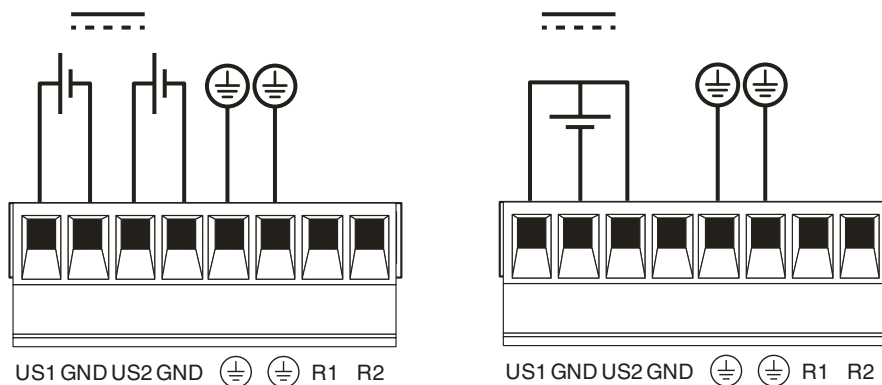


If redundant power supply monitoring is active (default setting), an error is indicated if only one voltage is applied. A bridge between US1 and US2 prevents this error message. However, it is also possible to deactivate monitoring using the browser-based management system.

2.3.1 Power (FL SWITCH 30... and FL SWITCH 40...)

Placing the switch onto a grounded rail connects it to the ground potential. In environments particularly prone to EMI, noise immunity can be increased through the additional ground connections on the power connector.

FL SWITCH 3005(T), FL SWITCH 3008(T), FL SWITCH 3004T-FX,
 FL SWITCH 3004T-FX ST, FL SWITCH 3006T-2FX, FL SWITCH 3006T-2FX ST,
 FL SWITCH 3006T-2FX SM, FL SWITCH 4008T-2SFP, FL SWITCH 3012E-2SFX, FL
 SWITCH 3012E-2FX, FL SWITCH 3012E-2FX SM,
 FL SWITCH 3016E



FL SWITCH 3016(T), FL SWITCH 4012-2GT-2FX, FL SWITCH 4008T-2GT-4FX SM,
 FL SWITCH 4012T-2GT-2FX ST, FL SWITCH 4008T-2GT-3FX SM

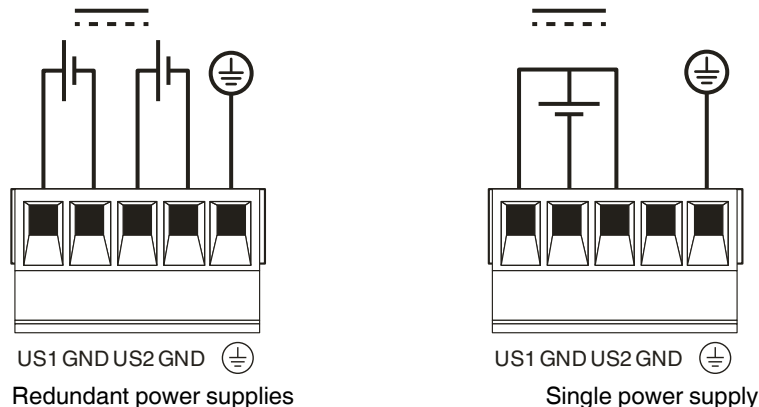


Figure 2-5 Power connections

2.3.2 Power (FL SWITCH 48...E...)

Two power modules are available for the FL SWITCH 48...E... switches: the FL SWITCH 4800E-P1 accepts 48 V DC nominal power; the FL SWITCH 4800E-P5 accepts 120/230 V AC/DC nominal power for the switch. Redundancy is provided by inserting two power modules into the switch and connecting a separate power source to each module.

If two power modules are installed, an algorithm in the FL SWITCH 48...E... determines from which module power is drawn based on available current to the module.



The US1 and US2 LEDs correspond to the two power module bays, not the primary and secondary.

There is no primary or secondary power supply differentiation for the FL SWITCH 48...E... units. Either power supply supports the full loading of the FL SWITCH 48...E... unit. The module with the higher power output automatically becomes the primary power supply for the switch unit.

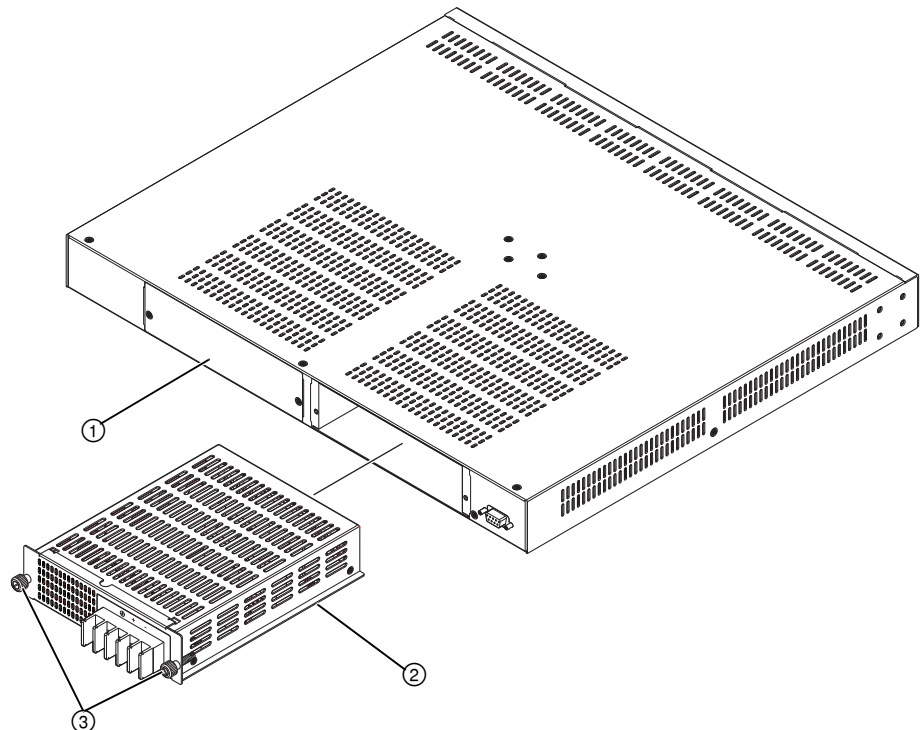


Figure 2-6 Power module installation

To install a power module:

1. Remove the cover (1) from the slot.
2. Align the module (2) with the slot and insert it straight into the switch.
3. Secure the power module using the two thumb screws.

4. Connect the user-supplied cable to the power module,

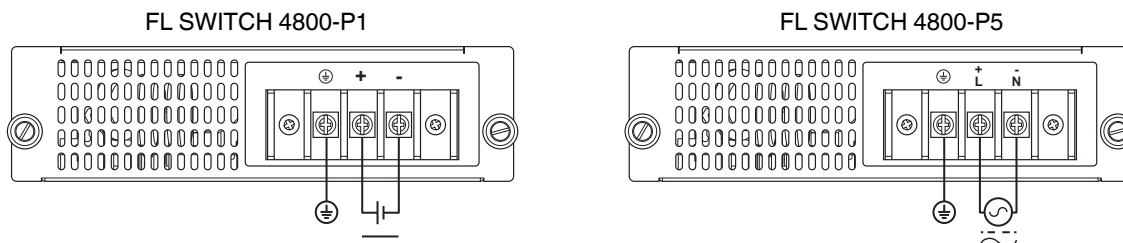


Figure 2-7 Power connections for FL SWITCH 48...E...

2.3.3 Alarm contacts

The FL SWITCH 30... and FL SWITCH 40... provides contacts R1 and R2 to connect to an external alarm in the event of a failure. If either power supply fails (<12 V) or a port fails (LNK), the internal dry contacts close.

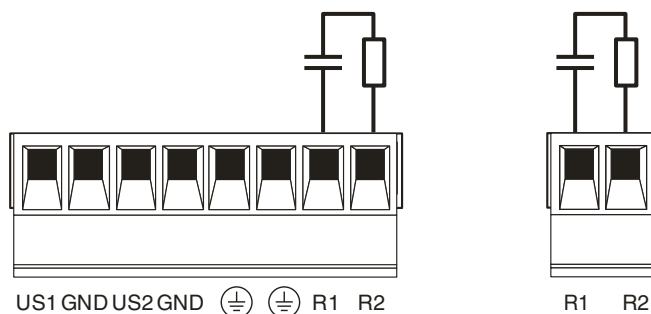


Figure 2-8 Alarm contact



The user is responsible to provide a suitable power source for the alarm contacts.



Alarm contacts are not available on the FL SWITCH 48...E... .

2.3.4 RS-232 (V.24) interface

Most configuration is accomplished through a browser by entering the IP address in the browser's address field. IP addressing and a limited set of configuration instructions are available through an RS-232 (V.24) interface.

The D-SUB 9 connector provides a serial interface to connect a local management station. It can be used to connect a VT100 terminal or a PC with corresponding terminal emulation to the management interface. The pinout for the connector is:

Table 2-1 D-SUB 9 connector pinout

Pin number	Function
2	Transmit (Tx)
3	Receive (Rx)
5	Ground (Gnd)

Set the following transmission parameters in the connected device:

Table 2-2 RS-232 parameters

Description	Value
Baud rate	115200 bps
Data bits	8
Parity	None
Stop bits	1
Flow control	None

2.3.5 Use of SFP slots (FL SWITCH 40... SFP and FL SWITCH 48...E...)

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

SFP modules are available separately as accessories (see “Ordering data” on page 161).

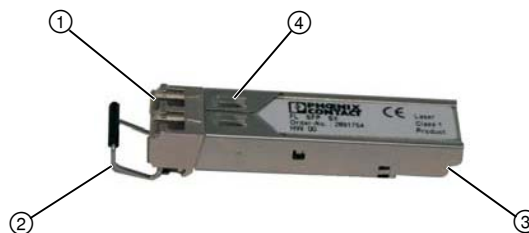


Figure 2-9 SFP module components

Be sure to select an SFP module with the same data rate as the switch (see Table 1-1 on page 6).

Installation

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

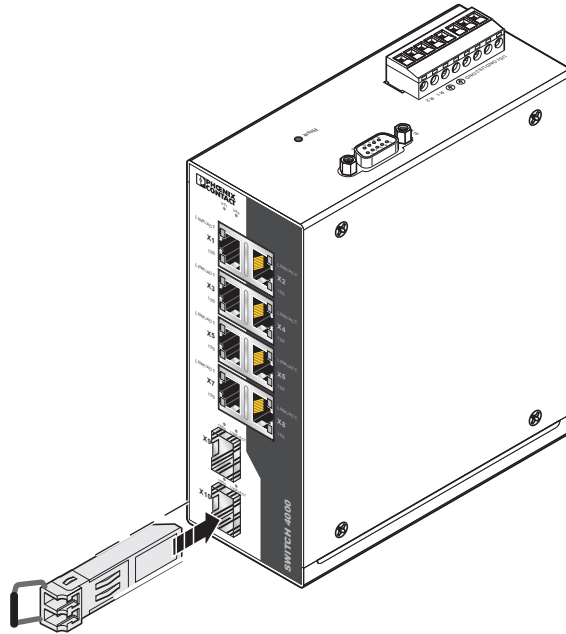


Figure 2-10 SFP module installation



Only use SFP modules listed as an accessory for the specific switch being installed (see "Ordering data" on page 161).

3 Initial setup

The FL SWITCH 30..., 40... and 48... has three methods for configuration: a web-based management (WBM) system that provides full access to all settings, an SNMP model that uses the IEFT MIB standard and a serial port connection (RS-232) that provides access to limited settings through a terminal emulation software, such as HyperTerminal®.



NOTE:

The boot-up process of the switch may take up to 60 seconds until the switch is ready.



NOTE:

The software update process may take up to six minutes for the file image to load and the reboot to complete. To use the software, you must reboot the switch. This can be done manually or automatically by selecting the “Update with Automatic Reboot” option (see “Software update” on page 48).



When using the “Submit” and “Apply” buttons to update the configuration (in the WBM only), please be aware that the changes are applied to the active configuration. The configuration must be saved in the internal memory with the configuration management menu (see “Configuration management” on page 59).



WBM can only be accessed using a valid IP address. Once the switch is reset to its default settings, it has no valid IP address and the addressing mechanism is set to BootP.

3.1 Web-based management

The user-friendly web-based management interface can be used to manage the switch from anywhere in the network using a standard browser. To do this, **http** or **https** can be used. This selection is made in the management interface (see “Web server protocol” on page 66). 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. Information about the device, the set parameters and the operating state can be viewed.



Modifications can only be made by entering a valid login. The default user name is **Admin**, and the password is **private**.



For security reasons, it is recommended that a new, unique password be selected.

3.2 Simple Network Management Protocol (SNMP)

SNMP is a manufacturer-neutral method for Ethernet management. It defines commands for reading and writing information, and defines formats for error and status messages.

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

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



The factory default password is **private** for all user interfaces except SNMPv3. Since the specification for SNMPv3 specifies a minimum password length of eight characters, the password is **privateadmin** for this user interface. SNMP V1/2 does not require passwords.



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



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

The agent of an FL SWITCH 30..., 40... and 48... manages Management Information Base II (MIB 2) according to RFC 1213, RMON MIB, Bridge MIB, If MIB, Etherlike MIB, Iana-address-family MIB, IANAifType MIB, SNMPv2 MIB, SNMP-FRAMEWORK MIB, P Bridge MIB, Q Bridge MIB, RSTP MIB, LLDP MIB, pnoRedundancy MIB, InetAddress and private SNMP objects from Phoenix Contact (FL-SWITCH-3000_V100-MIB.mib).

Phoenix Contact provides notification of ASN.1 SNMP objects (see www.phoenixcontact.com). Reading SNMP objects is not password-protected. However, a password is required for write access in SNMP. The factory default password for write access is **private** and can be changed by the user.

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

Table 3-1 Traps for the FL SWITCH 30..., 40... and 48...

Description	Trap	Definition	OID
Administrative password access	trapAdminPasswdAccess	Sent to the defined trap receivers on each modification of the device password. Contains information about the status of the last modification or attempted modification.	1.3.6.1.4.1.4346.11.11.3.0.14
SNMP authentication failure	authenticationFailure	Sent to the defined trap receivers when SNMP entity has received a protocol message that is not properly authenticated.	1.3.6.1.6.3.1.1.5.5
Firmware status changed	trapFWStatuschanged	Sent on each firmware-related modification. Contains additional information about the firmware status.	1.3.6.1.4.1.4346.11.11.3.0.15
Configuration saved	trapConfSaved	Sent each time the configuration is saved and informs the management station that the configuration has been saved successfully	1.3.6.1.4.1.4346.11.11.3.0.16
Power supply	trapPowerSupply	Every time the redundant has been lost, this trap sends out to the inform the management system about the event.	1.3.6.1.4.1.4346.11.11.3.0.4
(R)STP new root	newRoot	Sent each time the sending agent becomes the new root of the spanning tree. The trap is sent by a bridge soon after its election as the new root.	1.3.6.1.2.1.17.0.1
(R)STP topology changed	topologyChange	Sent each time by a bridge when any of its configured ports transitions from the learning state to the forwarding state, or from the forwarding state to the blocking state.	1.3.6.1.2.1.17.0.2
Cold start	coldStart	Sent each time the originator application is reinitialized to indicate the configuration may have been changed.	1.3.6.1.6.3.1.1.5.1
Link down	linkDown	Sent each time when the communication links enter the down state from some other state.	1.3.6.1.6.3.1.1.5.3
Link up	linkUp	Sent each time when the communication links leave the down state and transition into some other state.	1.3.6.1.6.3.1.1.5.4
Extended ring topology changed	trapExtRingFailure	Sent each time the ring fails.	1.3.6.1.4.1.4346.11.11.3.0.17
Trap manager connection	trapManagerConnection	Trap to test the connection between the SNMP agent and the network management station.	1.3.6.1.4.1.4346.11.11.3.0.99

3.2.1 Private MIBs

The private MIBs for the FL SWITCH 30..., 40... and 48... from Phoenix Contact can be found under object ID 1.3.6.1.4.1.4346. The 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)



The device-specific MIB files for FL SWITCH 30..., 40... and 48... switches can be downloaded from the device via the “Technical Data” page.

Download of MIBs can be initiated from the “Device Information/Technical Data” page. They are also listed in Section A, “Technical appendix – MIB objects”.

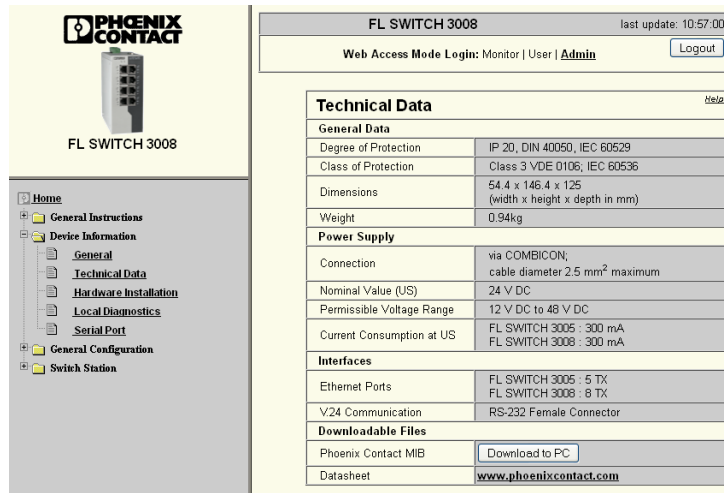


Figure 3-1 “Technical Data” page

3.3 Management via RS-232 (V.24)

Use of the RS-232 (V.24) connector is required for this section (see “RS-232 (V.24) interface” on page 23).

3.3.1 Login

The following procedure uses PuTTY terminal software, available for download at www.putty.org

Alternative terminal emulation software may be used.

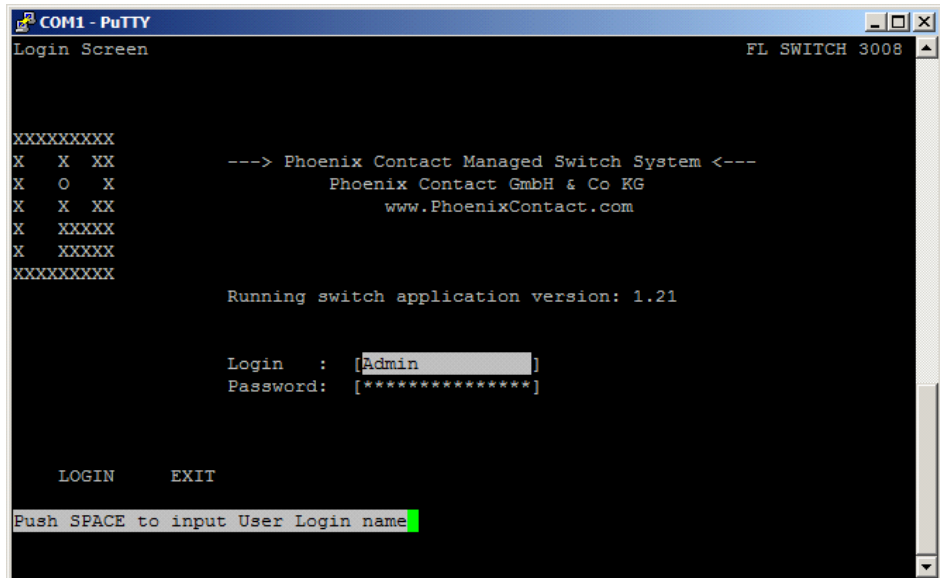


Figure 3-2 PuTTY login screen

1. Press the space key to place the cursor in the "Login" field.
Type **Admin** and press the <Enter> key.
2. Press enter to call the prompt "Push space to input User Password."

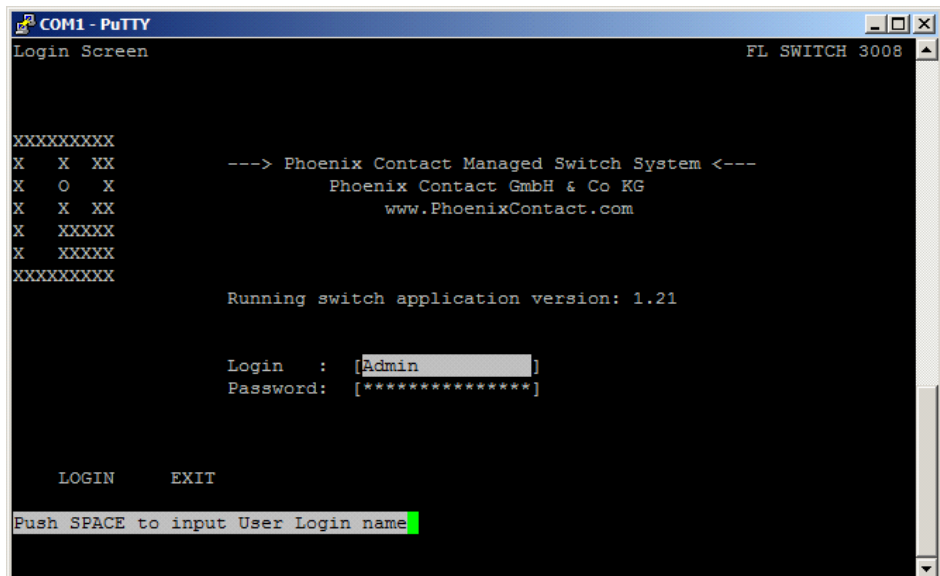


Figure 3-3 Prompt for user password

3. Press the space key. Type **private** and then press the <Enter> key.

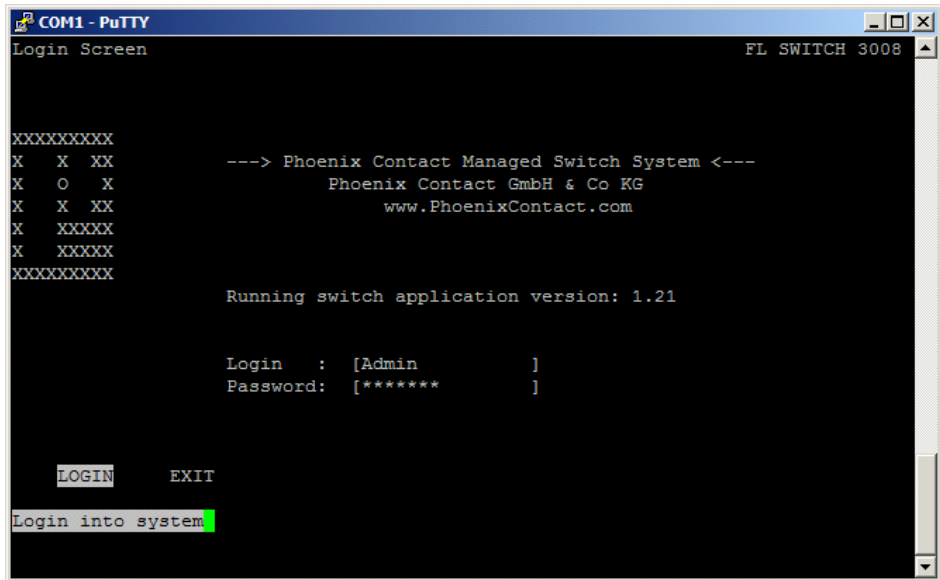


Figure 3-4 Login parameters entered in PuTTY

4. The prompt “Login into system” appears. Press the <Enter> key to execute login.

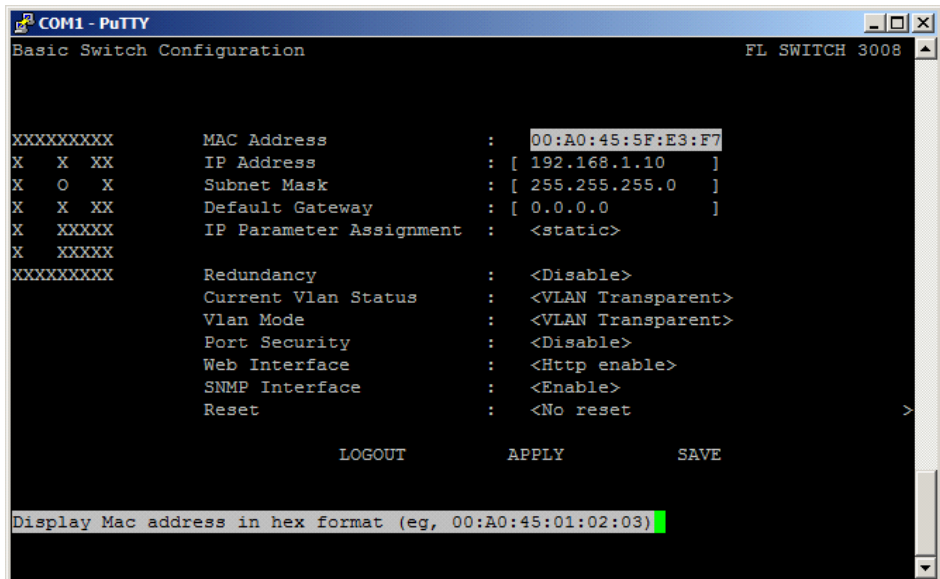


Figure 3-5 Switch configuration screen

3.4 Telnet interface functions

Telnet network protocol is used to establish a connection to a remote computer. This method is often used to retrieve a remote command line on the local computer, i.e., the outputs from the remote console are output on the local console, and the local key inputs are sent to the remote computer. The end result is the same as if sitting at the remote console.

Telnet can be activated/deactivated in the “General Configuration/Management Interfaces/Telnet” page.

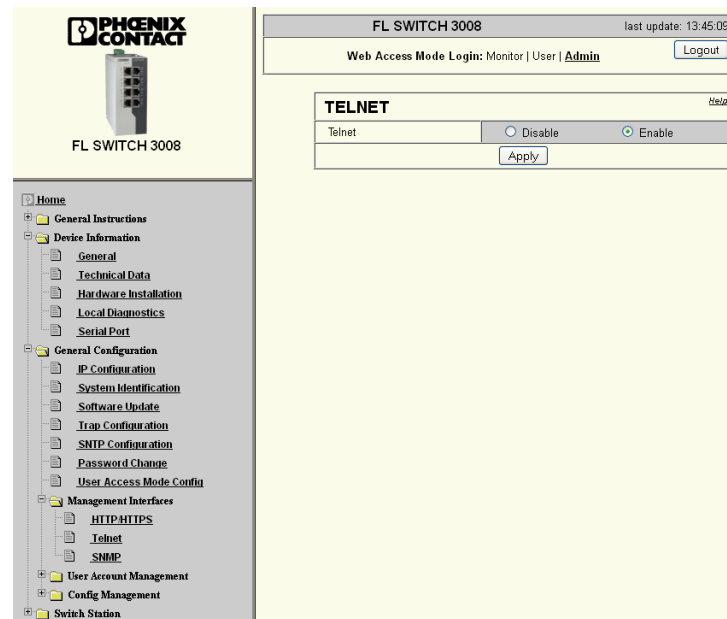


Figure 3-6 “Telnet” page

- **Telnet:** Click the appropriate radio button to “Enable” or “Disable” telnet access to this switch.
- **Apply:** Click the “Apply” button to save the settings to volatile memory (see “Configuration management” on page 59).

3.5 IP addressing

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, 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)
- Configuration via the DHCP protocol
- Static configuration via the management interfaces

3.5.1 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 address of the switch.

3.5.2 Assigning IP addresses

The IP address is a 32-bit address, which consists of a network part and a host 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 used for multicast and reserved, respectively.

Bit 1

Bit 32



Figure 3-7 Position of 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 following table. 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 is 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

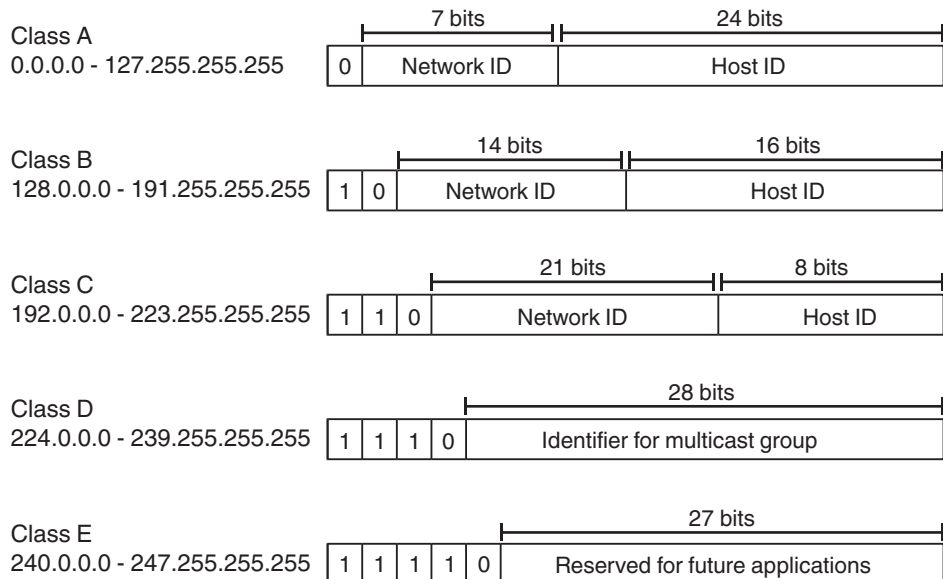


Figure 3-8 Structure of IP addresses

3.5.2.1 (X.X.X) 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.

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.

x.x.x.255 broadcast address

When 255 is entered as the last octet in an IP address, the message 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 this network). If the network is divided into subnetworks, the subnet masks must be observed during calculation; otherwise, some devices may be omitted.

0.x.x.x addresses

This range is only used by devices during initialization procedures. Value **0** is the ID of the specific network. If the IP address starts with a 0 (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.

3.5.3 Subnet masks

Routers and gateways divide large networks into several subnetworks. The IP addresses for individual devices are assigned to specific subnetworks by the subnet mask. 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: An IP address from Class A 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. ANDing the subnet mask and IP address gives the network prefix. Because the subnetwork is only recognized by local devices, the corresponding IP address appears as a "normal" IP address to all the other devices.

3.5.4 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	255.255.192.0	
Hexadecimal	1111 1111.1111 1111.1100 0000.0000 0000	
		Subnet mask bits
		Class B

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

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

IP address representation for device 2:

Hexadecimal	59.EA.55.32
Binary	1010 1001.1110 1010.0101 0101.0011 0010

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

3.5.5 Factory default settings

Except where specifically noted here, all other functions are disabled. This includes redundancy, performance, port mirroring, SNMP and security-related functions. By default or after the system is reset to the default settings, the following functions and properties are set:

- 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
 - 100 Mbps - full duplex
 - All counters of the SNMP agent are deleted
- The web and Telnet server, SNMP agent and RS-232 interface are active. The default baud rate for the RS-232 interface is 115,200 bps.
- Port security is deactivated for all ports.
- Port link monitoring is disabled.

- Access control for WBM is deactivated.
- The alarm contact link monitoring is disabled.
- The transmission of SNMP traps is deactivated, and the switch has no valid trap destination IP address.
- The MAC address aging time is set to 300 seconds.
- The WBM refresh interval is set to 30 seconds.
- Management is in VLAN 1.



The aging time is set using the “dot1dTpAgingTime” MIB object (OID 1.3.6.1.2.1.17.4.2). The available setting range is 10 - 10000 seconds. For static configuration, an aging time of 300 seconds is recommended.



Typically, settings are not automatically saved permanently. To permanently save the active configuration, click “Save ...” in the relevant user interface.

3.5.6 Assigning IP parameters

As long as the “BootP” setting has not been changed, when the supply voltage is switched on or the switch is reset, the switch sends requests (BootP requests) to assign IP parameters.



The “BootP” function is activated by default. If the switch has already been started up, the “BootP” function can be deactivated via the management.

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

Options for assigning IP parameters:

- Assignment using the IPAssign tool
- Configuration via the BootP protocol (default upon delivery)
- Static configuration via the management interfaces
- DHCP (Dynamic Host Configuration Protocol)



If DHCP is selected as the assignment mechanism, the DHCP server must offer a DHCP lease time of at least five minutes, so the switch accepts the assigned IP parameters.

3.5.6.1 Assigning IP parameters with IPAssign

IPAssign is a free tool that does not require installation, but can be used to assign IP parameters very easily using BootP. IPAssign can be found at

www.phoenixcontact.com.

1. Connect the switch to the PC and start IPAssign.



Figure 3-9 IPAssign splash screen

2. Click the “Next” button, and the tool then displays the devices that are sending BootP requests to assign an IP.

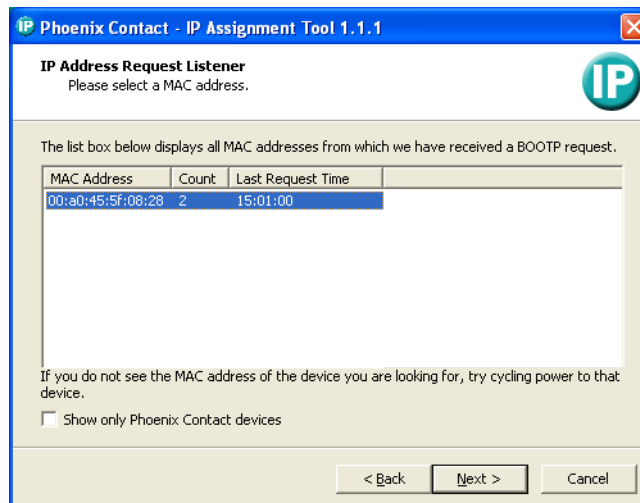


Figure 3-10 Devices sending BootP requests in IPAssign

3. Click the MAC address of the switch to be configured, and then click the “Next” button.

4. Enter the desired IP parameters in the appropriate fields. When finished, click the “Next” button.

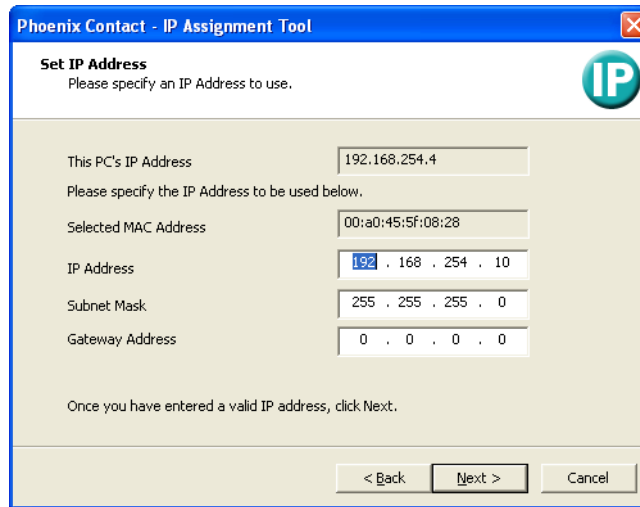


Figure 3-11 IP parameter settings

5. The window displays the new settings.



Figure 3-12 Completion screen

6. Click the “Finish” button to close the IPAssign tool.

3.5.6.2 Example for RS-232 (V.24) as a serial connection

Establish a communication connection as described in “Management via RS-232 (V.24)” on page 30.

Changing the IP address

1. Open the serial interface and log in. The default settings are:
User: **Admin**

Password: **private**

- Click the “IP Parameter Assignment” button and use the down arrow key to highlight the “IP Parameter Assignment” field. Change the selection to **Static**.

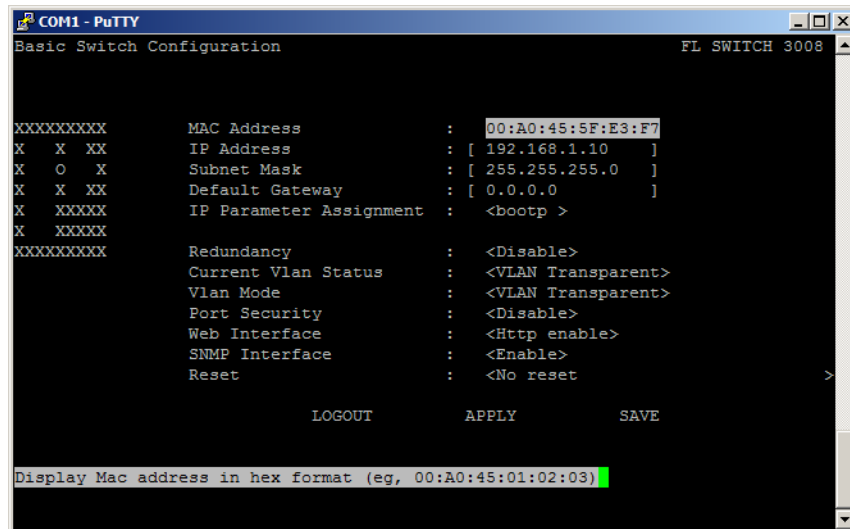


Figure 3-13 Static assignment of the IP via the serial interface

- Switch to “IP Address”, “Subnet Mask” or “Default Gateway” and make the desired settings.
- Switch to “APPLY” and confirm with ENTER; similarly switch first to “SAVE” and then to “LOGOUT”.

3.5.6.3 Assignment of IP parameters via DHCP

By default, it is not possible to assign IP parameters via DHCP. To activate these mechanisms, set the device to the desired operating mode via RS-232 (V.24) or WBM.

3.5.7 Log in using web-based management

The switch contains three web-based viewing modes (see “Web access modes” on page 53), which can be seen at the top of each web page. To make changes to the switch configuration or existing IP address:

- Open a web browser and enter the previously assigned IP address in the address field.
- Click the “Admin” or “User” field at the top of the page. With the factory default settings, the “User” mode provides access to most commonly used functions. The “Admin” mode provides access to all switch functions.

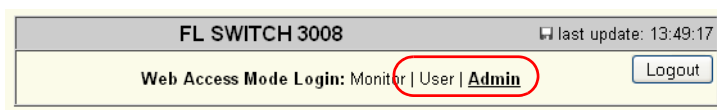


Figure 3-14 Web Access Mode selection

- A pop-up window requests confirmation to log in. Click the “Yes” button to continue to the login page.

4. Enter the User Name and Password.

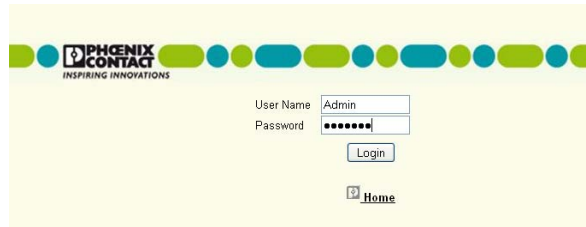


Figure 3-15 Sign-in Administrative page

If never accessed before, the factory default login settings are

- User Name: **Admin**
- Password: **private**



User names and passwords are case sensitive.

3.5.8 Modifying existing IP parameters

Requirements for the use of WBM

As the web server operates using the Hyper Text Transfer Protocol (http), a standard browser can be used. Access is via the URL address of the device.

Example: <http://172.16.116.100>

For full operation of the web pages, the browser must support JavaScript 1.2 and Cascading Style Sheets Level 1. Microsoft Internet Explorer 6.0 or higher is recommended.



WBM can only be called using a valid IP address. By default, the switch has no valid IP address. The "IPAssign.exe" tool (no installation required) can be used to assign the IP address. The IPAssign tool can be found at www.phoenixcontact.com.

Once all the necessary connections are established and the BootP server (IPAssign.exe) is running, start the FL SWITCH 30..., 40... and 48... switch or execute a reset. Following the boot phase, the switch sends the BootP requests that are received by the BootP server and displayed in the message window. If other devices are operating on 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.

3.5.8.1 Example for web-based management

In order to use web-based management, the switch must already have an IP address. This IP address may, for example, have been set via the serial connection or may have been assigned via the automatic BootP or DHCP mechanisms ("Assigning IP parameters with IPAssign" on page 38).

Changing the IP address

1. Open the web interface with a browser and the current IP address.
Example: <http://172.16.116.200>
2. Select the “General Configuration” page, and then click the “IP Configuration” button.
3. Under “Type of IP address assignment”, click the “Static assignment” button and enter the new IP address in the corresponding field.

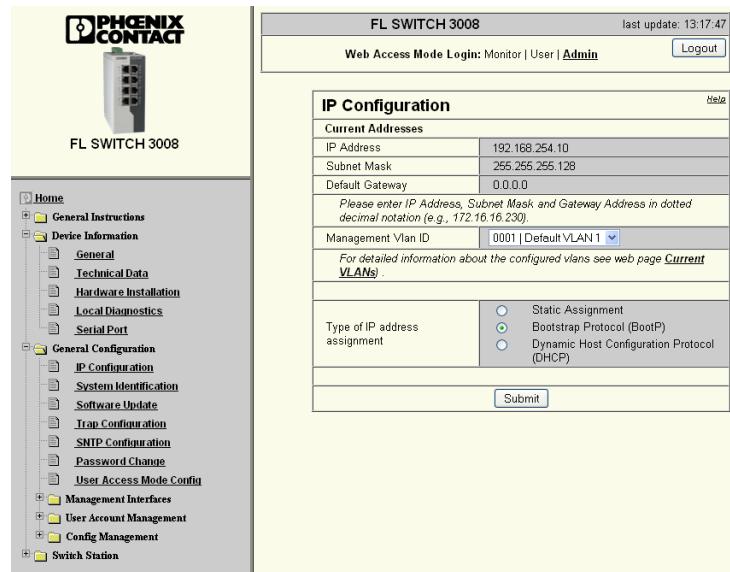


Figure 3-16 “IP Configuration” page in Administrator mode

4. Click the “Submit” button to apply the change.



Please note that, from the moment the modified IP address is activated, the switch can only be reached using the new address.

3.5.8.2 Changing IP parameters via SNMP

In order to use SNMP management, the switch must already have an IP address. This IP address may, for example, have been set via the serial connection or may have been assigned via the automatic BootP or DHCP mechanisms (see also “Assigning IP parameters with IPAssign” on page 38).

Changing the IP address

1. Open the OID (pIDevNetIfParamIpAddress) 1.3.6.1.4.1.4346.11.11.4.1.2 using a MIB browser, which is connected to the device via the current IP address.
2. Enter the desired IP and apply this using “Set”.

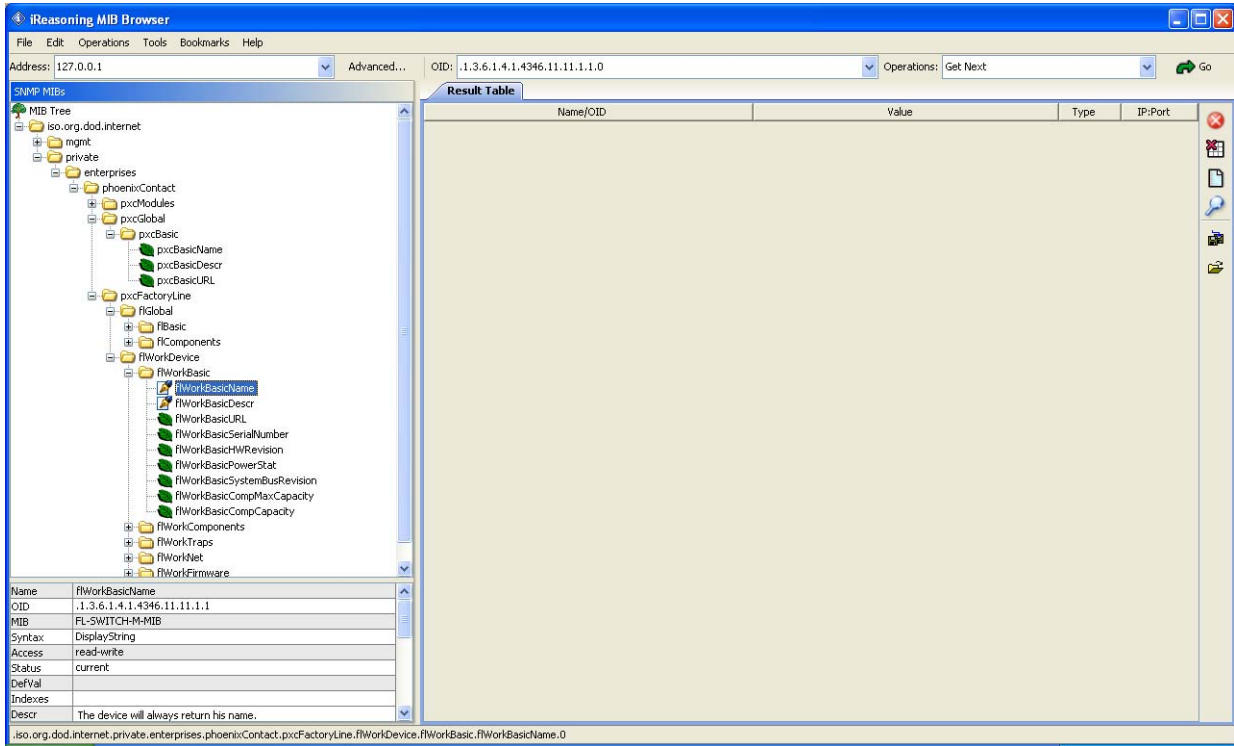
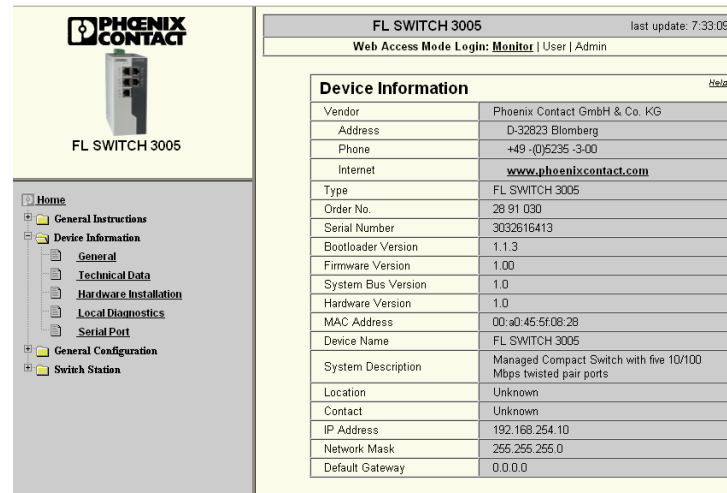


Figure 3-17 IP address assignment via SNMP

3.6 Device information

Information about the device can be viewed on the “Device Information/General” page.



The screenshot shows the Phoenix Contact web interface for the 'FL SWITCH 3005'. The page title is 'FL SWITCH 3005' and it shows the last update time as '7:33:09'. The user is logged in as 'Admin' in 'Monitor' mode. The navigation menu on the left includes: Home, General Instructions, Device Information (General, Technical Data, Hardware Installation, Local Diagnostics, Serial Port), General Configuration, and Switch Station. The main content area displays the 'Device Information' table.

Device Information	
Vendor	Phoenix Contact GmbH & Co. KG
Address	D-32823 Blomberg
Phone	+49 -(0)5236 -3-00
Internet	www.phoenixcontact.com
Type	FL SWITCH 3005
Order No.	28 91 030
Serial Number	3032616413
Bootloader Version	1.1.3
Firmware Version	1.00
System Bus Version	1.0
Hardware Version	1.0
MAC Address	00:a0:45:5f:08:28
Device Name	FL SWITCH 3005
System Description	Managed Compact Switch with five 10/100 Mbps twisted pair ports
Location	Unknown
Contact	Unknown
IP Address	192.168.254.10
Network Mask	255.255.255.0
Default Gateway	0.0.0.0

Figure 3-18 “Device Information” page

- **Vendor:** The vendor of this product.
- **Address:** The vendor’s address.
- **Phone:** The vendor’s telephone number.
- **Internet:** The official website of the vendor.
- **Type:** The product model.
- **Order No.:** The order number of this product.
- **Serial Number:** The serial number of this product.
- **Bootloader Version:** The bootloader version.
- **Firmware Version:** The currently installed firmware version.
- **System Bus Version:** The system bus version.
- **Hardware Version:** The hardware version of the device.
- **MAC Address:** The MAC address (configured in System Identification).
- **Device Name:** The user-assigned device name.
- **System Description:** The user-assigned system description.
- **Location:** The user-assigned physical location of this device.
- **Contact:** The user-assigned contact person responsible for this device (configured in IP Configuration).
- **IP Address:** The IP address assigned to this device.
- **Network Mask:** The subnet mask assigned to this device.
- **Default Gateway:** The default gateway assigned to this device.

3.7 System identification

System information, such as location, name, etc., can be entered to identify the switch. User-specific device data can be configured from the “General Configuration/System Identification” page.

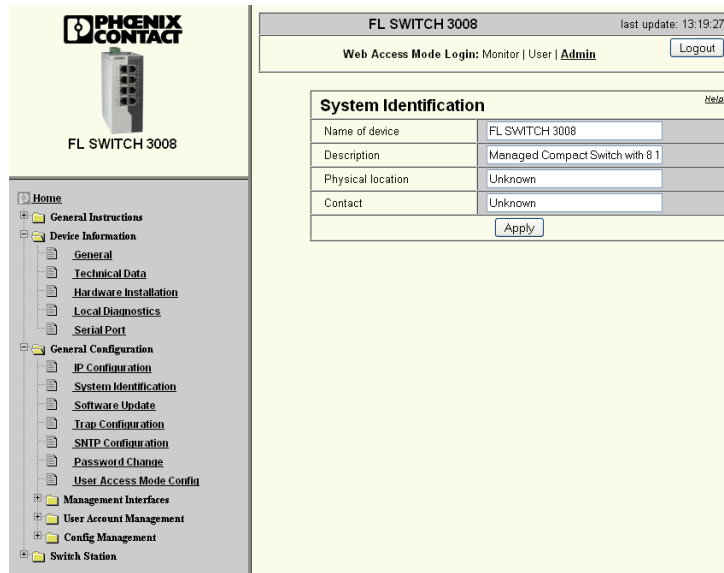


Figure 3-19 “System Identification” page

- **Name of device:** Enter a name for this device to easily identify it within the IP network. This field must be populated with a device name.
- **Description:** Enter a meaningful description of this device. This field may be left empty.
- **Physical location:** Enter the physical location of this device within the network infrastructure. This field may be left empty.
- **Contact:** Enter the contact information of the person responsible for this device. This field may be left empty.
- **Apply:** Click the “Apply” button to save the settings to volatile memory (see “Configuration management” on page 59).

3.8 Login session

The “Login Session” page displays a record of users and IP addresses currently logged into the switch.

The login session is viewed from the “General Configuration/User Account Management/Login Session” page.

The screenshot shows the web interface for a Phoenix Contact FL SWITCH 3008. The page title is "FL SWITCH 3008" with a "last update: 13:51:53" timestamp. Below the title, it says "Web Access Mode Login: Monitor | User | Admin" and includes a "Logout" button. The main content area is titled "Login Session" and contains a table with the following data:

ID	User Name	Connection From	Idle Time	Session Time	Session Type
0	Admin	149.208.49.47	00:00:00	00:37:55	HTTP

Below the table is a "Refresh" button. The left sidebar shows a navigation menu with categories like "General Instructions", "Device Information", "General Configuration", "Management Interfaces", "User Account Management", "Config Management", and "Switch Station".

Figure 3-20 “Login Session” page

There are no editable fields on the “Login Session” page.

3.9 Log out

A person logs out manually using the “Logout” button at the top of the page, or the session times out based on inactivity (see “Services” on page 63).

3.10 Software update

3.10.1 Software update

The software update function allows installation of updated firmware with new features as they are developed. New firmware, when released, is available as a free download at www.phoenixcontact.com

The “Software Update” page is used to view or modify the parameters for a software update and to trigger the update.

The screenshot shows the web interface for an FL SWITCH 3008. The top left features the Phoenix Contact logo and a navigation menu with categories like Home, Device Information, General Configuration, Management Interfaces, and Switch Station. The main content area is titled 'Software Update' and contains the following fields:

TFTP Server IP Address	TFTP:// 192.208.254.50
Downloadable File Name	FL_Switch_3000_V1_0.img
Kind of update	<input type="radio"/> Update without Reboot <input checked="" type="radio"/> Update with automatic Reboot
TFTP Update Status	No information available

Below the table, there is a note: "To start the new software the device must be rebooted. Note: The device reboots with the last stored configuration (save here before!)" and an "Apply" button.

Figure 3-21 “Software Update” page

- **TFTP Server IP Address:** Enter the IP address of the TFTP server. The factory default of the IPv4 address is **0.0.0.0**.
- **Downloadable File Name:** Enter the name of the file to be downloaded from the TFTP server. The factory default is blank.
- **Kind of update:** Click either the “Update without Reboot” or “Update with automatic reboot” radio button to select the desired reboot process.
- **TFTP update status:** The status of the software update is displayed during the file upload process.
- **Apply:** Click the “Apply” button to start the software update.

Procedure

1. Enter the IP address of the TFTP server from which the software upload will be requested.
2. In the “Downloadable File Name” field, enter the file name of the update. If the configuration has not been saved, save it now by clicking the “Save here before” link.
3. Click the “Apply” button to begin the process.

The update process can take up to six minutes for the file image to load and the reboot to complete. To use the software, you must reboot the switch. This can be done manually or automatically by selecting the “Update with automatic Reboot” option.

Following reboot, the switch operates with the new firmware.



A reboot is not carried out automatically following a firmware update unless the “Update with automatic Reboot” radio button is selected.



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

3.11 SNTP configuration

The Simple Network Time Protocol (SNTP) is defined in RFC 4330 (SNTP clients in automation technology) and is used to synchronize the internal system time with any NTP server, which represents the “timer”, i.e., the universal time. The aim is to synchronize all the components in a network with the universal time and thus to create a uniform time base.

Time synchronization provides valuable assistance when evaluating error and event logs, as the use of time synchronization in various network components enables events to be assigned and analyzed more easily.

Time synchronization is carried out at fixed synchronization intervals known as polling intervals. The client receives a correction time by means of an SNTP server, with the packet runtime for messages between the client and server being integrated in the time calculation in the client. The local system time of the client is thus constantly corrected. Synchronization in the NTP is carried out in Universal Time Coordinated (UTC) format.

The current system time is displayed as Universal Time Coordinates (UTCs). This means that the displayed system time corresponds to Greenwich Mean Time. The system time and the “UTC Offset” provide the current local time.

For switches with firmware revision 1.31 and above, the SNTP function allows one switch to function as the primary SNTP server and, optionally, one switch as the backup SNTP server. These two switches connect to an external master clock and all other switches in the system will reference these two switches. This approach reduces external clock connections, simplifying the network.

To allow one or more switches to function as an SNTP server, the following guidelines must be followed:

- All switches using the SNTP must have the SNTP client operating mode set to **Unicast mode**.
- One switch in the network must have a connection to an external SNTP server clock.
- All other switches on the network will have this switch’s IP address in the “Primary Server IP Address” field and, if used, the backup switch’s IP address in the “BackUp Server IP Address” field.

3.11.1 Configuring SNTP

The use of SNTP can be configured on the “General Configuration/SNTP Configuration” page.

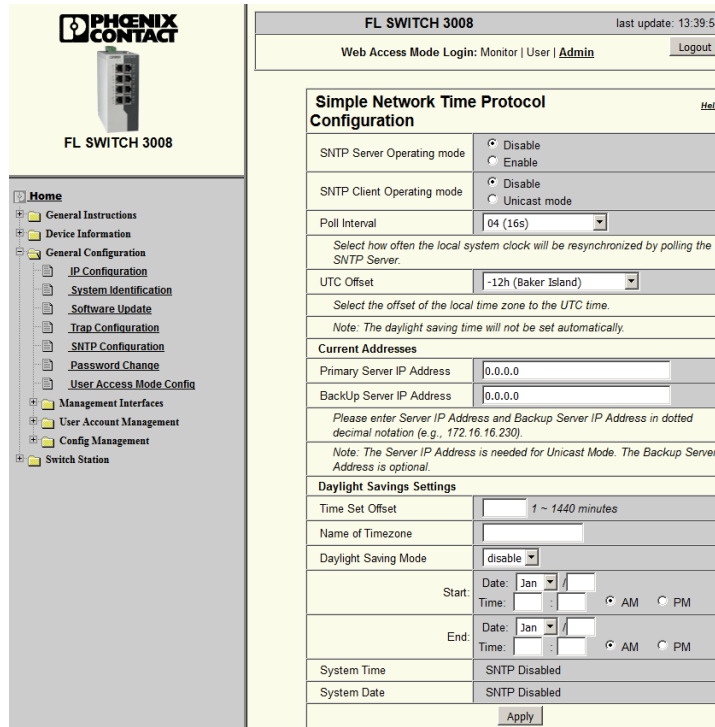


Figure 3-22 “Simple network time protocol configuration” page



Make sure the system time from the server corresponds to Greenwich Mean Time (GMT). The current local time is calculated based on the system time and the “UTC Offset”.

Configuration sequence

- **SNTP Server Operating mode:** Select either:
 - **Enable:** Enables the SNTP server function in the switch.
 - **Disable:** Disables the SNTP server function in the switch.
- **SNTP Client Operating mode:** Select either:
 - **Unicast Mode:** The client receives its time from a fixed primary server.
 - **Disable:** The switch does not receive time from an SNTP server.
- **Poll Interval:** Sets how often the SNTP client (the FL SWITCH 30..., 40... and 48... switch) will poll the SNTP server for the time.
- **UTC Offset:** Sets the time offset from GMT. Select the desired region from the drop-down menu.
- **Primary Server IP Address:** Enter the IP address of the primary SNTP server to synchronize with.
- **Backup Server IP Address:** Enter the IP address of a backup SNTP server to synchronize with in the event of a communication failure with the primary server.

- **Time Set Offset:** Enter the difference in time, in minutes, if a daylight savings period is used.
- **Name of Timezone:** Enter a name for the time zone. This must be at least three characters.
- **Daylight Savings Mode:** Select enable or disable from the drop-down menu.
- **Start:** Enter the start date and time of daylight savings mode.
- **End:** Enter the end date and time of daylight savings mode.
- **System Time:** Displays the current system time from the SNTP server.
- **System Date:** Displays the current system date from the SNTP server.
- **Apply:** Click the “Apply” button to save the SNTP parameters to the device’s active configuration.

3.12 Changing the user password

The FL SWITCH 30..., 40... and 48... switch offers comprehensive security features, such as password protection, HTTPS, Telnet, various user access options and port security features.

To modify parameters, log into the FL SWITCH 30..., 40... and 48... switch via login access (see “Login session” on page 47).



After successfully logging in for the first time, it is recommended that the password be changed.

The current passwords can be changed and activated on the “General Configuration/Change Password” page.

The screenshot displays the web interface for an FL SWITCH 3008. At the top, it shows the device name and a 'Logout' button. Below this is the 'Change Password' section, which includes a form with four input fields: 'Enter username', 'Enter old password', 'Enter new password', and 'Retype new password'. A note below the form specifies password requirements and security: 'The password must be between 7 and 12 characters long. NOTE: The password will be sent unencrypted over the network!'. An 'Apply' button is located at the bottom of the form. On the left side, a navigation menu is visible, with 'Password Change' highlighted under the 'General Configuration' section.

Figure 3-23 “Change Password” page

- **Enter username:** The username must be entered in the “Enter username” field.
- **Enter old password:** The old password is required for authorization purposes.

FL SWITCH 30..., 40... and 48...

- **Enter new password:** Enter the new password. This must be between 7 and 12 characters long.
- **Retype new password:** Retype the new password to ensure accuracy.
- **Apply:** Click the “Apply” button to save the new password for this user.

4 User accounts and web management

Various user roles can be created on the FL SWITCH 30..., 40... and 48.... While an administrator has access to all functions, user access can be customized on a page basis.

4.1 Web access modes

The FL SWITCH 30..., 40... and 48... managed switches have three modes that are used to access the switch setup parameters and diagnostics. These modes simplify the use of the switch based on who the user is and why they are accessing the switch. In each mode, the web pages of the switch are optimized for the intended purpose.

Monitor mode

“Monitor” mode provides quick and easy access to the switch’s diagnostic pages (all other setup pages are removed). It provides read-only access, and no login is required. It is intended for ongoing maintenance and network monitoring.

Admin mode

“Admin” mode is intended for the initial selection of functions to be used in the application and for adding functions as the network grows. All functions in the switch are accessible. In this respect, it is like a library that contains all the switch functions. Access is typically by senior control engineers or network administrators. A username and password login are required.

User mode

“User” mode is for day-to-day use of the switch, especially in start-up situations. The pages that are viewed can be customized to each user, making available only pages that are applicable to that user. The customization of the user mode interface is defined on the “User Access Mode Config” page while in “Admin” mode (see “User account management” on page 57). A user name and password login are required.

4.1.1 Login

At the top of each page is a link to the different access modes. The selected mode is displayed in bold and underlined text. Once logged into a “User” or “Admin” mode, you can select “lower” modes without logging in again. Simply click on the desired mode. This allows one to log into “Admin” mode, choose the pages to be viewed and then go to “User” mode

with its simplified web interface to start up the network and make further adjustments. Another example is to log in to “User” mode to make several switch parameter changes, and then go to “Monitor” mode for a simplified view of how the network is running.

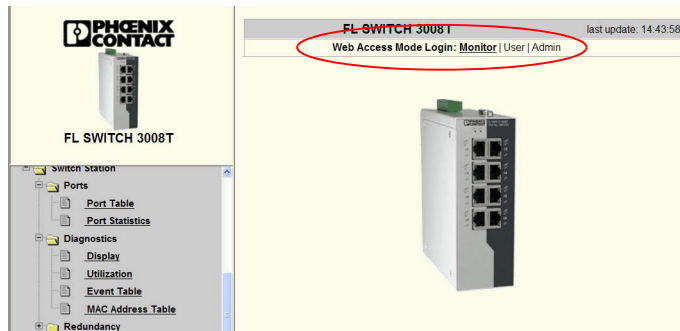


Figure 4-1 Mode display

4.1.2 Login and user accounts

The main purpose of user accounts is to provide security by controlling who has access to the switch functions and who is allowed to change parameters or only view them. In the case of the FL SWITCH 30..., 40... and 48... switches, it also allows added ease of use. The “User” mode pages can be customized to groups of people or even customized down to individual people.

The default login user name and password, as shipped from the factory, are:

- User Name: **Admin**
- Password: **private**



User names and passwords are case sensitive.

The factory default login provides access to all pages and functions of the switch in “Admin” mode. To access the switch in either “User” or “Admin” modes, a login with user name and password must be entered. “Monitor” mode only requires the IP address and provides view-only access.

Account setup procedure

1. Log in to the switch (see “Log in using web-based management” on page 41). If this is the initial access to the switch, use the factory default user name and password.

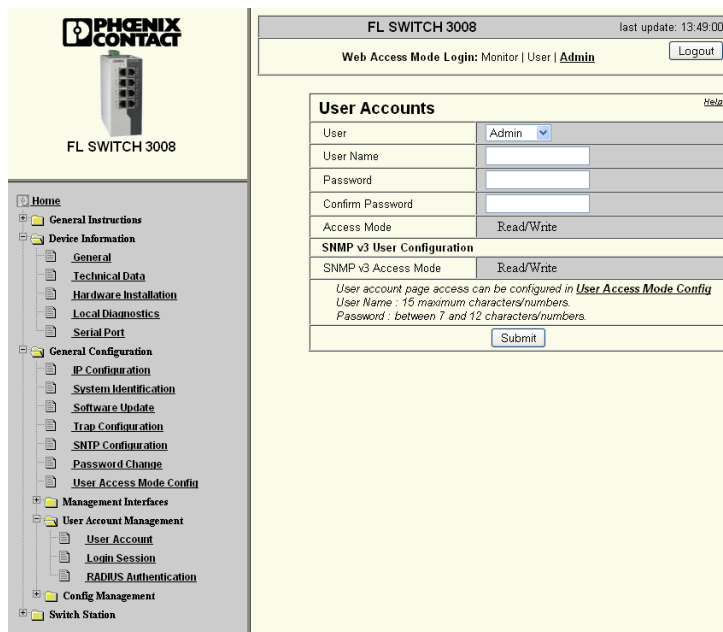


Figure 4-2 “User Accounts” page

2. From the “General Configuration/User Account Management/User Account” page, create a new account.
 - a) From the “User” drop-down menu, select the type of account. Select **Create/User** to create an account that provides access only to the specified pages. Select **Create/Admin** to create an account that has access to all pages and functions.



All existing accounts are also listed in the drop-down menu under **Account**.

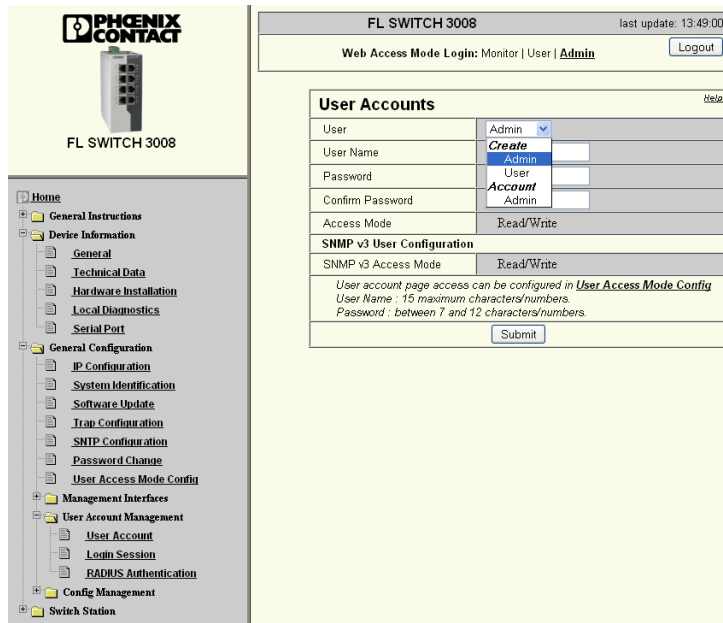


Figure 4-3 Select the user account type

- b) Enter the user name, password and re-enter the password in the appropriate fields. Be sure to record each account’s login settings, and remember that these are case sensitive.
The user name must be 1-15 characters. The password must be 7-12 characters.



If you forget or lose your login information, you will need to reset the switch to factory defaults using the hardware reset button on the top of the switch, which will delete all setup parameters, IP addresses and user accounts (see “Structure” on page 8).

- c) Click the “Access Mode” radio button for “Read only” or “Read/Write” access.
 - d) Click the “SNMP V3 Access Mode” radio button to allow access via the secure SNMP V3 network protocol. For SNMP V3 each user account must have separate access rights (defined on this page), a separate encryption type and a separate SNMP V3 password (see “Activating SNMP” on page 68) defined.
 - e) Click the “Submit” button to save the changes.
3. Repeat step 2 for all desired accounts. At least one of the new accounts should be an Admin account so all pages are accessible.
 4. After setting up at least one new account using “Admin” mode, delete the original factory-created Admin account.



NOTE:
If the factory-default account is not deleted automatically, anyone can get the default values from the Internet and have a “backdoor” method of unauthorized access to the switch, bypassing many security functions.
Do not delete the original factory-default account before an alternative “Admin” mode account is created or access to some pages may be unavailable, depending on the configuration of the “User” mode pages.

5. After all the accounts are created and configured, save the configuration to flash memory by clicking the small disc icon at the top of the page.

**NOTE:**

If the configuration is not saved and power is removed from the switch, all account setup information will be lost.

4.2 User account management

FL SWITCH 30..., 40... and 48... managed switches have an extensive set of network performance, redundancy and security options. However, in any one application, only a small quantity of these functions are used. Navigating around many unused web pages can increase complexity and add unnecessary troubleshooting or system start-up/expansion time.

In “Admin” mode, the web interface is fixed and shows all the functions, just like a typical industrial switch (see “Login” on page 53 for more on viewing modes). In “User” mode, the web interface can be completely customized to hide unwanted web pages. If the network is eventually expanded or changed, some or all of these pages can be added back in. It is also possible to configure functions in “Admin” mode, then hide all the related pages in the “User” mode.

Customization options

Both the default “User” mode pages and the pages associated with a particular user account can be customized.

- By customizing the default “User” mode pages, anyone with a login to the default user account will see the same set of pages. From the “User” mode, everyone can see the switch as a simple/basic managed switch, i.e., all the advanced functions are hidden.
- Specific accounts can be created for specific users or groups of users. For a group of users, a single user account can be created and the login info shared, or multiple accounts can be created with the same function access for each account.
- Large organizations may have different personnel responsible for initial configuration of the switch (administrator) than the personnel starting or using the switch in an application (user). In this case, different functions can be enabled in “Admin” mode and then customized as for a “User” mode to simply access the pages for start-up and ongoing use. Each time the administrator logs in, “Admin” mode is used, but by selecting “User” mode, only the start-up pages are used, simplifying navigation within the configuration pages.

Manually configuring a user account

1. Log in to the switch (see “Log in using web-based management” on page 41).

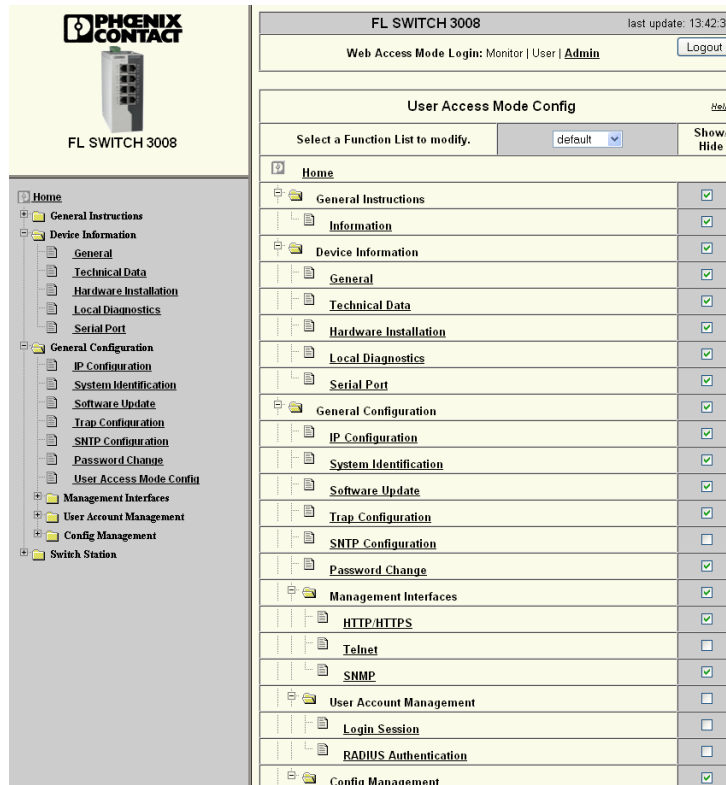


Figure 4-4 “User Access Mode Config” page

2. In “Admin” mode, go to the “General Configuration/User Access Mode Config” page. Click the desired account name from the “Select a Function List to modify” drop-down box.
3. Add or delete pages by clicking the check box for the desired page. Repeated clicks in a check box toggle the page on and off. To select a group of pages, click the check box associated with the group.
Alternatively, click the “Show all” and “Hide all” buttons at the bottom of the page.
4. Click the “Apply” button to save the settings to volatile memory (see “Configuration management” on page 59).

Automatically configuring a user account

The FL SWITCH 30..., 40... and 48... can also automatically select the pages for a user account.

1. Log in to the switch (see “Log in using web-based management” on page 41).
2. While in “Admin” mode, configure the switch using all the pages one would normally use.
3. Go to the “General Configuration/User Access Mode Config” page and click the “Cleanup” button. This causes the FL SWITCH 30..., 40... and 48... to “check” any page that contains a function that is enabled and uncheck pages without an enabled function.

4. Review the selected pages, and click the check box to toggle on or off any additional pages.
5. Click the “Apply” button to save the settings to volatile memory (see “Configuration management” on page 59).

4.3 Configuration management

4.3.1 Saving the configuration

The “Configuration Management” page is used to view all parameters required to save the active configuration or load a new configuration. It can also be used to restart the system with the relevant configuration.

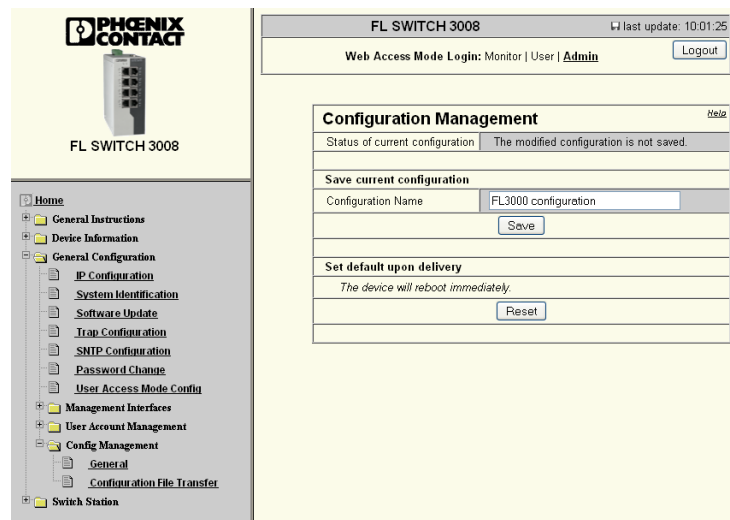


Figure 4-5 “Configuration Management” page



When using the “Submit” and “Apply” buttons to update the configuration, please be aware that the changes are only applied to the active configuration. The configuration must be saved to the internal memory from the “Configuration Management” page.



WBM can only be called using a valid IP address. Once the switch is reset to its default settings, it has no valid IP address and the addressing mechanism is set to BootP.

- **Status of current configuration:** Indicates if the current configuration is saved or not saved.
- **Configuration Name:** Enter a name for this configuration (optional).
- **Save:** Click the “Save” button to save the running configuration to non-volatile memory.
- **Reset:** Click the “Reset” button to return the switch to the factory defaults. All passwords are reset to defaults. The IP address is deleted, and the configuration on internal memory is removed.

On pages that can be modified, there is a “Submit” or “Apply” button. Click this button to save the changes made on that page to RAM memory. If the switch is reset or turned off at this time, the changes will be lost, as RAM is volatile memory. After clicking either the “Submit” or “Apply” button, a “Save” icon and time stamp appear at the top of the page. The time stamp indicates the time of the last save.

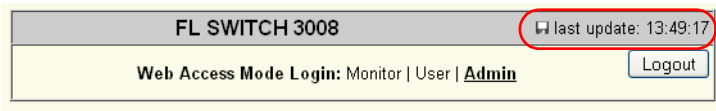


Figure 4-6 “Save” icon

Click the “Save” icon to go to the “Configuration Management” page. This page will indicate the status of the changes (see Figure 4-5). To save the changes to non-volatile memory, click the “Save” button. Power to the switch can then be removed, and the configuration settings will remain when restarted.

4.3.2 Configuration file transfer

The configuration file transfer function allows upload and download of the configuration to and from the switch. This function is found on the “General Configuration/Config Management/ Configuration File Transfer” page.

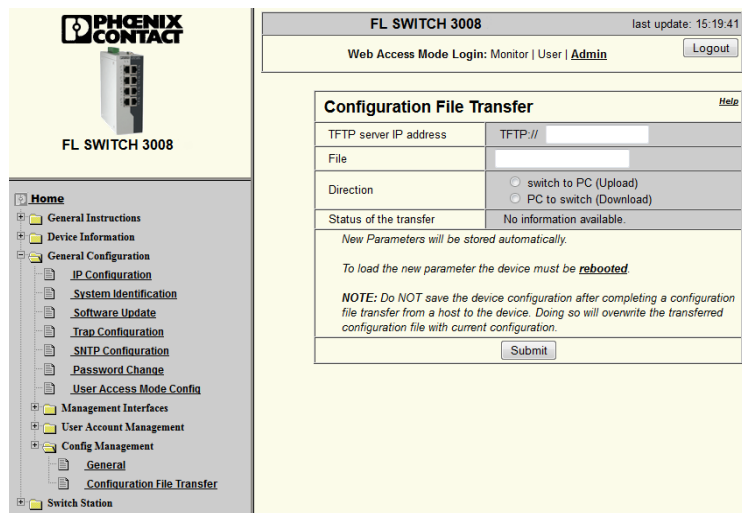


Figure 4-7 “Configuration File Transfer” page

- **TFTP Server IP Address:** Enter the IP address of the TFTP server in the “TFTP://” field. The factory default of the IPv4 address is **0.0.0.0**.
- **File:** Type the name of the file to be downloaded or uploaded to or from the TFTP server in the available field. The factory default is blank.
- **Direction:** Click either the “switch to PC (Upload)” or “PC to switch (Download)” radio button to select the desired transfer process.
- **Status of the transfer:** The status of the configuration file transfer is displayed during the file upload or download process.
- **Submit:** Click the “Submit” button to start the file transfer.

Procedure

1. Enter the IP address of the TFTP server from which the configuration file transfer will be requested.
2. In the "File" field, enter the file name of the upload or download. If the configuration has not been saved, save it now by clicking the "Save here before" link.
3. Click the "Submit" button to begin the process.

The transfer process may take a few seconds for the configuration file to upload or download to the TFTP server. New parameters will be stored automatically. To activate the new parameters, the device must be rebooted.

5 Switch station functions

5.1 Services

The “Services” page provides access to general functions of the switch, such as rebooting and login. The login session duration can be set to a maximum of 120 minutes. The page refresh interval can be customized on this page. The hardware reset button can be enabled and disabled to suit the user application.

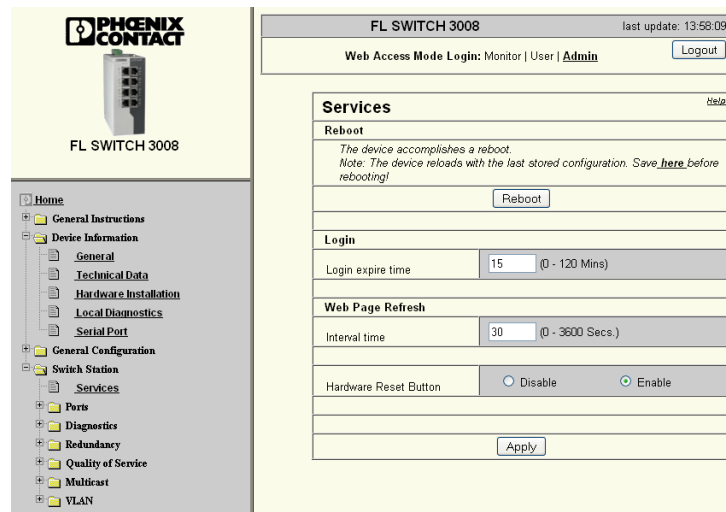


Figure 5-1 “Services” page

- **Reboot:** Click the “Reboot” button and the switch will restart. The switch will reboot to the saved configuration. A link is provided to go to the “Configuration Management” page and save the current configuration, if desired (see “Configuration management” on page 59).
- **Login expire time:** This sets the amount of inactive time (minutes) before an automatic exit of the session occurs. Enter a time between **0** and **120** minutes. The default is **15** minutes.
- **Interval time:** This sets the time between page redraws. Enter an interval time between **0** and **3600** seconds. The default is **30** seconds.
- **Hardware reset button:** Select the radio button to enable or disable the hardware reset switch.
- **Apply:** Click the “Apply” button to save the settings to volatile memory (see “Configuration management” on page 59).

5.2 Port configuration

Port configuration settings can occur at a switch-wide level (see “Port configuration table” on page 64) or each port can be configured individually (see “Individual port configuration” on page 65). In addition, the port configuration settings can be viewed in a non-editable table (see “Querying port states” on page 79).

5.2.1 Port configuration table

The port configuration table is a summary of the configuration of all of the switch ports. The default settings available for the combo ports correspond to those available for an SFP module. A copper link must be established to allow the selection of 100Full, 100Half, 10Full or 10Half. An SFP fiber optic link must be established to change them back to allow selection of 1000Full.

The “Port Configuration Table” page allows the review and setting of the basic settings for each port. The port configuration table is found on the “Switch Station/Ports/Port Configuration Table” page.

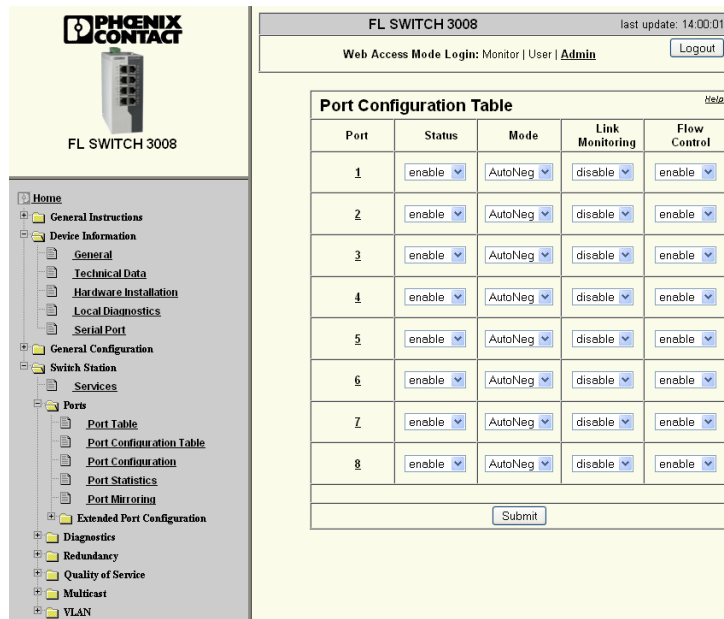


Figure 5-2 “Port Configuration Table” page

Each port is shown on a row, and there are four functions that can be set for each port.

- **Status:** Use the drop-down menu to “Enable” or “Disable” the selected port.
- **Mode:** Use the drop-down menu to select one of the following:
 - **AutoNeg:** Automatically sets the port to the best transfer speed based on the internal algorithms.
 - **10/HD:** Sets the port to operate in half-duplex mode at 10 Mbps.
 - **10/FD:** Sets the port to operate in full-duplex mode at 10 Mbps.
 - **100/HD:** Sets the port to operate in half-duplex mode at 100 Mbps.
 - **100/FD:** Sets the port to operate in full-duplex mode at 100 Mbps.

- **Link monitoring:** Use the drop-down menu to “Enable” or “Disable” the alarm contact notification in the event of link loss for the selected port.
- **Flow control:** Use the drop-down menu to “Enable” or “Disable” flow control for the selected port.
- **Submit:** Click the “Submit” button to save the settings to volatile memory (see “Configuration management” on page 59).

5.2.2 Individual port configuration

The “Port Configuration” page displays the current settings of an individual port.

The “Port Configuration” page manages the settings of an individual port. The port configurations can be configured from the “Switch Station/Ports/Port Configuration” page.

The screenshot shows the web interface for an FL SWITCH 3008. The main content area is titled 'Port Configuration' and displays settings for 'port-1'. The settings are as follows:

Port Number	port-1
Type	TX 10/100
Port Name	Port 1
Status	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
QoS Priority Level	<input checked="" type="radio"/> Low <input type="radio"/> High
Link State	Connected
Negotiation Mode	auto
Speed	100 MBit/s
Duplex Mode	full
Port Mode	Note for the installation of Ethernet cables: Auto Crossover is supported only in the Auto Negotiation mode. <input checked="" type="radio"/> Auto Negotiation <input type="radio"/> 10 MBit / Half Duplex <input type="radio"/> 10 MBit / Full Duplex <input type="radio"/> 100 MBit / Half Duplex <input type="radio"/> 100 MBit / Full Duplex
Link Monitoring	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Flow Control	<input type="radio"/> Disable <input checked="" type="radio"/> Enable

At the bottom of the form, there is a 'Submit' button and navigation links for 'Port Configuration of Port 1: General | Security | (R)STP | VLAN' and 'Port Statistics of Port 1: General'.

Figure 5-3 “Port Configuration” page

- **Port number:** Select the desired port from the drop-down menu.
- **Type:** Displays the type of port, either TX 10/100 or FX 100 FD.
- **Port name:** Allows the entry of a user-defined description for the port. Enter up to 15 characters.
- **Status:** Use the drop-down menu to “Enable” or “Disable” the selected port. This is also available from the “Port Configuration Table” page.
- **QoS Priority Level:** Click either the “High” or “Low” radio button to set the port priority level.
- **Link State:** Displays the link status of the port, either **Connected** or **Disconnected**.
- **Negotiation mode:** Displays the current negotiation mode, either **Auto** or **Manual**.
- **Speed:** Displays the connection speed of the port, either **10 MBit/s** (Mbps) or **100 MBit/s** (Mbps).
- **Duplex mode:** Displays the mode of the port, either **full** or **half** duplex.

- **Port Mode:** Click the radio button to select one of the following:
 - **Auto Negotiation:** Automatically sets the port to the best transfer speed based on the internal algorithms.
 - **10 MBit / Half Duplex:** Sets the port to operate in half-duplex mode at 10 Mbps.
 - **10 MBit / Full Duplex:** Sets the port to operate in full-duplex mode at 10 Mbps.
 - **100 MBit / Half Duplex:** Sets the port to operate in half-duplex mode at 100 Mbps.
 - **100 MBit / Full Duplex:** Sets the port to operate in full-duplex mode at 100 Mbps.
- **Link Monitoring:** Use the radio buttons to “Enable” or “Disable” alarm contact notification in the event of link loss for the selected port.
- **Flow control:** Use the radio buttons to “Enable” or “Disable” flow control for the selected port.
- **Submit:** Click the “Submit” button to save the settings to volatile memory (see “Configuration management” on page 59).



With link monitoring enabled, the user can go to the alarm contact to enable link monitoring (see “Configuring alarm contacts” on page 84). A loss of link on monitored ports will be indicated by the closed alarm contacts.

5.3 Management interfaces

The FL SWITCH 30..., 40... and 48... switch offers comprehensive security features, such as password protection, a security environment, HTTPS, Telnet, various user access options and port security features.

5.3.1 Web server protocol

When the HTTPS protocol is selected, communication between the WBM pages for the switch and the browser on the computer is encrypted. The HTTP protocol communicates with unencrypted data.

The web server can be set to HTTP, HTTPS, HTTPS with TLS, HTTPS with TLS (2048-bit group), or disabled from the “General Configuration/Management Interfaces/HTTP/HTTPS” page.

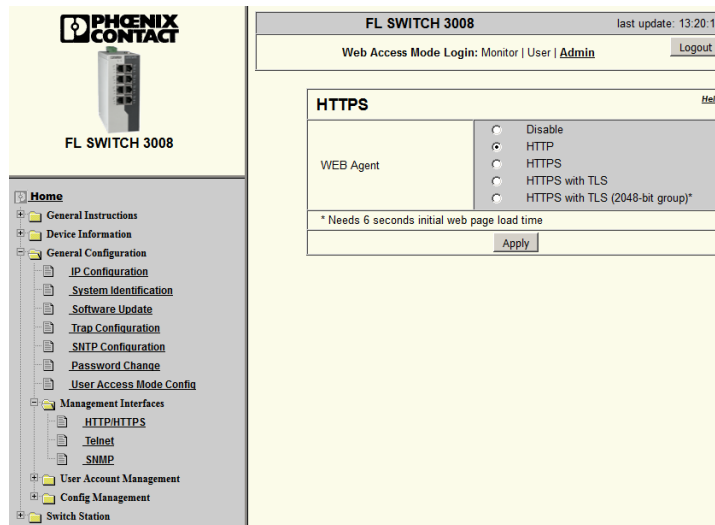


Figure 5-4 “HTTPS” page

- **Web Agent:**
 - Disable: Disables HTTP and HTTPS connections
 - HTTP: Allows only HTTP connections
 - HTTPS: Allows only HTTPS connections
 - HTTPS with TLS: Allows only HTTPS connection with TLS and disables SSL v3.0.
 - HTTPS with TLS (2048-bit group): Allows only HTTPS connection with TLS 20148-bit group and disables SSL v3.0. This needs six seconds for initial page load time.
- **Apply:** Click the “Apply” button to save the settings to volatile memory (see “Configuration management” on page 59).

5.3.2 Activating SNMP

The use of SNMP can be activated and deactivated, or the protocol version can be configured from the “General Configuration/Management Interfaces/SNMP” page.

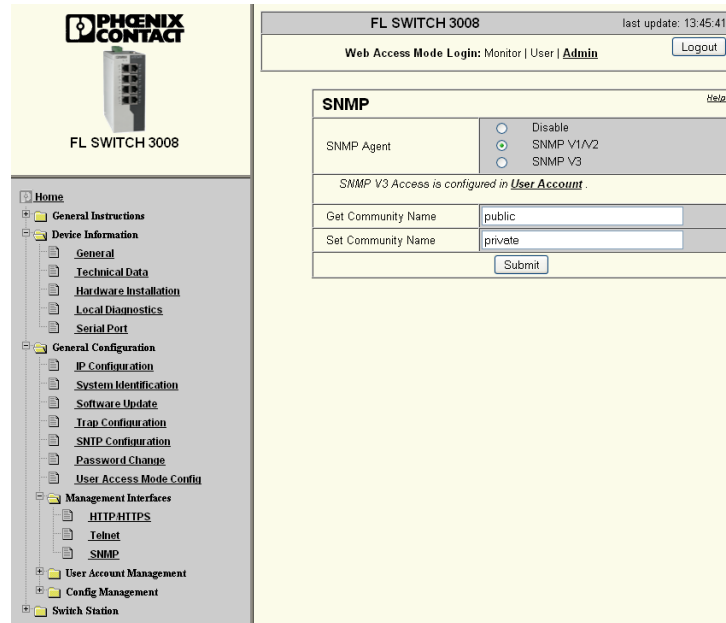


Figure 5-5 “SNMP” page with V1/V2 options

- **SNMP agent:** Click the appropriate radio button to “Disable” or set the switch to accept “SNMP V1/V2” or “SNMP V3” commands.
- **SNMP V1/V2:**
Get Community Name: Enter the password required to read from objects. The default password is **public**.

Set Community Name: Enter the password required to write to objects. The default password is **private**.

The screenshot shows the web interface for an FL SWITCH 3008. The top header includes the Phoenix Contact logo and the device name. Below the header is a navigation menu with categories like Home, General Instructions, Device Information, General Configuration, Management Interfaces, User Account Management, and Config Management. The main content area is titled 'SNMP' and contains the following configuration options:

- SNMP Agent:** Radio buttons for Disable, SNMP V1/V2, and SNMP V3 (selected).
- SNMP V3 Access:** A note stating 'SNMP V3 Access is configured in User Account'.
- Authentication and Encryption:** A dropdown menu set to 'SNMPV3 Auth-MD5'.
- Authentication Password:** A text input field containing 'privateadmin'.
- Submit:** A button to save the configuration.

Figure 5-6 “SNMP” page with V3 options

– SNMP V3:



SNMP access parameters are defined separately for each login account. For each account accessing SNMP via secure V3, the read/write access, authentication/encryption type and authentication password need to be defined. The SNMP V3 access rights are configured on the “User Account” page (see “User account management” on page 57).

- **Authentication and Encryption:** From the drop-down menu, select the method of authentication and encryption to be used for SNMP V3:
 - **No Auth.:** No authentication.
 - **Auth MD5:** Authentication based on HMAC-MD5 algorithm.
 - **Auth SHA:** Authentication based on HMAC-SHA algorithm.
 - **Priv Auth MD5:** Authentication based on HMAC-MD5 algorithm and CBC-DES encryption.
 - **Priv Auth SHA:** Authentication based on HMAC-SHA algorithm and CBC-DES encryption.
- **Authentication Password:** Enter the password used for authenticating the SNMP V3 connection.
- **Submit:** Click the “Submit” button to save the settings to nonvolatile memory (see “Configuration management” on page 59).

5.4 Security

The FL SWITCH 30..., 40... and 48... switch offers comprehensive security features, such as password protection, a security environment, HTTPS, Telnet, various user access options and port security features.

Managed switches are one part of a comprehensive “defense in depth” solution that helps protect against unwanted access to manufacturing-level networks. The FL SWITCH 30..., 40... and 48... switch offers comprehensive security features, such as:

- Protect network access by user accounts
 - Defining switch login rights and user mode access by person (see “User account management” on page 57).
 - 802.1x RADIUS authentication (see “RADIUS authentication (IEEE 802.1x)” on page 71).
- Protect network access by devices
 - Port security (see “Port security and IEEE 802.1x” on page 70).
- Protect network access to the switch
 - Enable/disable external interfaces, such as web, Telnet, serial port and reset button (see “Initial setup” on page 27).
 - Encrypted web (HTTPS) (see “Web server protocol” on page 66) and SNMP (V3) communication (see “Activating SNMP” on page 68) to the switch.
 - VLAN isolation of traffic (see “VLAN” on page 135).

5.4.1 Port security and IEEE 802.1x

The use of MAC-based port security or the IEEE 802.1x (RADIUS authentication) function must first be enabled/disabled from the “Switch Station/Ports/Ext. Port Configuration/General Security Configuration” page.

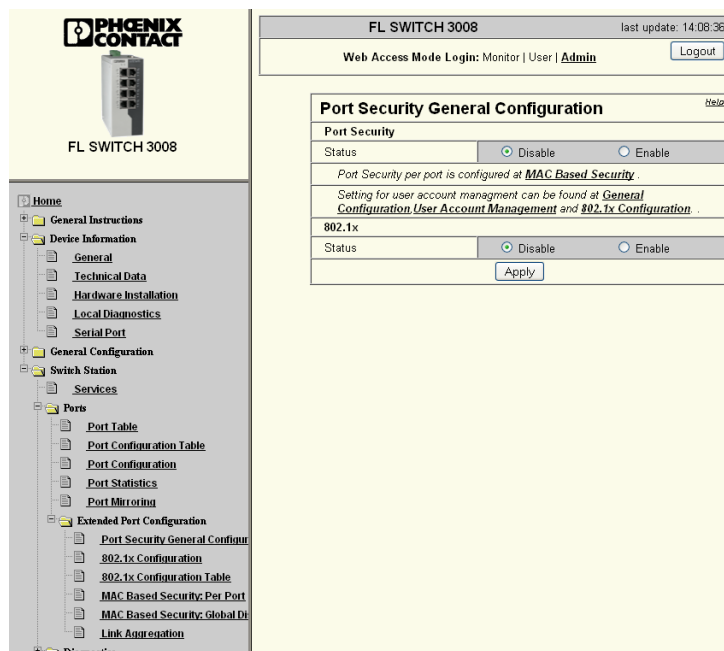


Figure 5-7 “General Security Configuration” page

- **Port Security Status:** Port security for the entire switch is activated by selecting the “Enable” button. Detailed configuration of this function is found at “MAC-based security per port” on page 75.
- **802.1x Status:** IEEE 802.1x radius authentication is activated by selecting the “Enable” button. Detailed configuration of this function is found at “RADIUS authentication (IEEE 802.1x)” on page 71.
- **Apply:** Click the “Apply” button to save the settings to volatile memory (see “Configuration management” on page 59).



Links are provided to easily move to other pages with more detailed settings for security.

5.4.2 RADIUS authentication (IEEE 802.1x)

Radius authentication implements the authentication method according to standard IEEE 802.1x. This standard provides a general method for authentication and authorization in IEEE 802 networks. When a person attempting access to the network (the “supplicant”) connects to the switch, a physical port of the switch sends the PC’s certificates to a RADIUS authentication server using the **Extensible Authentication Protocol (EAP)**. This verifies and, if applicable, sends a command back to the switch that permits access to the services offered by the authenticator, i.e., the switch. This option of using an authentication server also enables local, unrecognized devices to be granted access to the network. For example, members of an external service team can log into a network.

This authorization is usually performed once when the device initially connects, though authentication servers can have other options. Once the device is disconnected, the switch closes the port until the next connection. To guard against sophisticated attempts at unauthorized access, the switch can be configured to re-authenticate on a periodic timed basis.

The configuration of 802.1x RADIUS authentication requires working with several pages.

- First, the enabling of the 802.1x function, which also activates all the other 802.1x related pages, is done using the “Port Security General Configuration” page.
- The setup of both the basic and advanced authentication protocol options is accomplished using the “802.1x Configuration” page.
- The “802.1x Configuration Table” page allows one to see the authentication status of all ports on the switch and change the basic operating mode.
- The addressing and time out parameters related to the authenticating server are configured on the “RADIUS Authentication Server” page.

The parameters required for IEEE 802.1x can be set from the “Switch Station/Ports/Ext. Port Configuration/802.1x Configuration” page. The recommended parameters are preset.

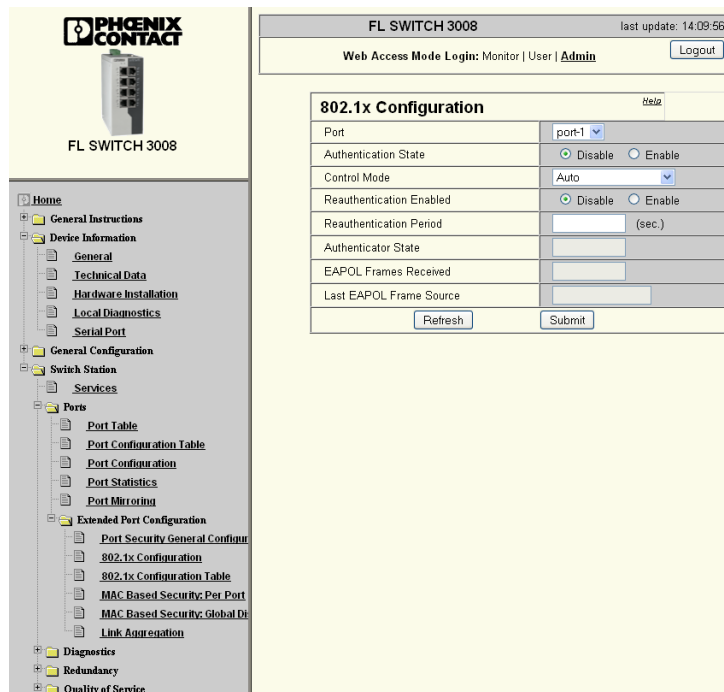


Figure 5-8 “802.1x Configuration” page

- **Port:** Select the desired port from the drop-down menu.
- **Authentication State:** Click the radio button to “Enable” or “Disable” the selected port as an authenticator.
- **Control Mode:** Use the drop-down menu to choose one of the following:
 - **Auto:** The port will send EAPs to the supplicant but requires an acknowledgement from the authentication server to become authorized.
 - **Force Authorized:** The port does not need to be authorized by the authentication server because it is always authorized. This mode is useful when 802.1x is desired but not on any particular port.
 - **Force Unauthorized:** The port cannot be authorized, essentially disabling the port from use.
- **Reauthentication Enabled:** Click the radio button to “Enable” or “Disable” periodic re-authentication on this port based on the “Reauthentication Period” parameter.
- **Reauthentication Period:** Enter the re-authentication time period, in seconds.
- **Authenticator State:** Displays the current authentication state of the port.
- **EAPOL Frames Received:** Displays the number of EAPOL (Extensible Authentication Protocol Over LAN) frames received on this port.
- **Last EAPOL Frame Source:** Displays the MAC address of the last device to send an EAPOL frame to this port.
- **Refresh:** Click the “Refresh” button to update the data on the page.
- **Submit:** Click the “Submit” button to save the settings to volatile memory (see “Configuration management” on page 59).

5.4.3 802.1x configuration table

The “802.1x Configuration Table” page is used to view the 802.1x authentication status of all ports at the same time. It is also used to make quick authentication-mode changes during special circumstances, such as transitioning from a start-up to normal operation.

The screenshot shows the web interface for an FL SWITCH 3008. The main content area is titled "802.1x Configuration Table" and contains a table with the following data:

Port	Mode	Authenticator State
1	Authorize all	Authorized
2	Auto	
3	Auto	
4	Auto	
5	Auto	
6	Auto	
7	Auto	
8	Auto	

Below the table is a "Submit" button. The interface also includes a navigation menu on the left and a header with the device name and user information.

Figure 5-9 “802.1x Configuration Table” page

- **Port:** The port being configured. Clicking the port link will navigate the user to the “802.1x Configuration” page with that port pre-selected.
- **Mode:** The 802.1x control mode configured on this port. For start-up or other unusual conditions, the port control mode for all ports can be changed from this one page. One example might be to change from the easier access **Force Authorized** mode to the more restrictive, normal operation **Auto** or **Force Unauthorized** modes.
- **Authenticator State:** The current authentication state of the port.
- **Submit:** Click the “Submit” button to save the settings to volatile memory (see “Configuration management” on page 59).

5.4.4 Configuring the RADIUS server

The RADIUS server implements the authentication method according to standard IEEE 802.1x. This standard provides a general method for authentication and authorization in IEEE 802 networks. On network access, a physical port of the switch in the LAN authenticates an external device using an authentication server: the RADIUS server. This verifies and, if applicable, permits access to the services offered by the authenticator.

This option of using an authentication server also enables local, unrecognized devices to be granted access to the network. For example, members of an external service team can log into a network without the definition of open guest access or similar.

The RADIUS server is configured from the “General Configuration/User Account Management/RADIUS Authentication” page.

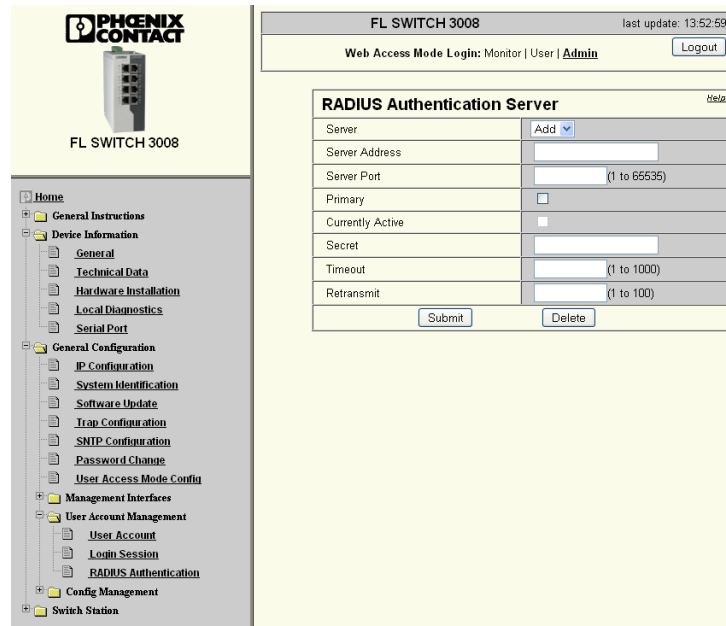


Figure 5-10 “RADIUS Authentication Server” page

- **Server:** Use the drop-down menu to “Create”, “View” or “Configure” an authentication server to be used for 802.1x.
- **Server Address:** Enter the IP address of the authentication server.
- **Server Port:** Enter the logical port number used by the authentication server.
- **Primary:** Click the check box to make this authentication server the primary authentication server.
- **Currently Active:** Displays if the selected server is actively being used by the switch for authentication purposes.
- **Secret:** Enter the authentication server’s password.
- **Timeout:** Enter a timeout value between **1** and **1000** seconds. After this amount of time, the authentication will time out.
- **Retransmit:** Enter the time between authentication attempts, from **1** to **100** seconds. This is the amount of time that passes after a timeout before another authentication attempt is made.
- **Submit:** Click the “Submit” button to save the settings to volatile memory (see “Configuration management” on page 59).
- **Delete:** Click the “Delete” button to delete the selected server.

5.4.5 MAC-based security overview

The FL SWITCH 30..., 40... and 48... switches can allow or block communications with industrial devices by looking at their hardware MAC addresses. The “MAC Based Security: Per Port” page defines which device the MAC addresses are allowed to communicate with each port. This is typically used to only allow communication with the I/O, PLCs, etc., and their approved spare units or approved maintenance laptops connected to those ports.

The “MAC Based Security: Global Discard” page defines which MAC addresses are blocked from communicating with any port on the switch (all ports block communications to those devices). This may be used to prevent specific laptops in other areas or departments of the plant from accessing a particular part of the network.

5.4.6 MAC-based security per port

Each port is allowed to communicate with up to 24 MAC addresses. This “multiple MAC address” capability allows for:

- the connection of multiple devices via other unmanaged or managed switches.
- multiple maintenance laptops to be connected.
- “pre-approved” spare devices to allow fast swap out of failed equipment without switch re-configuration.

The necessary parameters can be set from the “Switch Station/Ports/Ext. Port Configuration/MAC Based Security” page.

The screenshot displays the web interface for a Phoenix Contact FL SWITCH 3008. The main content area is titled "MAC Based Security: Per Port" and shows configuration for "port-1". The "Security Mode" is set to "None". A "Last Learned Source Mac Address" is shown as "00:15:c5:3d:e5:01". Below this is a table for "Allowed Mac Addresses" with columns for Description, MAC Address, VLAN, and Del. The table contains 9 rows, each with a default MAC address of "00:00:00:00:00:00". At the bottom, there are "Submit" and "Delete" buttons, and a note stating "The port will reject all but the MAC addresses entered here. The port security is disabled. You can find the global port security status at General Security Configuration".

Description	MAC Address	VLAN	Del
Address 1	00:00:00:00:00:00		<input type="checkbox"/>
Address 2	00:00:00:00:00:00		<input type="checkbox"/>
Address 3	00:00:00:00:00:00		<input type="checkbox"/>
Address 4	00:00:00:00:00:00		<input type="checkbox"/>
Address 5	00:00:00:00:00:00		<input type="checkbox"/>
Address 6	00:00:00:00:00:00		<input type="checkbox"/>
Address 7	00:00:00:00:00:00		<input type="checkbox"/>
Address 8	00:00:00:00:00:00		<input type="checkbox"/>
Address 9	00:00:00:00:00:00		<input type="checkbox"/>

Figure 5-11 “MAC Based Security: Per Port” page

- **Port:** Select the desired port from the drop-down menu.

- **Security mode:** Click either the “None” or “Block Packets” radio button. This function defines the response to a wrong device.
 - **None:** No blocking of packets occurs, allowing communication to any MAC address. During system start-up situations, setting the security mode to **None** allows preconfiguring all MAC addresses, but does not activate the security checking until the proper time in the start-up.
 - **Block packets:** Allows packets only to the listed MAC addresses.
- **Allowed MAC Addresses:** MAC addresses can be typed in manually or entered automatically. For automatic entry, connect the first approved device to the port and click the “arrow” icon next to the “MAC Address” field. This reads the address, has the device generate traffic (for example, automatically by BootP/DHCP requests or by pinging from a PC) (source address) of the device and enters it in the field. Disconnect this device, connect the next device and click the “arrow” icon for the next row. Continue in this way until all addresses are entered. For each MAC address, an optional name can be entered in the “Description” field. For added MAC checking associated with specific VLANs, select the required VLAN ID from the “VLAN” drop-down menu.
- **Submit:** Click the “Submit” button to save the settings to volatile memory (see “Configuration management” on page 59).
- **Delete:** If the application changes or a failed device is removed or replaced, MAC address entries can be deleted. Click the “Del” check box next to the address to be deleted, then click the “Delete” button.



MAC Addresses must be deleted from the “MAC Based Security: Per Port” menu in the “Allowed MAC Addresses” group. Clicking the “Disable” button in the “Port Security General Configuration” page (see Figure 5-7) alone will not disable the feature.

5.4.7 MAC-based security global discard

MAC-based security global discard configures the MAC addresses that are to be blocked from communicating at any port. All ports will reject communication attempts from these devices.

The screenshot shows the web interface for the FL SWITCH 3008. The page title is "MAC Based Security: Global Discard". The header includes the device name "FL SWITCH 3008" and the user information "Web Access Mode Login: Monitor | User | Admin" with a "Logout" button. The main content area has two input fields: "Add MAC address (Ex: 00:11:22:33:44:55)" and "Delete MAC address" with a dropdown menu. Below these fields is a note: "MAC addresses entered here, will be reject by all ports." and a "Submit" button. The left navigation menu includes sections like Home, General Instructions, Device Information, General Configuration, Switch Station, Services, Ports, Extended Port Configuration, Diagnostics, and Redundancy.

Figure 5-12 “MAC Based Security: Global Discard” page



The MAC-based security global discard function filter operates on the destination address in unicast frames only.

- **Add MAC address:** Enter the first address in the “Add MAC address” field, then click the “Submit” button. After the field is blank, repeat the process until all desired MAC addresses are entered. To confirm correct entry, verify that the MAC address appears in the “Delete MAC address” drop-down menu. Up to 29 MAC addresses can be displayed at once, then a scroll bar appears.
- **Deleting MAC address:** From the “Deleting MAC address” drop-down menu, select the MAC address to be removed. After selecting, click the “Submit” button. Repeat the process for all desired MAC addresses. When the address is deleted, the field will be cleared.
MAC addresses may need to be removed if application conditions change.
- **Submit:** Click the “Submit” button to save the settings to volatile memory (see “Configuration management” on page 59).

5.5 Diagnostics

5.5.1 Trap configuration

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

The FL SWITCH 30..., 40... and 48... allows configuration of the events that are to trigger the sending of a trap, as well as the trap receivers.

The use of traps can be configured from the “General Configuration/Trap Configuration” page.

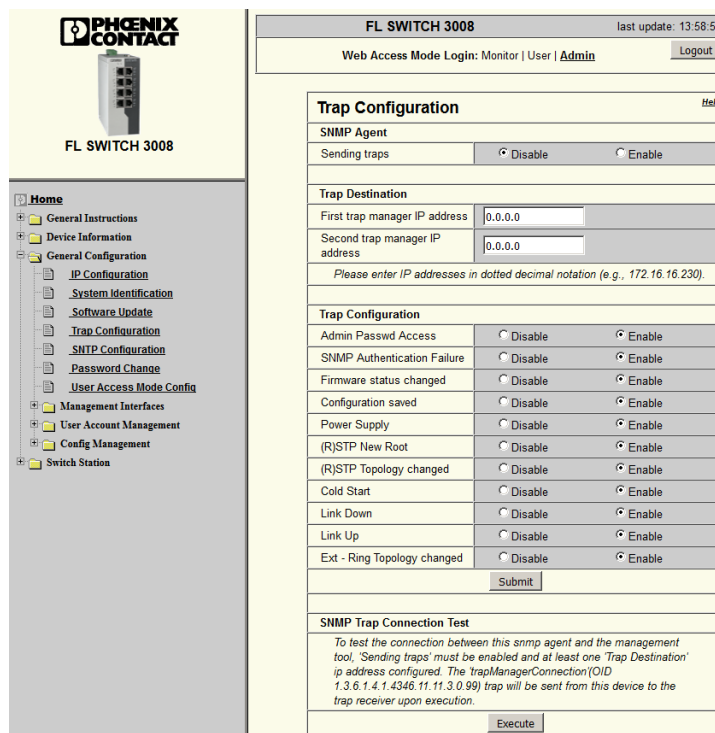


Figure 5-13 “Trap Configuration” page

- **Sending traps:** Click a radio button to “Enable” or “Disable” the sending of traps.
- **First trap manager IP address:** Enter the IP address of the first trap manager.
- **Second trap manager IP address:** Enter the IP address of the second trap manager.

- **Trap Configuration:** The following types of traps can be enabled or disabled by clicking the appropriate radio button.
 - Admin Passwd Access
 - SNMP Authentication Failure
 - Firmware status changed
 - Configuration saved
 - Power Supply
 - (R)STP New Root
 - (R)STP Topology changed
 - Cold Start
 - Link Down
 - Link Up
 - Ext - Ring Topology changed: When using the extended ring redundancy function, the trap message is triggered when both ring's status go to the "Block" or "Down" state. The same "trapExtRingFailure" trap message is sent when the coupling ring state is changed.
- **Submit:** Click the "Submit" button to save the settings to volatile memory (see "Configuration management" on page 59).
- **Execute:** Click the "Execute" button to send a test trap between the SNMP agent and the management tool. At least one trap destination IP address must be entered, and one trap must be enabled.

5.5.2 Querying port states

The settings of all the ports can be viewed on a single page.

An overview of all ports can be obtained in the "Switch Station/Ports/Port Table" page.

The screenshot shows the web interface for the FL SWITCH 3008. The page title is "FL SWITCH 3008" with a last update time of 12:53:57. The navigation menu includes Home, General Instructions, Device Information, General Configuration, Switch Station, Ports, Port Table, Port Statistics, Diagnostics, Redundancy, Multicast, and VLAN. The "Port Table" is displayed with the following data:

Port	Type	Port Status	Mode	Link Monitoring	Flow Control
1	TX 10/100	Enable	100 MBit FD	Disable	Enable
2	TX 10/100	Enable	Not Connected	Disable	Enable
3	TX 10/100	Enable	Not Connected	Disable	Enable
4	TX 10/100	Enable	Not Connected	Disable	Enable
5	TX 10/100	Enable	Not Connected	Disable	Enable
6	TX 10/100	Enable	Not Connected	Disable	Enable
7	TX 10/100	Enable	Not Connected	Disable	Enable
8	TX 10/100	Enable	Not Connected	Disable	Enable

Note: This page will automatically refresh in 25 seconds.

Figure 5-14 "Port Table" page

The page is arranged in a table format with the ports listed down the left column and the corresponding port settings shown in each row.

- **Port:** Displays the port number.
- **Type:** Displays the type of port, either **TX 10/100** or **FX 100**.
- **Port status:** Displays the current status of the port as either **Enable** or **Disable**.
- **Mode:** Displays the operating mode of the port as **Not Connected**, **Auto-Neg**, **10 Mbps/HD**, **10 Mbps/FD**, **100 Mbps/HD**, **100 Mbps/FD**.
- **Link monitoring:** Displays the current status of the alarm contact notification in the event of link loss for the port as either **Enable** or **Disable**.
- **Flow control:** Displays the current status of flow control as either **Enable** or **Disable**.

5.5.3 Using port statistics

This view provides detailed statistical information about the volume of received data for each individual port.

Port-specific data can be viewed or the counters cleared from the “Switch Station/Ports/Port Statistics” page.

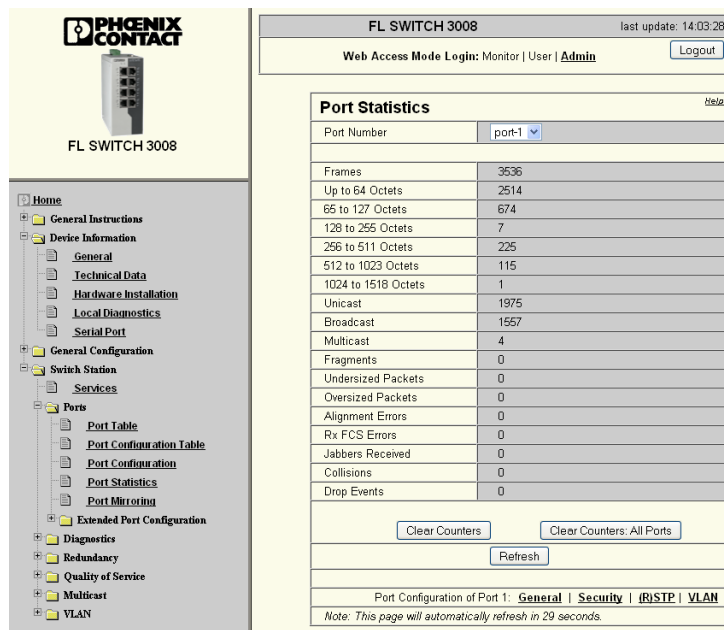


Figure 5-15 “Port Statistics” page

- **Port number:** Select the desired port number from the drop-down menu. The following data can be viewed for the selected port.
 - **Frames:** Total number of frames.
 - **Up to 64 Octets:** Quantity of frames 64 octets in size.
 - **65 to 127 Octets:** Quantity of frames 65 to 127 octets in size.
 - **128 to 255 Octets:** Quantity of frames 128 to 255 octets in size.
 - **256 to 511 Octets:** Quantity of frames 256 to 511 octets in size.
 - **512 to 1023 Octets:** Quantity of frames 512 to 1023 octets in size.
 - **1024 to 1518 Octets:** Quantity of frames 1024 to 1518 octets in size.

- **Unicast:** Quantity of unicast frames.
- **Broadcast:** Quantity of broadcast frames.
- **Multicast:** Quantity of multicast frames.
- **Fragments:** Quantity of fragmented frames.
- **Undersized Packets:** Quantity of undersized packets.
- **Oversized Packets:** Quantity of oversized packets.
- **Alignment Errors:** Quantity of alignment errors.
- **Rx FCS errors:** Quantity of received frame check sequence errors.
- **Jabbers Received:** Quantity of jabbers received.
- **Collisions:** Quantity of collisions.
- **Drop Events:** Quantity of packets dropped.
- **Clear Counters:** Click the “Clear Counters” button to reset all counters for the selected port to zero.
- **Clear Counters: All Ports:** Click the “Clear Counters: All Ports” button to reset all counters for all ports to zero.
- **Refresh:** Click the “Refresh” button to update the page.

5.5.4 Configuring port mirroring

The “Port Mirroring” page activates/deactivates and sets port mirroring. Port mirroring is used to passively read input or output data that is being transmitted via a selected port. To do this, connect a PC to the destination port, which records the data.



Ports grouped to one trunk via link aggregation cannot be included in the mirroring, either individually or as a complete trunk. This applies for use as the mirroring source or destination.



A selected port that is used as the destination port only forwards the packets redirected to it from the source ports. It no longer forwards packets that are sent directly to this port. In addition, it no longer forwards received packets to other switch ports. The availability of the network-based user interface of the switch (WEB, SNMP, etc.) is no longer ensured via this port.



IGMP membership report messages will not be copied from the source port to the mirror port when IGMP snooping is enabled.

For the FL SWITCH 48...E... , the WBM is not accessible on a mirror port. The mirror capture port is only for mirror capture. This port will not forward incoming traffic and is not for use as a management port or normal switch port.

Port mirroring is configured in the “Switch Station/Ports/Port Mirroring” page.

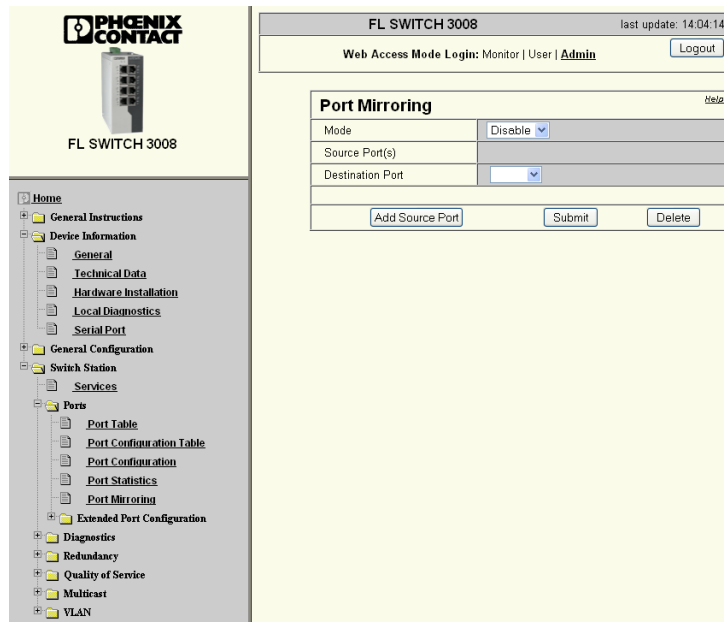


Figure 5-16 “Port Mirroring” page

- **Mode:** Use the drop-down menu to enable or disable port mirroring.
- **Add Source Port:** Click the “Add Source Port” button to select the port number to be mirrored. Click the “Enable” button after the “Add Source Port” button to load the port.
- **Destination port:** Use the drop-down menu to select the destination port.

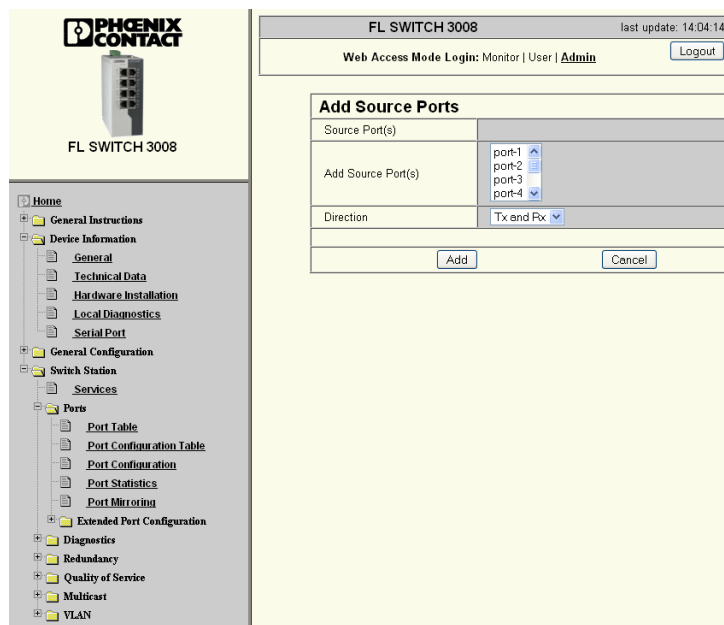


Figure 5-17 “Adding Source Ports” page

- **Source Port(s):** Displays any ports already configured as a source port.

- **Add Source Port(s):** Use the drop-down menu to select a source port. Click the “Add” button after selecting the port. To select multiple ports, click the drop-down arrow, hold the <Ctrl> key and click the desired ports. After selection, release the <Ctrl> key and click the “Add” button.
- **Direction:** Indicates the mirroring function direction.
- **Add:** Click the “Add” button after the source ports are selected.
- **Submit:** Click the “Submit” button to save the settings to volatile memory (see “Configuration management” on page 59).
- **Delete:** Click the “Delete” button to delete a source port.

5.5.5 Display

The “Display” page shows the current operating status of the switch, alarm contact and power supply.

Monitor the switch operating status from the “Switch Station/Diagnostics/Display” page.

The screenshot shows the web interface for an FL SWITCH 3008. The top header includes the Phoenix Contact logo and the device name 'FL SWITCH 3008' with a 'last update: 12:56:04' timestamp. Below the header, the 'Web Access Mode Login: Monitor | User | Admin' is displayed. The main content area is titled 'Display' and contains three sections:

Display	
Operating Status	Firmware is working.
Alarm Contact	
Status	At Present no event to trigger the alarm contact is recognized.
Power Supply	
Status	Power supplies US1 and US2 are connected.

A note at the bottom of the page states: "Note: This page will automatically refresh in 20 seconds." On the left side, a navigation menu is visible, showing a tree structure with categories like Home, General Instructions, Device Information, General Configuration, Switch Station, Ports, Diagnostics (with sub-items: Display, Utilization, Event Table, MAC Address Table), Redundancy, Multicast, and VLAN.

Figure 5-18 “Display” page

- **Operating Status:** Displays if the firmware is working.
- **Alarm Contact Status:** Displays any alarms that are active.
- **Power Supply Status:** Displays the status of the supply power connected to the switch.

5.5.6 Configuring alarm contacts

Alarms can be activated and deactivated. Alarm events cause the alarm contacts to close, providing notification to any connected monitoring devices.

The use of alarm contacts is configured from the “Switch Station/Diagnostics/Alarm Contact” page.

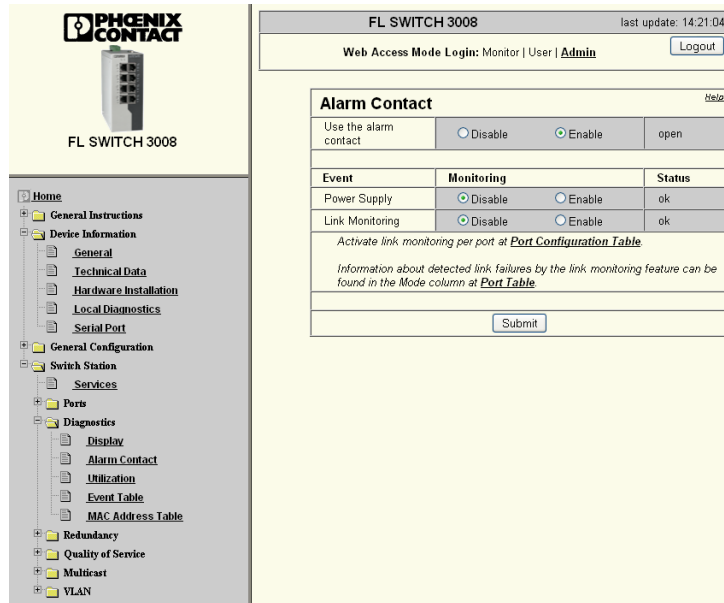


Figure 5-19 “Alarm Contact” page

- **Use the alarm contact:** Click the radio buttons to “Enable” or “Disable” the alarm contact function.
- **Power Supply:** Click the radio buttons to “Enable” or “Disable” monitoring of the power supply.
- **Link monitoring:** Click the radio buttons to “Enable” or “Disable” monitoring of the links. Link monitoring must first be enabled from this page for individual port monitoring to function. If disabled, individual port monitoring will not function, regardless of the individual port setting.



To activate link monitoring per port, see “Port configuration table” on page 64.

- **Submit:** Click the “Submit” button to save the settings to volatile memory (see “Configuration management” on page 59).

5.5.7 Utilization

The “Utilization” page shows the network capacity of each individual port as a bar graph. The display is automatically updated according to the refresh interval.

Monitor the network utilization from the “Switch Station/Diagnostics/Utilization” page.

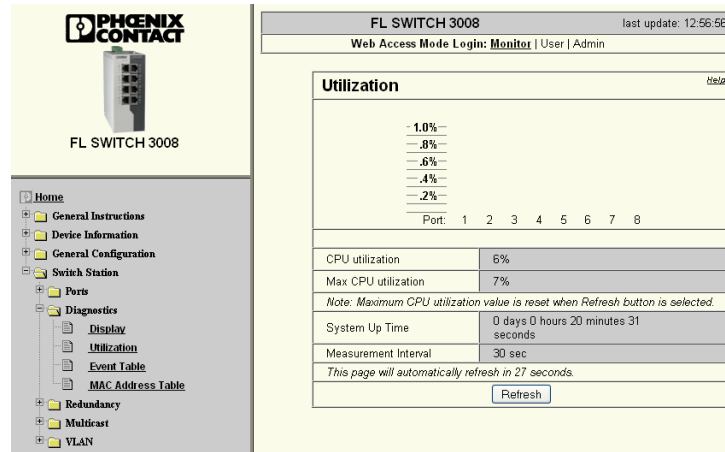


Figure 5-20 “Utilization” page

At the top of the “Utilization” page is a graph that displays the bandwidth utilization of each port as a percentage of the maximum capacity of the switch. For switches with nine or more ports, a second graph displays the utilization of the additional ports.



The percent utilization value measures both transmitted and received packets. For full duplex settings, a fully loaded port will indicate 200% utilization (100% for transmitted plus 100% for received packets).

- **CPU utilization:** Displays the current CPU usage as a percentage of the maximum capacity.
- **Max CPU utilization:** Displays the maximum CPU usage since the last reboot as a percentage of the maximum capacity.
- **System Up Time:** Displays the time since the last reboot of the switch.
- **Measurement interval:** Displays how often the port utilization graph refreshes.
- **Refresh:** Click the “Refresh” button to reset the Max CPU utilization displayed.

5.5.8 Event table

The “Event Table” page displays diagnostic events in table format, including the system time stamp, on all events.

Events are displayed on the “Switch Station/Diagnostics/Event Table” page.

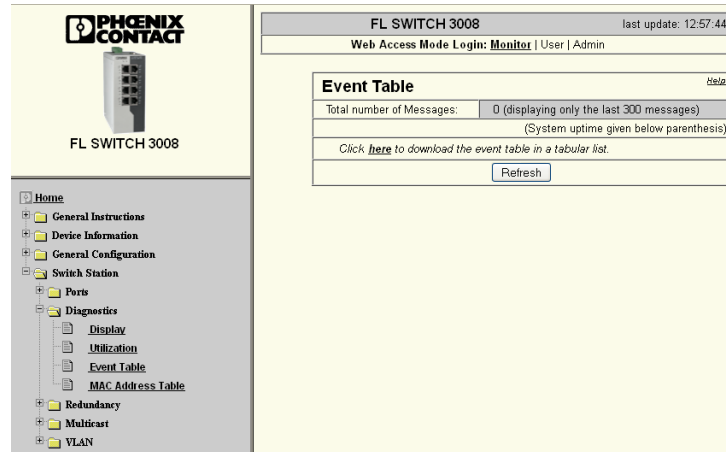


Figure 5-21 “Event Table” page

- **Total number of Messages:** Displays the number of messages stored in the switch. The maximum number of messages that can be displayed in the event table is 300.
- **Refresh:** Click the “Refresh” button to update the data on the page.

To download and view the most recent 300 messages, click the link on the page.

5.5.9 Displaying the MAC address table

The “MAC Address Table” page displays the MAC addresses of all devices connected to the device according to their port.

The MAC addresses of the devices are displayed in the “Switch Station/Diagnostics/MAC Address Table” page.

The screenshot shows the web interface for a Phoenix Contact FL SWITCH 3008. The page title is "FL SWITCH 3008" with a "last update: 12:58:37" timestamp. Below the title, it says "Web Access Mode Login: Monitor | User | Admin". The main content area is titled "MAC Address Table" and contains a table with the following data:

No.	VLAN	Mac Address	Port
1	1	00:15:c5:3d:e5:01	1

Below the table, there is a link: "Click [here](#) to download MAC address table in a tabular list." and a "Refresh" button.

Figure 5-22 “MAC Address Table” page

5.5.10 Link layer discovery protocol

The switch supports the link layer discovery protocol (LLDP) according to IEEE 802.1AB and enables topology detection of devices that also have LLDP activated.

Advantages of using LLDP:

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

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

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

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

General

The LLDP, according to 802.1AB, is used by network devices to learn and maintain the individual neighbor relationships.

Function

A network infrastructure component transmits a port-specific link layer discovery protocol data unit (LLDPDU), which contains the individual device information, at the **Message Transmit Interval** to each port in order to distribute topology information. The partner connected to the relevant port learns the corresponding port-specific neighbors from these messages.

The information learned from an LLDPDU is saved for a defined period of time known as the **time to live (TTL)** value. Subsequent receipt of the same LLDPDU information resets the TTL value, and the information is still saved. If the TTL expires, the neighbor information is deleted.



The FL SWITCH 30..., 40... and 48... manages a maximum of 50 items of neighbor information. All other information is ignored.



If several neighbors are displayed on one switch port, then there must be at least one other switch/hub installed between this switch and the neighbor.

Table 5-1 Event table for LLDP

Event	Activity of the local LLDP agent	Response of neighboring LLDP agent
Activate LLDP agent or device startup	Transmit LLDPDUs to all ports	Include sender in the list of neighbors
De-activate LLDP agent or software reset	Transmit LLDPDUs with a TTL value of 0 seconds to all ports	Delete sender from the list of neighbors
Link up	Send port-specific LLDPDUs	Include sender in the list of neighbors
Link down	Delete all neighbors for this port	–
Timer (Message Transmit Interval)	Cyclic transmission of LLDPDUs to all ports	Update information
Aging (TTL)	Delete all neighbor information	–
Receiving an LLDPDU from a new neighbor	Extend list of neighbors	–

Configuration options are displayed on the “Switch Station/Diagnostics/LLDP General” page.

Figure 5-23 “Link Layer Discovery Protocol” page

- **LLDP Status:** Click the “Enable” or “Disable” radio button to enable or disable LLDP.
- **LLDP Mode:** Click either the “Default (IEEE)” radio button, or the “Profinet” or “NMS” radio button. PNIO PortStatus and PNIO Chassis MAC are included by default in the LLDP message content when PROFINET mode is enabled. When network management software (NMS) operation is selected, the LLDP port ID subtype is changed from “Locally Assigned” to “Interface Name” and the port IDs are transmitted with a fixed designation. For example, “fen” (fast Ethernet 100 Mbps) where *n* is the port number. Some network management software packages require a specific LLDP data format.



The system name of the switch must only consist of the characters “a...z”, “0...9” and “-”. Do not use upper-case letters.

- **Message TTL Multiplier:** This value is multiplied by the Message Transmit Interval to determine the time a neighbor will consider the entry to be valid. The range is 2 to 10 with a default of 4.
- **Message Transmit Interval:** The range is 5 to 32768 seconds. Five is the default.
- **Global TLV Settings LLDP Optional Message Content:** The Type Length Value (TLV) settings determine which types of LLDP data (optional message content) will be sent by the switch. Use the check boxes to select the LLDP message content. The default is all message content checked.
- **Submit:** Click the “Submit” button to save the settings to volatile memory (see “Configuration management” on page 59).

5.5.11 LLDP topology

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

The information that is collected is presented in the LLDP Topology table in web-based management. The table includes the port numbers that are used to connect both devices, as well as the management (IP) address, the chassis ID (MAC address) or device system name of neighboring devices, and the device icon, if available.

5.5.11.1 Default (IEEE) mode

The “LLDP Topology” page displays the local switch’s port number and the addresses of the neighboring devices connected to that port, as well as the port number of the connected neighbor.

Topology information is displayed on the “Switch Station/Diagnostics/LLDP Topology” page.

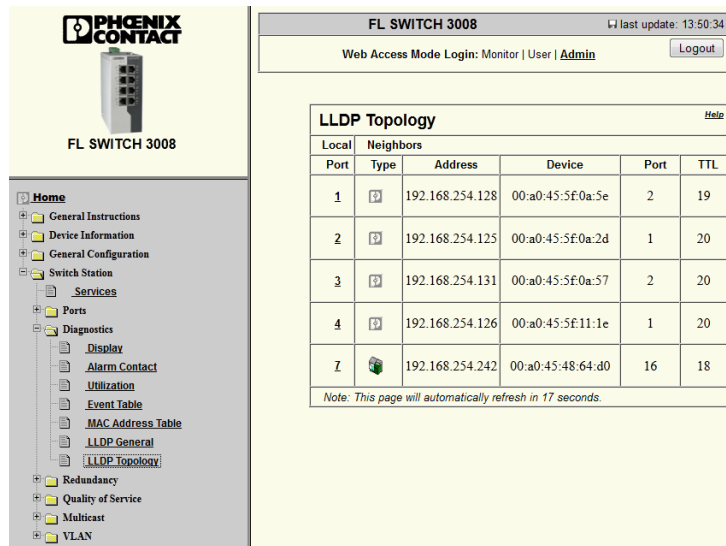


Figure 5-24 “LLDP Topology” page in IEEE mode

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

- **Local port:** Contains the port number of the local switch used to connect a neighbor to this switch. The port number is also a link to the local “Port Configuration” page.
- **Type:** An icon is displayed here that corresponds to the neighboring device type. **Ethernet Device** is displayed in general for devices produced by other manufacturers.
- **Address:** Indicates the management IP address for the neighbor. The “Management Address” check box (IP address) must be selected to display the ID. Otherwise, **0.0.0.0** is displayed.
- **Device:** Indicates the chassis ID (MAC address) of the neighbor.
- **Port:** Indicates the port number of the neighboring switch.
- **TTL:** Time to live value. Indicates how long the neighbor information is valid.



The “Message Time To Live” field is determined by multiplying the message transmit interval with the message transmit hold multiplier. The default value is 4.

5.5.11.2 PROFINET mode

The “LLDP Topology” page displays the local switch’s port number and the addresses of the neighboring devices connected to that port, as well as the port number of the connected neighbor.

Topology information is displayed on the “Switch Station/Diagnostics/LLDP Topology” page.

The screenshot shows the web interface for a Phoenix Contact FL SWITCH 3008. The main content area displays the "LLDP Topology" page, which includes a table of neighboring devices. The table has columns for Local Port, Type, Address, Device, Port, and TTL. The data is as follows:

Local Port	Type	Address	Device	Port	TTL
1	[Icon]	10.250.133.110	switch	port-001	16
2	[Icon]	10.250.133.100	rfc-470-pn-24-08-a6	port-001	18
3	[Icon]	10.250.133.131	axl-bk1	port-001	16
4	[Icon]	10.250.133.132	axl-bk2	port-002	17
5	[Icon]	10.250.133.133	il-bk3	port-001	115
6	[Icon]	10.250.133.134	il-bk4	port-002	20

Note: This page will automatically refresh in 9 seconds.

Figure 5-25 “LLDP Topology” page in PROFINET mode

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

- **Local port:** Contains the port number of the local switch used to connect a neighbor to this switch. The port number is also a link to the local “Port Configuration” page.
- **Type:** An icon is displayed here that corresponds to the neighboring device type. **Ethernet Device** is displayed in general for devices produced by other manufacturers.
- **Address:** Indicates the management IP address for the neighbor. The “Management Address” check box (IP address) must be selected to display the ID. Otherwise, **0.0.0.0** is displayed.
- **Device:** Indicates the device system name of the neighbor.
- **Port:** Indicates the port number of the neighboring switch.
- **TTL:** Time to live value. Indicates how long the neighbor information is valid.



The “Message Time To Live” field is determined by multiplying the message transmit interval with the message transmit hold multiplier. The default value is four.

5.6 Redundancy

IEEE-based redundancy protocols **Spanning Tree Protocol (STP)**, **Rapid Spanning Tree Protocol (RSTP)**, **Multiple Spanning Tree (MST)** and the proprietary **extended ring** protocol can be selected as the redundancy mechanisms. Please note the different configuration and topology requirements.

The 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 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 communication is interrupted. The meshed structure is replaced by a logical, deterministic path with a tree structure without loops using the spanning tree algorithm. In the event of data path failure, some of the previously disconnected connections are reconnected to ensure uninterrupted network operation.

RSTP (IEEE 802.1w) is a standardized method that enables the use of Ethernet networks with redundant data paths and prevents the long timer-controlled switch-over times of STP.

If RSTP is operated using the default values, it is suitable for up to seven switches along the relevant path. RSTP/STP/MST may all be simultaneously used in the same switch. They operate independently of one another with topology changes in one completely isolated from the other. The mix of RSTP and extended ring protocols allows redundant connections to higher-level IT-compatible networks and lower-level time-critical control networks.

In order to configure and manage an RSTP network, several pages must be considered.

For most applications, the use of RSTP with default parameters will be sufficient. In this case, the following pages are all that need to be considered:

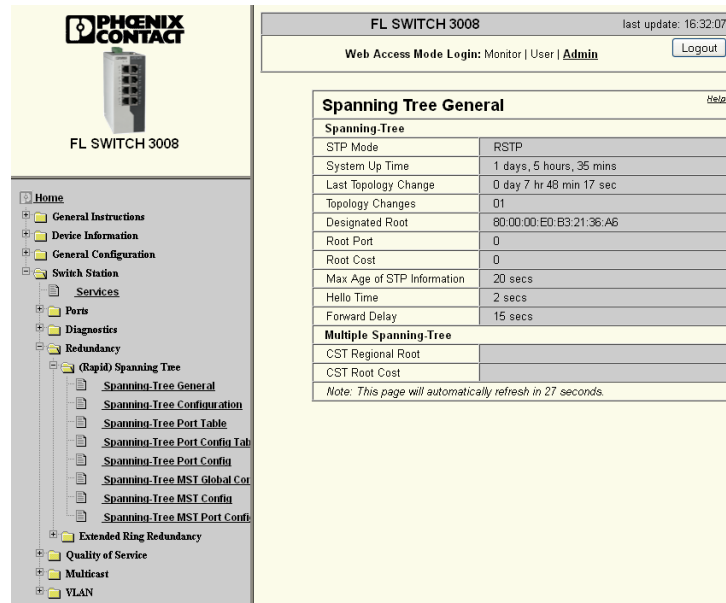
- The “Spanning Tree General” page displays the overall diagnostic status of RSTP/STP (and MST).
- The “Spanning Tree Configuration” page enables RSTP, STP (or MSTP), allowing one to manually set this as the root switch, and contains optional system-wide timing parameters.

For advanced applications, the following pages need to be considered:

- The “Spanning Tree Port Table” page is a diagnostic status display that shows the RSTP/STP status of all the ports on the switch.
- The “Spanning Tree Port Config Table” page allows viewing and configuration of the major RSTP/STP parameters for all ports in the switch.
- The “Spanning Tree Port Config” page allows viewing and configuration of all RSTP/STP parameters for one port at a time. This page also forces the use of STP (or RSTP) instead of the normal IEEE progression of first attempting RSTP before falling back to STP.

5.6.1 Spanning tree general

The “Spanning Tree General” page displays the overall diagnostic status of RSTP/STP (and MST). General STP settings can be viewed from the “Switch Station/Redundancy/(Rapid) Spanning Tree/Spanning-Tree General” page.



The screenshot shows the web interface for FL SWITCH 3008. The main content area displays the 'Spanning Tree General' configuration page. The page includes a table with the following data:

Spanning Tree	
STP Mode	RSTP
System Up Time	1 days, 5 hours, 35 mins
Last Topology Change	0 day 7 hr 48 min 17 sec
Topology Changes	01
Designated Root	80:00:00:E0:B3:21:36:A6
Root Port	0
Root Cost	0
Max Age of STP Information	20 secs
Hello Time	2 secs
Forward Delay	15 secs
Multiple Spanning-Tree	
CST Regional Root	
CST Root Cost	

Note: This page will automatically refresh in 27 seconds.

Figure 5-26 “Spanning Tree General” page

- **STP Mode:** The currently enabled STP mode (RSTP or MSTP).
- **System Up Time:** The time between the last switch reboot and the last page refresh.
- **Last Topology Change:** The time since the last spanning tree topology change and the last page refresh.
- **Topology Changes:** The number of times the STP topology has converged since this switch’s last reboot.
- **Designated Root:** The root bridge for this spanning tree.
- **Root Port:** The lowest cost path from this bridge to the root bridge.
- **Root Cost:** Indicates the path cost of this segment to the root bridge.
- **Max Age of STP Information:** This is the time the bridge should wait after hearing its last bridge protocol data unit (BPDU) before it attempts to change the spanning-tree topology. Acceptable values are between 6 and 40 seconds. This value is usually set 10 times the hello time.
- **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” (twice the forward delay).
- **CST Regional Root (Common Spanning Tree Regional Root):** In MSTP, the root of a region within the common internal spanning tree.
- **CST Root Cost:** The path cost from this bridge to the regional root.

5.6.2 Configuring RSTP

RSTP is used to implement network topologies with redundant paths and is an official IEEE standard (802.1D-2004).

Start-up 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 redundant topology.

The “Spanning Tree Configuration” page enables RSTP, STP (or MSTP), allowing one to manually set this as the root switch, and contains optional system-wide timing parameters. When using more than one virtual LAN (VLAN) in a network, the MSTP redundancy mechanism defined in IEEE 802.1Q-2005 is also supported.

The Spanning Tree variants can be selected and activated from the “Switch Station/Redundancy/(Rapid) Spanning Tree/Spanning-Tree Configuration” page.

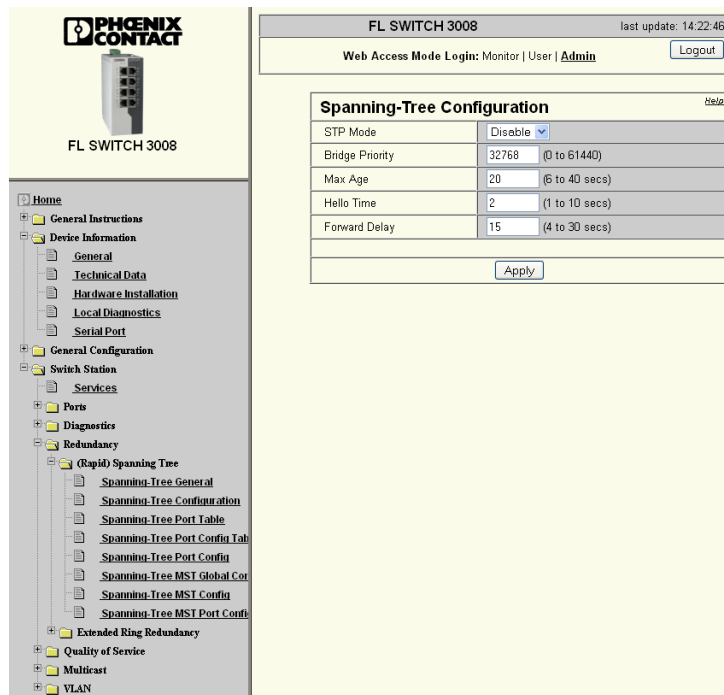


Figure 5-27 “Spanning-Tree Config” page

It is sufficient to set the RSTP status to “Enable” in order to start RSTP using default settings. Priority values can be specified for the switch. The bridge and backup root can be specified via these priority values. Only multiples of 4096 are permitted. The desired value can be entered in the “Bridge Priority” field. The value will be rounded automatically to the next multiple of 4096.

- **Max Age:** The maximum age of STP information parameter is set by the root switch and is used by all switches in the topology. The parameter is set to make sure that each switch in the network has a constant value against which the age of the saved configuration is tested.

The “Max Age”, “Hello Time” and “Forward Delay” fields have the same meaning for STP. These values are used when this switch becomes a root.

- **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” (twice the forward delay).



The “Max Age”, “Hello Time” and “Forward Delay” parameters are optimized by default. They should only be modified by qualified personnel.

- **Apply:** Click the “Apply” button to save the settings to volatile memory (see “Configuration management” on page 59).

5.6.3 Spanning tree port table

Spanning tree diagnostic status showing the RSTP/STP role of all the ports on the switch can be viewed in a non-editable table format from the “Switch Station/Redundancy/(Rapid) Spanning Tree/Spanning-Tree Port Table” page.

The screenshot shows the Phoenix Contact web interface for an FL SWITCH 3008. The main content area displays the "STP Port Table" for MST ID CIST-ID 0. The table has 5 columns: Port, Operational Edge Port, Protocol, STP State, and STP Role. All 8 ports listed have "no edge port" in the Operational Edge Port column, "Disable" in the Protocol and STP State columns, and "Disable" in the STP Role column. A note at the bottom of the table states: "Note: This page will automatically refresh in 19 seconds."

Port	Operational Edge Port	Protocol	STP State	STP Role
1	no edge port	Disable	Disable	Disable
2	no edge port	Disable	Disable	Disable
3	no edge port	Disable	Disable	Disable
4	no edge port	Disable	Disable	Disable
5	no edge port	Disable	Disable	Disable
6	no edge port	Disable	Disable	Disable
7	no edge port	Disable	Disable	Disable
8	no edge port	Disable	Disable	Disable

Figure 5-28 “STP Port Table” page

- **MST ID:** When the MST function is used, select the “CIST ID” number from the drop-down menu.

The basic information for each port is displayed in a table format. The first column indicates the port with successive columns providing the status of Operational Edge Port, Protocol, STP State and STP Role. Click the port number in the first column to go to the individual STP port configuration page (see “STP port configuration” on page 97).

5.6.4 Spanning tree port configuration table

The spanning tree settings for each port on the switch can be edited in a table format from the “Switch Station/Redundancy/(Rapid) Spanning Tree/Spanning-Tree Port Config Table” page.

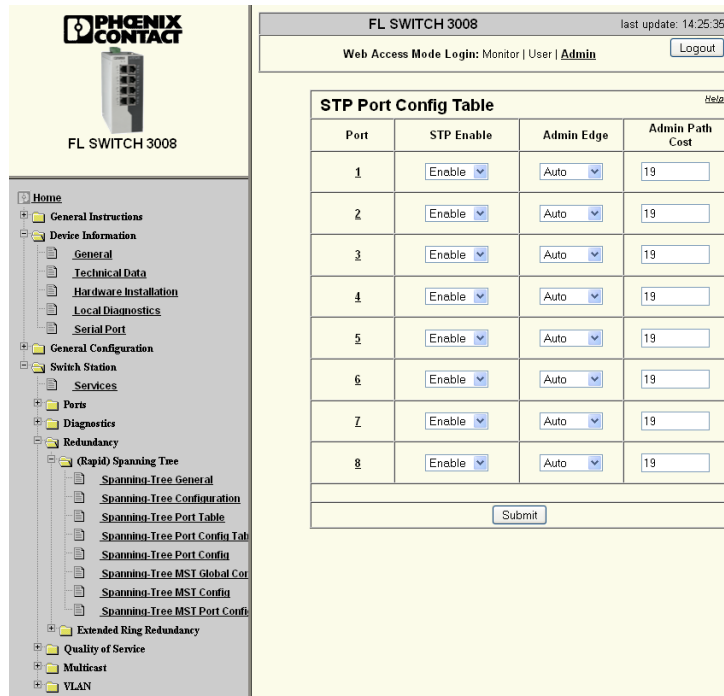


Figure 5-29 “STP Port Config Table” page

The basic information for each port is displayed in a table format. The first column indicates the port with successive columns providing the status of Operational Edge Port, Protocol, STP State and STP Role.

- **Port:** Click the port number in the first column to go to the individual STP port configuration page (see “STP port configuration” on page 97).
- **STP Enable:** Select “Enable” or “Disable” from the drop-down menu to enable or disable STP redundancy control for the port.
- **Admin Edge Port:** From the drop-down menu, select “Enable”, “Disable” or “Auto Edge Port”. The “Auto Edge Port” option allows the switch to automatically detect whether the port is operating as an edge port (an end device is connected to the port).
- **Admin Path Cost:** Enter the maximum path cost value for the selected port. Path costs are based on IEEE 802.1D. Table 5-2 provides the value entered in the field and the corresponding maximum transfer rate.

5.6.5 STP port configuration

The “Spanning Tree Port Config” page allows viewing and configuration of all RSTP/STP parameters for one port at a time. This page also forces the use of STP (or RSTP) instead of the normal IEEE progression of first attempting RSTP before falling back to STP.

Individual ports can be configured with STP from the “Switch Station/Redundancy/(Rapid) Spanning Tree/Spanning-Tree Port Config” page.

The screenshot shows the web interface for a Phoenix Contact FL SWITCH 3008. The main content area is titled "STP Port Config" and contains a table of configuration parameters for port-1. The parameters include Port Number, Port Name, STP Port State, STP Role, STP Enable, Operational Edge Port, Admin Edge Port, Priority, Admin Path Cost, Path Cost, Forward Transitions, Designated Root, Designated Bridge, Designated Port ID, and Designated Cost. Below the table are buttons for "Apply" and "Force RSTP". A "Protocol Compatibility" section shows "Port Mode" as "Port is in the Spanning Tree mode." At the bottom, it indicates "Port Configuration of Port 1: General | Security | (R)STP | VLAN".

STP Port Config	
Port Number	port-1
Port Name	Port 1
STP Port State	STP disabled
STP Role	Forwarding
STP Enable	Enable
Operational Edge Port	Not operating as an edge port
Admin Edge Port	Auto Edge Port
Priority	128 (0 to 240)
Admin Path Cost	19 (0 to 20000000, 0 = Auto)
Path Cost	19
Forward Transitions	1
Designated Root	00:00:00:E0:B3:21:36:A6
Designated Bridge	00:00:00:E0:B3:21:36:A6
Designated Port ID	80:01
Designated Cost	0
<input type="button" value="Apply"/> <input type="button" value="Force RSTP"/>	
Protocol Compatibility	
Port Mode	Port is in the Spanning Tree mode.
Port Configuration of Port 1: General Security (R)STP VLAN	

Figure 5-30 “STP Port Config” page

- **Port:** Select the desired port from the drop-down menu.
- **STP Port State:** Specifies the port’s spanning tree state:
 - **Forwarding:** The port is integrated in the active topology and forwards data.
 - **Discarding:** This port does not take part in data transmission.
 - **Learning:** This port does not take part in data transmission of the active topology; however, MAC addresses are learned.
 - **Blocking/discarding:** The port has a link but has not been set to the “Discarding” state by RSTP.
- **STP Role:** Specifies this port’s role in the spanning tree topology:
 - **Disabled:** The port is disabled.
 - **Root:** The port is the lowest cost to the root.
 - **Designated:** The port is forwarding.
 - **Blocking:** The port does not take part in data transmission.
 - **Alternate:** The port is the backup in the event of failure of the main port.
- **STP Enable:** Select “Enable” or “Disable” from the drop-down menu to enable or disable STP redundancy on this port.

- **Operational Edge Port:** Displays if the port is an edge port or not. All ports that do not receive any (R)STP BPDUs, such as termination device ports, become edge ports, i.e., ports that go to the “Forwarding” state immediately after restart.
- **Admin Edge Port:** From the drop-down menu, select “Enable”, “Disable” or “Auto Edge Port”. The “Auto Edge Port” option allows the switch to automatically detect if the port is operating as an edge port (an end device is connected to the port).
- **Priority:** Sets the priority for this port (default 128). Due to backward compatibility with STP, priority values can be set that are not configurable in RSTP.
- **Admin Path Cost:** Allows the setting of a maximum path cost for the selected port. Path costs are based on IEEE 802.1D. Table 5-2 provides the value entered in the field and the corresponding maximum transfer rate.

Table 5-2 Path costs

Value	Maximum speed
2 000 000	10 Mbps
200 000	100 Mbps
20 000	1 Gbps

- **Path Cost:** Displays the calculated path cost.
- **Forward Transitions:** Displays how often the port switches from the “Discarding” state to the “Forwarding” state. Additional parameters provide information about network paths in a stable topology that are used by the BPDU telegrams.
- **Designated Root:** Displays the MAC address of the root switch (bridge) for this spanning tree.
- **Designated Bridge:** Displays the MAC address of the switch that has the lowest path cost to the root switch.
- **Designated Port ID:** Indicates the port priority and port number from which the BPDUs are sent from the designated switch (bridge). The first two digits (**80** in Figure 5-30) are the HEX representation of the port priority (80 HEX = 128 = default port priority). The third and fourth digits (**01** in Figure 5-30) indicate port number.
- **Designated Cost:** Displays the path cost of this segment to the root switch.
- **Protocol Compatibility/Port Mode:** Displays the spanning tree protocol active on the port.
- **Apply:** Click the “Apply” button to save the settings to volatile memory (see “Configuration management” on page 59).
- **Force RSTP:** The IEEE function automatically tries RSTP first, then reverts to an STP mode if there is an RSTP problem. This toggle button allows manually forcing RSTP or STP operation. For known RSTP or STP operation, this saves reaction time by eliminating the automatic discovery timing.

5.6.6 MST

The STP and RSTP redundancy protocols solve most industrial applications. However, in more advanced and large applications with extensive VLAN usage, it is important to better manage how RSTP and VLANs interact. With standard RSTP, the redundancy recovery mechanism can span multiple VLANs. A change in one VLAN area can cause a topology change in another VLAN area.

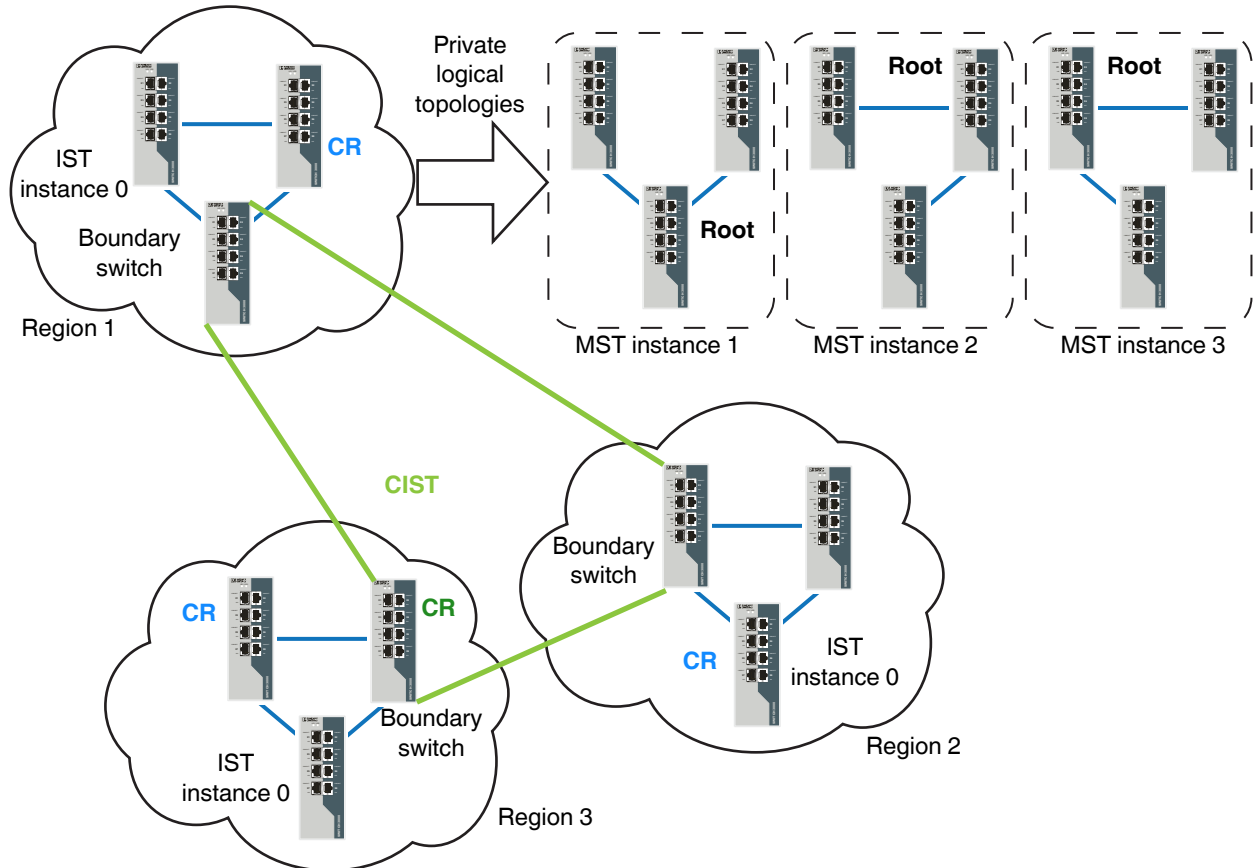


Figure 5-31 MSTP example network

Multiple Spanning Tree Protocol (MSTP) allows the user to define regions where the redundancy recovery approach is isolated to the regions. A region can consist of one or more VLANs. Within a region, the network engineer can also define different normal topologies, therefore balancing the traffic within the region based on which switch is the root. Each different root definition, and resulting steady state topology, is called an MST “instance” (MSTI). To ensure redundant communication between regions, a **Common Internal Spanning Tree (CIST)** is formed (a spanning tree that connects all the regional spanning trees) by identifying boundary switches for each region. The different regions are interconnected by these boundary switches.

The configuration of MST is accomplished on three levels or steps:

- The first step is to globally configure the switch, defining the different regions (see “MST Global Config” on page 100).

- The second step is to allow the individual MST regions to access the different switches (see “MST Config” on page 101).
- The third step involves configuring individual ports to optimize the performance of the recovery in the event of a “break” (see “MST Port Config” on page 102).

5.6.7 MST Global Config

Configure the region from the “Switch Station/Redundancy/Spanning-Tree MST Global Config” page.

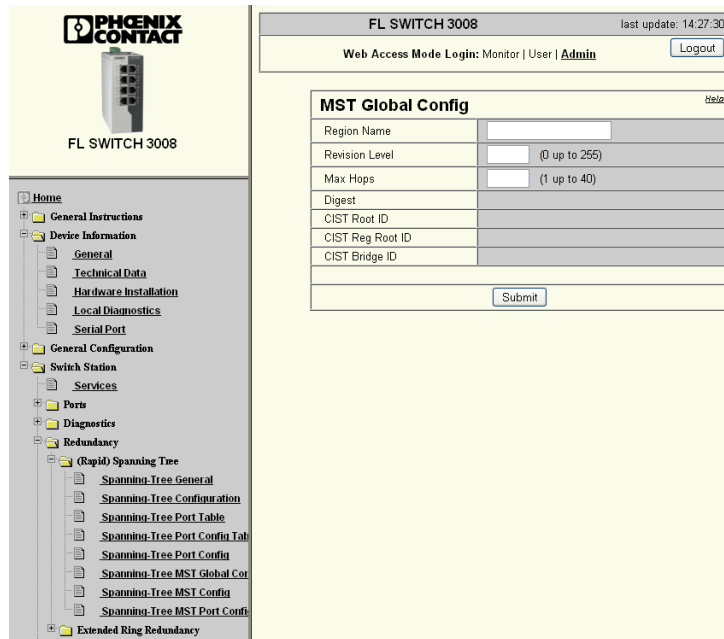


Figure 5-32 “MST Global Config” page

- **Region Name:** The name of the region. A region is a physical group of switches that can be partitioned into a logical topology. This is the first of three parameters that must match in order for a switch to be part of the same region.
- **Revision Level:** The revision number of the MSTP configuration. An integer value. This is the second of three parameters that must match in order for a switch to be part of the same region.
- **Max Hops:** The value used by the IST root to set the Remaining Hops parameter in its BPDUs.
- **Digest:** A hash value calculated from VLAN to MST instance mappings that are used to detect errors in said mappings.
- **CIST Root ID (Common Internal Spanning Tree Root Identifier):** The root of the common internal spanning tree.
- **CIST Reg Root ID (CIST Regional Root ID):** The root of a region within the common internal spanning tree.
- **CIST Bridge ID:** Comprised of the bridge priority and MAC address, the lowest CIST Bridge ID determines the CIST Root ID.
- **Submit:** Click the “Submit” button to save the settings to volatile memory (see “Configuration management” on page 59).

5.6.8 MST Config

Configure the MST from the “Switch Station/Redundancy/Spanning-Tree Global Config” page.

The screenshot shows the web interface for an FL SWITCH 3008. The top header includes the Phoenix Contact logo and the device name. Below the logo is a navigation tree with categories like Home, General Instructions, Device Information, General Configuration, Switch Station, Services, Ports, Diagnostics, and Redundancy. The 'Redundancy' section is expanded to show '(Rapid) Spanning Tree' options, including 'Spanning-Tree General', 'Spanning-Tree Configuration', 'Spanning-Tree Port Table', 'Spanning-Tree Port Config Tab', 'Spanning-Tree Port Config', 'Spanning-Tree MST Global Cor', 'Spanning-Tree MST Config', and 'Spanning-Tree MST Port Config'. The 'Spanning-Tree MST Config' option is selected, leading to the 'MST Config' page. The page title is 'FL SWITCH 3008' with a 'last update: 14:26:24' timestamp. Below the title is a 'Web Access Mode Login: Monitor | User | Admin' with a 'Logout' button. The main content area is titled 'MST Config' and contains a form with the following fields: 'MST Instance Number' with a dropdown menu set to 'Create'; 'MST Instance ID' with a text input field and a range indicator '(1 to 15)'; and 'VLAN ID' with a list box. An 'Apply' button is located at the bottom of the form.

Figure 5-33 “MST Config” page

- **MST Instance Number:** From the drop-down menu, select “Create”, “View” or “Configure” an MST instance.
- **MST Instance ID:** Enter a unique number to identify an instance (or logical topology) within a region. MST ID 0 represents the IST by default, so only values 1 through 15 are assignable.
- **VLAN ID:** This displays the VLANs associated with the MSTI.
- **Apply:** Click the “Apply” button to save the settings to volatile memory (see “Configuration management” on page 59).

5.6.9 MST Port Config

Configure the MST ports from the “Switch Station/Redundancy/Spanning-Tree Global Config” page.

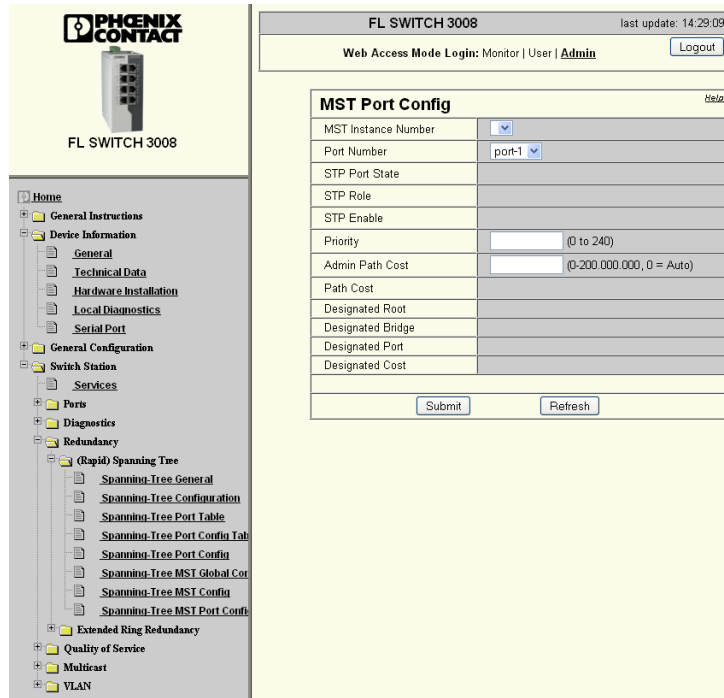


Figure 5-34 “MST Port Config” page

- **MST Instance Number:** Create, view or configure an MSTI.
- **Port Number:** Select a port to view or configure within the MSTI.
- **STP Port State:** The port’s STP state within the MSTI.
- **STP Role:** The port’s role within the MSTI.
- **STP Enable:** The STP status of the MSTI.
- **Priority:** The priority of the port within the MSTI.
- **Admin Path Cost:** The administratively assigned path cost associated with this port within the MSTI.
- **Path Cost:** The calculated path cost of this port within the MSTI.
- **Designated Root:** Displays the root bridge MAC address.
- **Designated Bridge:** Displays the MAC address of the bridge that provides the minimum root path cost.
- **Designated Port:** Displays the port that connects this switch to the designated bridge.
- **Designated Cost:** Displays the cost from this bridge to the root bridge.
- **Submit:** Click the “Submit” button to save the settings to volatile memory (see “Configuration management” on page 59).
- **Refresh:** Click the “Refresh” button to update the data displayed on the page.

5.6.10 Extended ring redundancy

The extended ring redundancy is a proprietary Phoenix Contact protocol for critical industrial and infrastructure applications where faster recovery times than IEEE standard RSTP/STP are required. The extended ring has the following characteristics:

- **Large capacity:** Up to 200 switches in a single ring, and multiple coupled-ring topologies containing more than 300 switches are possible.
- **Fast recovery times:** 15 ms recovery times for 200 devices on a ring (18 ms when using 1000 Mbps SFP modules) and 17 ms for ring-to-ring coupling.
- **Easy setup:** Simply define which ports are used for the ring function, and then enable the function.
- **Flexible application layouts:** Dual homing, redundant ring-to-ring coupling and daisy chaining with ring combinations are all possible.

Extended ring concepts

Extended ring redundancy encompasses several functional components. These components are a combination of the physical topology and the configuration settings of the switch.

- **Ring:** This function allows the creation of a single, basic ring of switches. It is the simplest and most widely used redundancy topology.
- **Coupling:** This function allows two or three rings to be connected together. It provides redundancy for larger or geographically distributed applications.
- **Dual ring:** This function allows a second, redundant ring to be added around an existing ring. The same switches then have two rings passing between them, providing a higher level of fault tolerance to the application.
 - The second ring is called the “redundant ring”. To implement a dual ring redundancy topology, both the ring and redundant ring settings must be configured.
 - The coupling function may also be used to connect multiple dual rings.
- **Path control:** Normally the primary and backup extended ring path is determined by the switch and is not predictable. Path control defines a single location in a ring where the preferred blocking port will be located. After power up, or after a broken ring is recovered from a fault, the blocked port will be at the user-defined location. In applications where mixed link speeds, media types, or a preferred topology is desired, this feature gives the user the ability to define the backup link location and desired primary path.

5.6.10.1 Operation overview

Ring ports are used to connect the switch to the ring. Ring coupling ports connect a ring to another ring. These ports must be selected and configured before connecting switches.

Upon power up, the switches automatically choose the “last switch in the ring” as the last switch that powers up. This last switch then blocks a ring port and sends out packets to determine the health of the ring.

Each switch in the ring monitors the status of its ring ports. Upon a ring link failure, the adjacent switches send a “link down” message out on the ring to the last switch, which unblocks the previously blocked port.

Extended ring ports cannot be mirrored by the Port Mirroring function.

Once the failed link is repaired, it continues to be the blocked port.

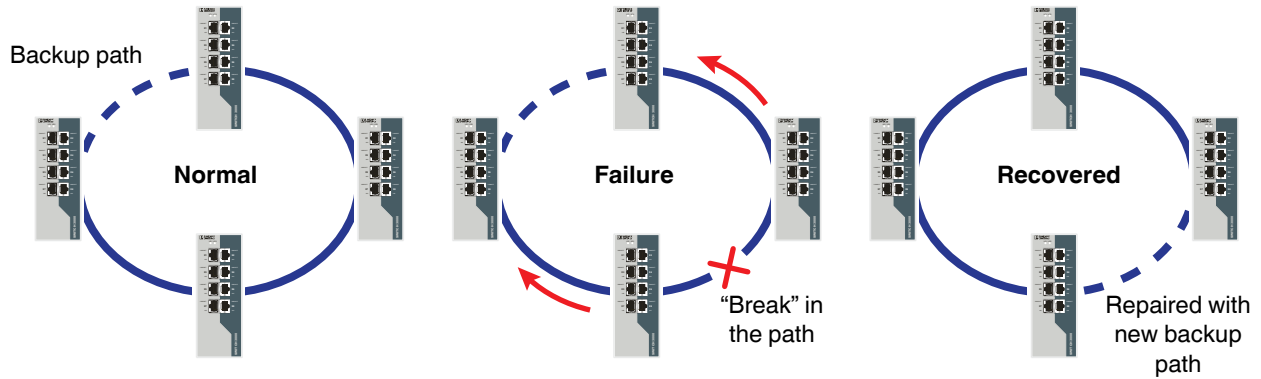


Figure 5-35 Ring restructure process

5.6.10.2 Ring layout guidelines

There are five main rules for laying out an extended ring system.

- There is a maximum of 200 switches per ring.

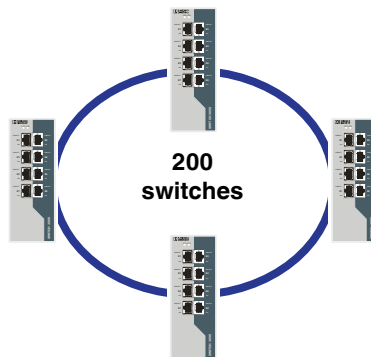


Figure 5-36 Basic ring

- A maximum of two coupling ports can be active in any one ring. The coupling ports may be on the same switch or split between two switches.

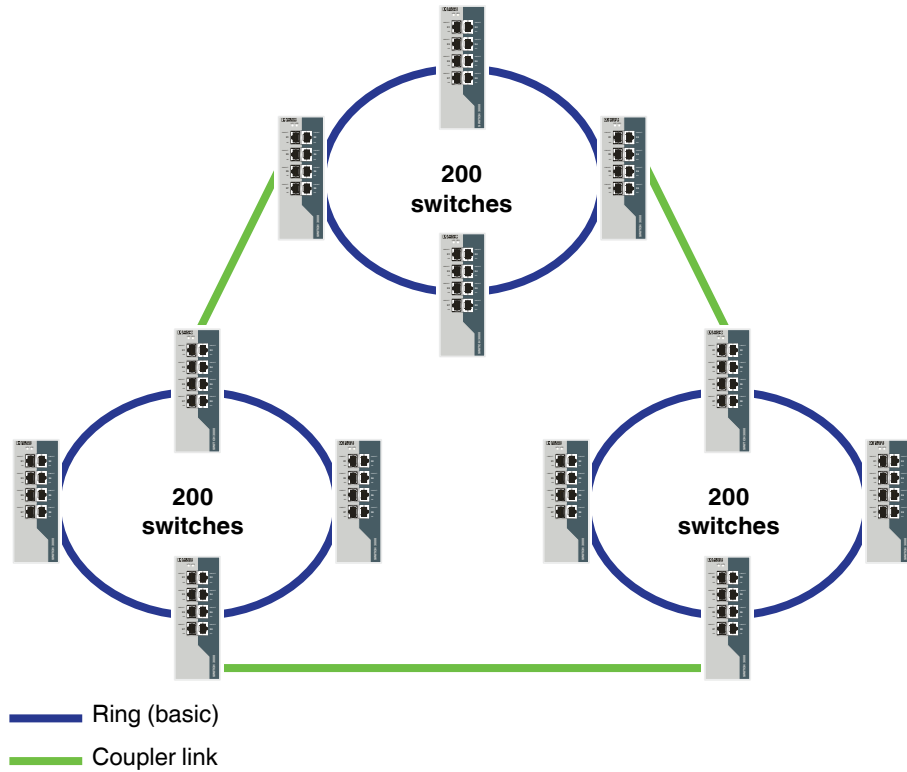


Figure 5-37 Extended ring made from three single rings

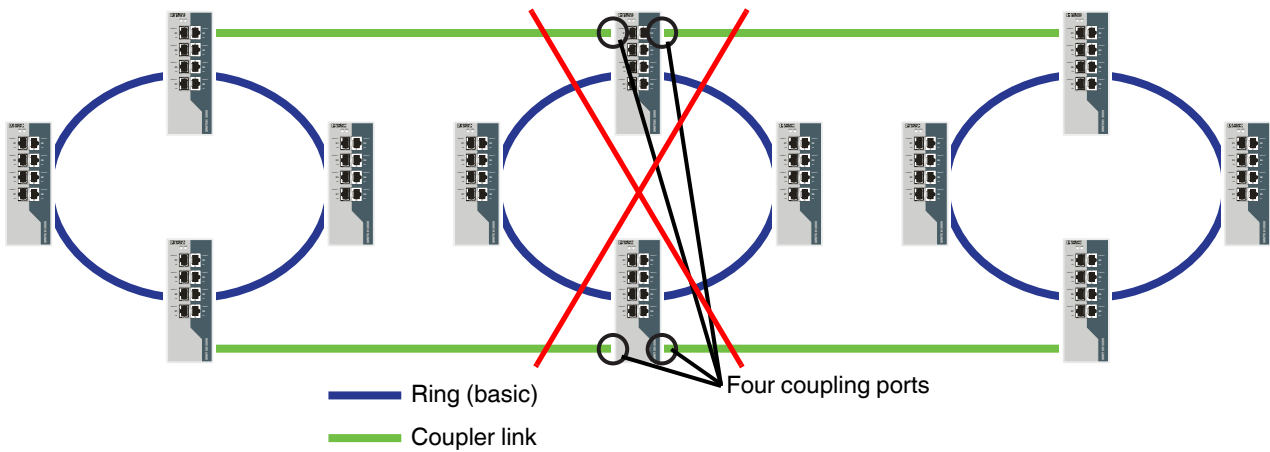


Figure 5-38 Incorrect extended ring structure with four coupling ports

- The ring coupling path may contain a daisy chain of switches. A maximum of 134 switches may be daisy chained on any single ring-to-ring coupling path.

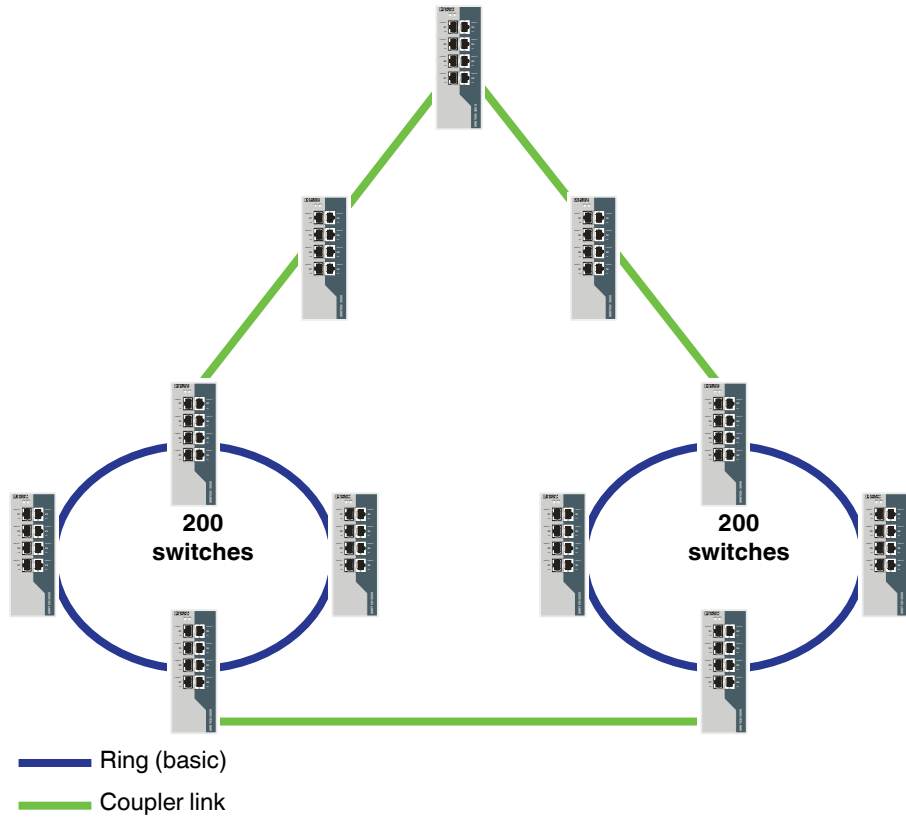


Figure 5-39 Two-ring extended ring coupling path with additional switches

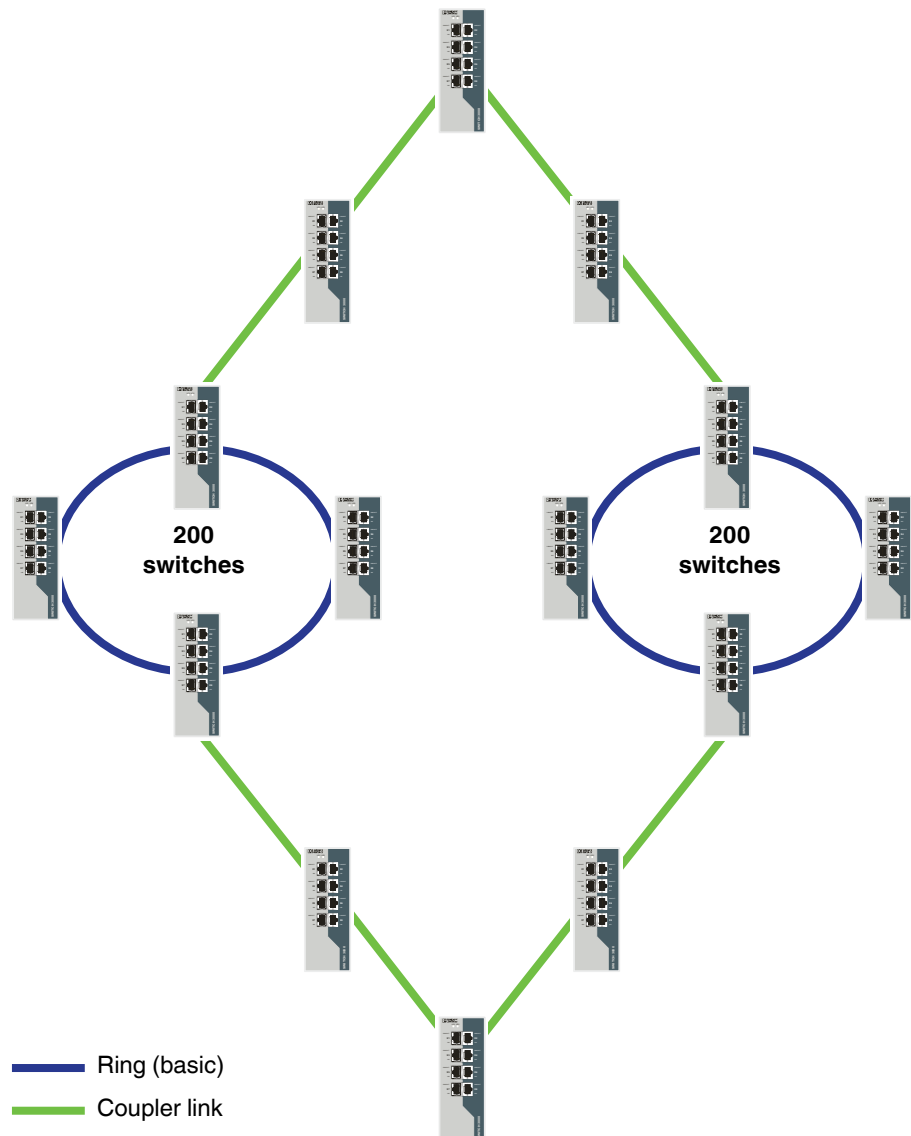


Figure 5-40 Extended ring coupling path example

- No other devices are allowed to be inserted into the switch-to-switch ring connections. Only switch ports configured for extended ring redundancy may be connected to a switch's active ring ports.
When daisy chaining a switch in a coupler link, two ring ports must still be specified. The unused ring port must remain unconnected.

- Coupling may be used where two rings are joined by a single switch.

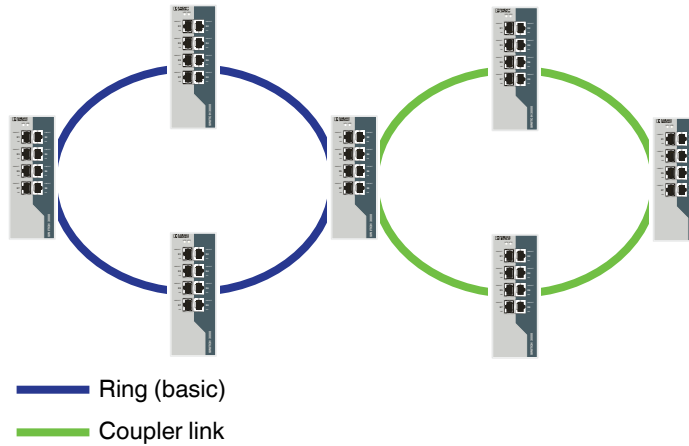


Figure 5-41 Joining rings with a single switch

5.6.10.3 Dual ring

Dual ring requires the configuration of a paired ring.

Dual ring capability is for the most critical applications where the highest levels of fault tolerance are needed. Each switch may be connected by dual redundant rings so that multiple cable breaks may occur without compromising communications to all switches.

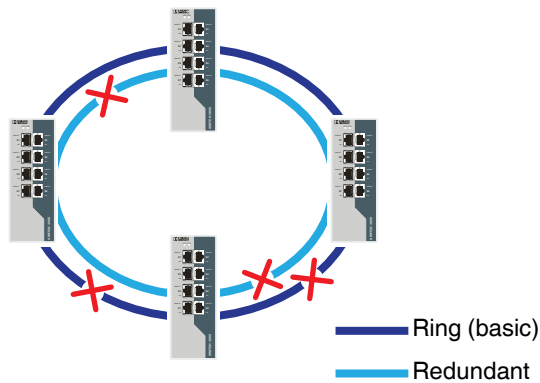


Figure 5-42 Dual ring topology

Each link is individually redundant to maximize availability. Similar to a single ring, when a broken link is repaired it becomes the new backup link.

Application flexibility

When the dual ring function is combined with the coupling function, layouts that include a higher level supervisory control network and distributed "field" networks can be created.

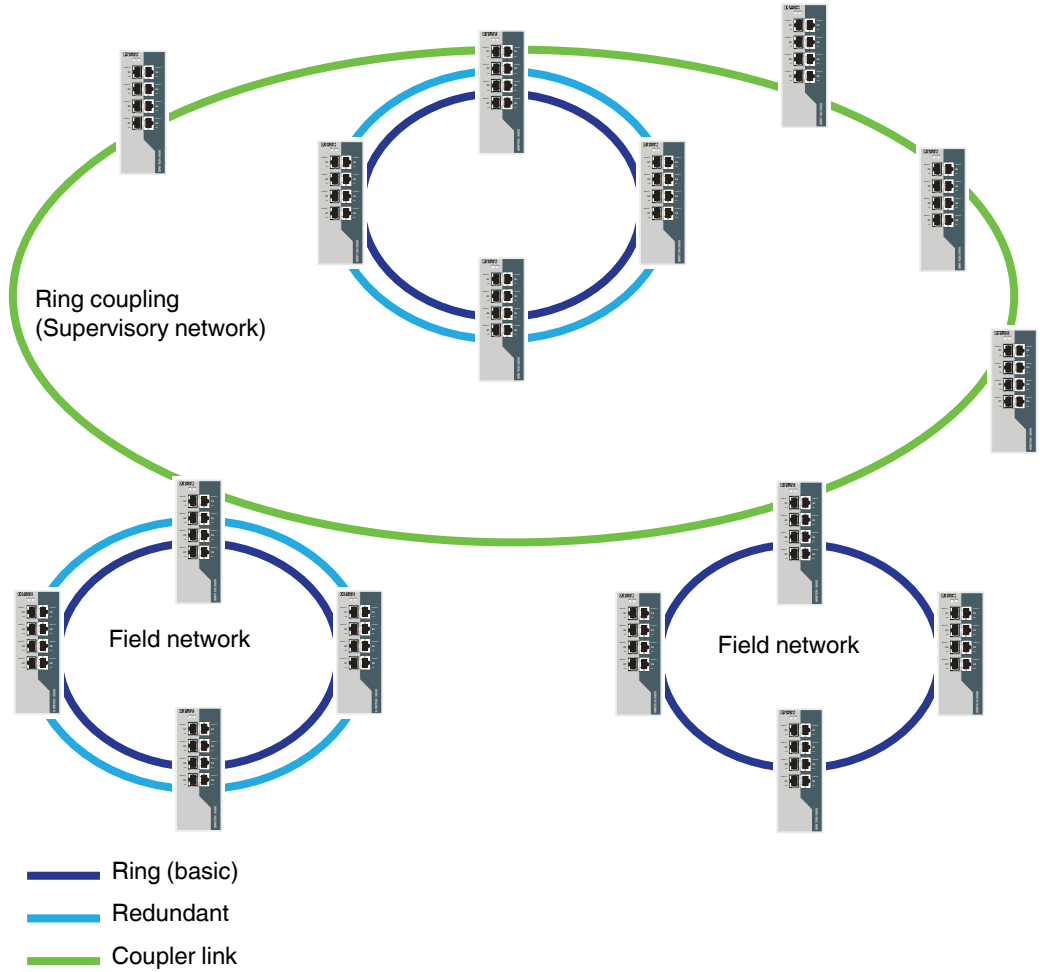


Figure 5-43 Supervisory and field networks

Application guidelines

- Dual ring cannot be used to couple switches with other rings. Only ring coupling can do this.
- Redundant ring cannot back up a coupling link.

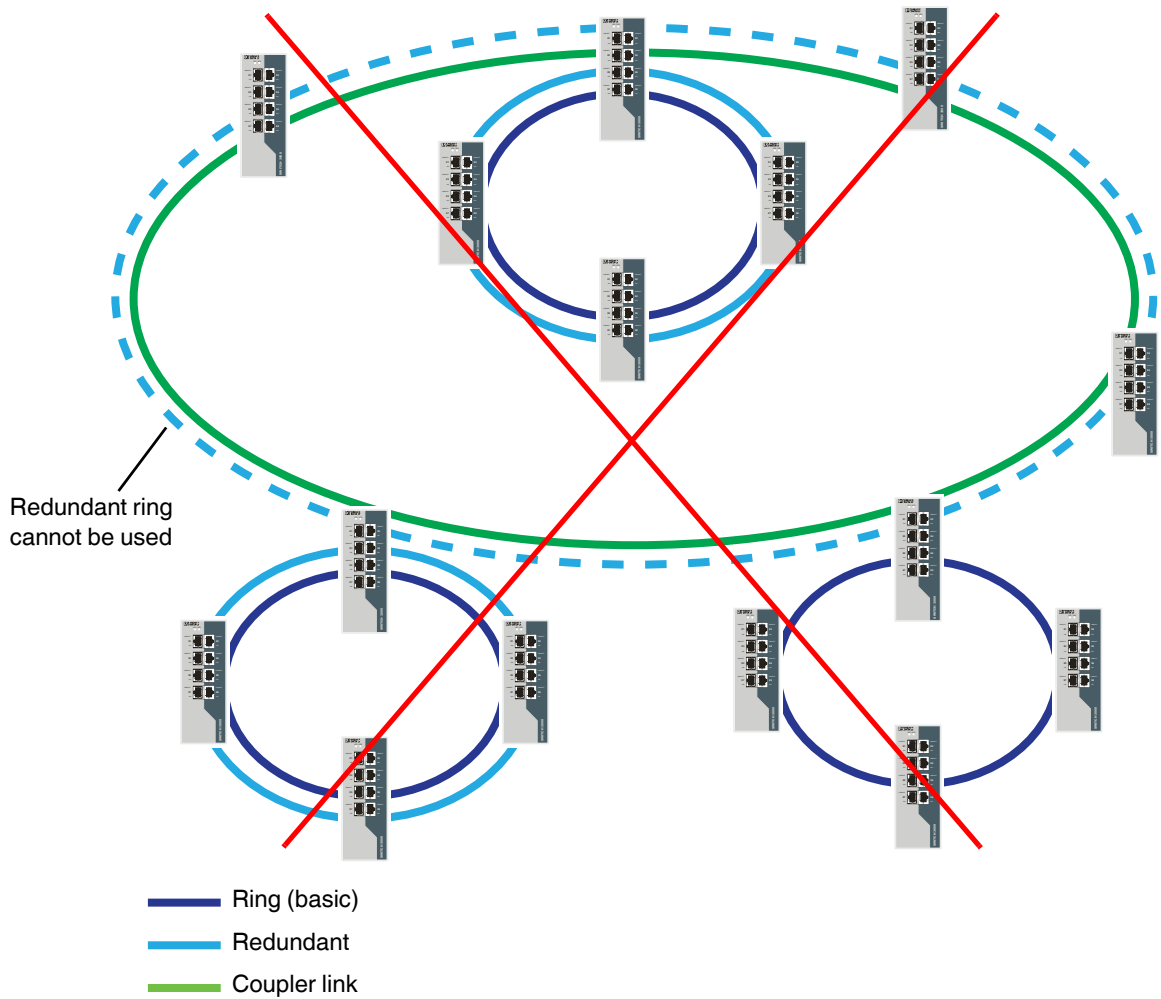


Figure 5-44 Improper use of redundant ring

5.6.10.4 Configuration

The “Extended Ring” page is divided into three groups.



The redundant ring section applies only to firmware version 1.2 and above.

Configure the extended ring redundancy from the “Switch Station/Redundancy/Extended Ring” page.

Extended Ring <small>Help</small>		
Ring state	enable ▾	
Set Ring port	Ring port1	Ring port 2
	1 ▾	8 ▾
Ring port state	FORWARD	BLOCK
Redundant Ring state	enable ▾	
Set Redundant Ring port	Redundant Ring port1	Redundant Ring port 2
	3 ▾	4 ▾
Redundant Ring port state	BLOCK	BLOCK
Ring-coupling state	enable ▾	
Set Ring-coupling port	Ring-coupling port1	Ring-coupling port 2
	5 ▾	6 ▾
Ring-coupling port state	FORWARD	FORWARD
Apply		
<small>Note: This page will automatically refresh in 11 seconds.</small>		

A	Configures a basic ring.
B	Configures a redundant ring to the basic ring, resulting in a dual ring topology.
C	Configures the ports as coupling ports to communicate between multiple rings.

Figure 5-45 “Extended Ring” page

Group A: Basic ring configuration

- **Ring state:** Select “enable” or “disable” from the drop-down menu to enable or disable a basic ring.
- **Set ring port:** Select the two ports that connect to the ring from the drop-down menu.
- **Ring port state:** Displays the status of the ring ports. Options are
 - **Forward:** Port is operating correctly and forwarding traffic.
 - **Block:** Port is intentionally blocked as part of extended ring function.
 - **Down:** Link is down with no communications, typically caused by a cable failure or powered down switch.
 - **Suspend:** Operation of the ring-to-ring coupling function is suspended (stopped) due to an improper configuration. The other port's coupling function is either not enabled or the other port is incorrectly configured as a ring port.

Group B: Redundant ring configuration

- **Redundant ring state:** Select “enable” or “disable” from the drop-down menu to enable or disable the switch to function in a redundant ring.
- **Set redundant ring port:** Select the two ports that connect to the redundant ring.
- **Redundant ring port state:** Displays the status of the redundant ring ports. The options are:
 - **Forward:** Port is operating correctly and forwarding traffic.
 - **Block:** Port is intentionally blocked as part of extended ring function.
 - **Down:** Link is down with no communications, typically caused by a cable failure or powered down switch.
 - **Suspend:** Operation of the ring-to-ring coupling function is suspended (stopped) due to an improper configuration. The other port’s coupling function is either not enabled or the other port is incorrectly configured as a ring port.

Group C: Ring coupling configuration

- **Ring-coupling state:** Select “enable” or “disable” from the drop-down menu to enable the switch to couple with a second ring.
- **Set ring-coupling port:** Select the two ports that couple to the second ring.
- **Ring-coupling port state:** Displays the status of the coupled ports. The options are:
 - **Forward:** Port is operating correctly and forwarding traffic.
 - **Block:** This port is intentionally blocked as part of extended ring function.
 - **Down:** Link down and no communications, typically caused by a cable failure or powered down switch.
 - **Suspend:** Operation of the ring-to-ring coupling function is suspended (stopped) due to an improper configuration. The other port’s coupling function is either not enabled or the other port is incorrectly configured as a ring port.
- **Apply:** Click the “Apply” button to save the settings to volatile memory (see “Configuration management” on page 59).

Ring coupling requires that both ring ports be defined, even if there is no connection to an extended ring. In these types of applications, one of the unused ring ports may connect to an end device or another switch, but the second ring port must be defined although not used.

If only one coupling port is needed, it must use ring coupling port 1.

When selecting the redundant ring ports and installing the redundant ring cables, the path of the redundant ring cables must be identical to the extended ring path.

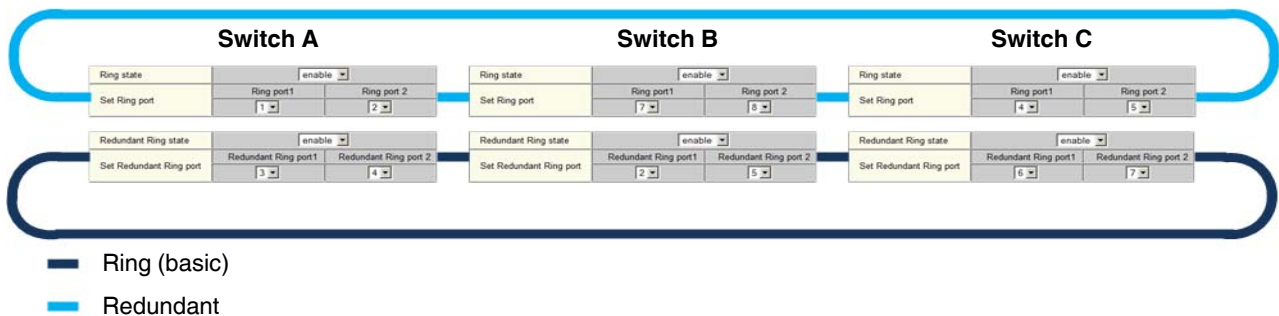


Figure 5-46 Ring port and redundant ring port pairs

The pairs of ring ports and redundant ring ports (ring port 1 and redundant ring port 1 is a pair; ring port 2 and redundant ring port 2 is a pair) must go to the same switch (see Figure 5-46).



Failure to have the basic and redundant ring pairs follow the same path may result in improper network operation or shutdown.

Figure 5-47 shows an incorrect installation with the ports on switch A connected in a different order on the ring as opposed to the redundant ring.

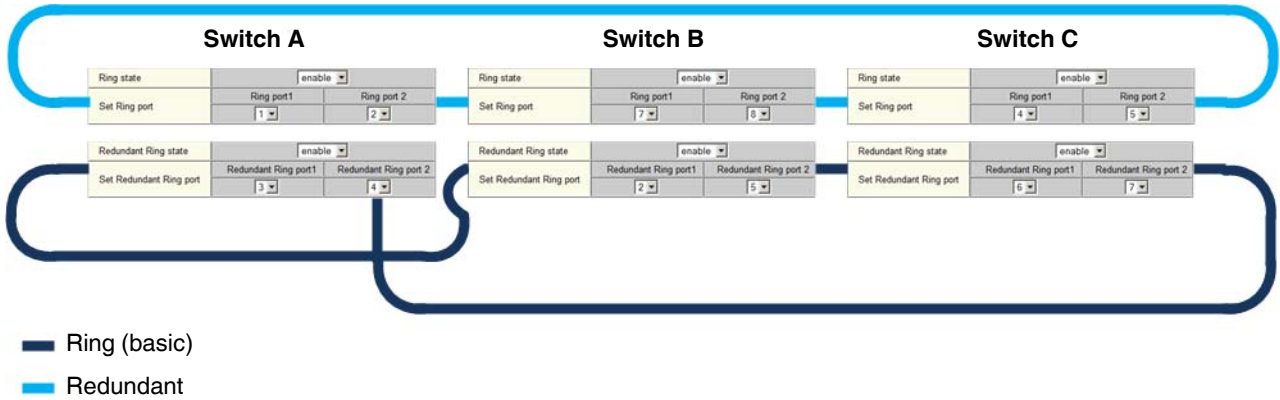


Figure 5-47 Incorrect port pairings and connections

5.6.10.5 Ring general

Additional diagnostics for the extended ring functions are found on the “Switch Station/Redundancy/Ring General” page. The “Ring General” page is included with firmware versions 1.2 and above.

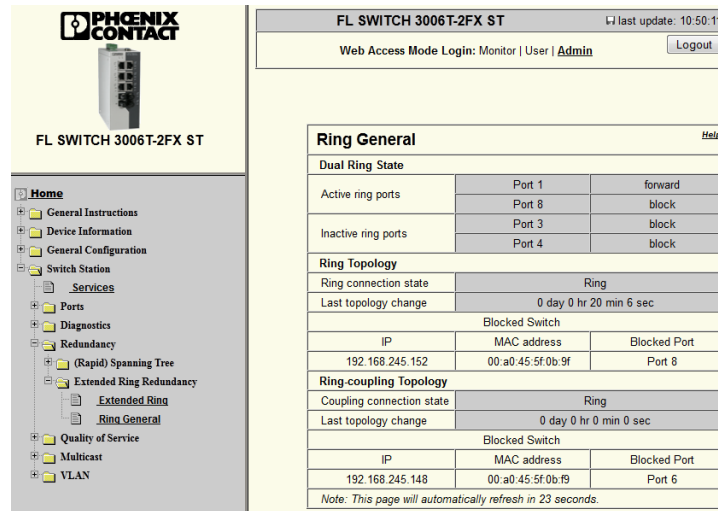


Figure 5-48 “Ring General” screen

Dual Ring State

This section provides the status of the main and redundant rings used in the switch.

- **Active ring ports:** Displays which ports are actively forwarding or blocking traffic.
- **Inactive ring ports:** Indicates which ports are inactive. These ports are, therefore, currently blocked.

The status indication is as follows:

- **Forward:** Port is operating correctly and forwarding traffic.
- **Block:** This port is intentionally blocked as part of extended ring function.
- **Down:** Link is down with no communication.
- **Suspend:** Operation of the ring-to-ring coupling function is suspended (stopped).

Ring Topology

This section provides diagnostics for this switch and other switches used in the active rings of the extended ring system.

- **Ring Connection State:** Indicates whether the switch is operating within a ring or dual ring topology.
- **Last Topology Change:** Displays the amount of time elapsed since the last network disruption that caused the redundancy function to change the topology by unblocking certain ports.
- **Blocked Switch:** Indicates the IP address and MAC address of the switch that is blocking the listed port.

Ring Coupling Topology

This section provides layout diagnostics that include the coupling links between rings used in the extended ring system.

- **Coupling Connection State:** Indicates whether a simple ring-to-ring coupling (Line) or a coupling ring topology is used (Ring).
- **Last Topology Change:** Displays the time of the last network disruption that caused the coupling links to change the topology by unblocking certain ports.
- **Blocked Switch:** Indicates the IP address and MAC address of the switch that is blocking the listed ring coupling port.

5.6.10.6 Configuration examples

For most applications, setting up the ring is a one- or two-step process.

- Define the ring ports: Setting the ring state parameter to **Enable** activates the ring function. Then select the two ports that will reside in the ring.
- Define the ring-to-ring coupling ports: If this switch will also be used to couple this ring to another ring, then enable the “Ring Coupling” state, and select which port or ports will be used in coupling to the other ring.



Always click the “Apply” button to save the settings to volatile memory (see “Configuration management” on page 59).

Using RSTP and extended ring together

In applications where compatibility with existing IT-based systems and high speed control redundancy is required, both RSTP and the extended ring protocols may be used simultaneously in the same switch. The configuration is as follows:

- Enable and configure RSTP and extended ring per the preceding chapters (no special configuration is needed when using both).
- Ensure that any one extended ring (includes coupling and dual ring functions) area is linked to RSTP through only one switch. Having two switches with RSTP enabled, connected to the same extended ring area will cause improper network operation.

The diagnostic status of both the ring ports and ring-coupling ports are also displayed.

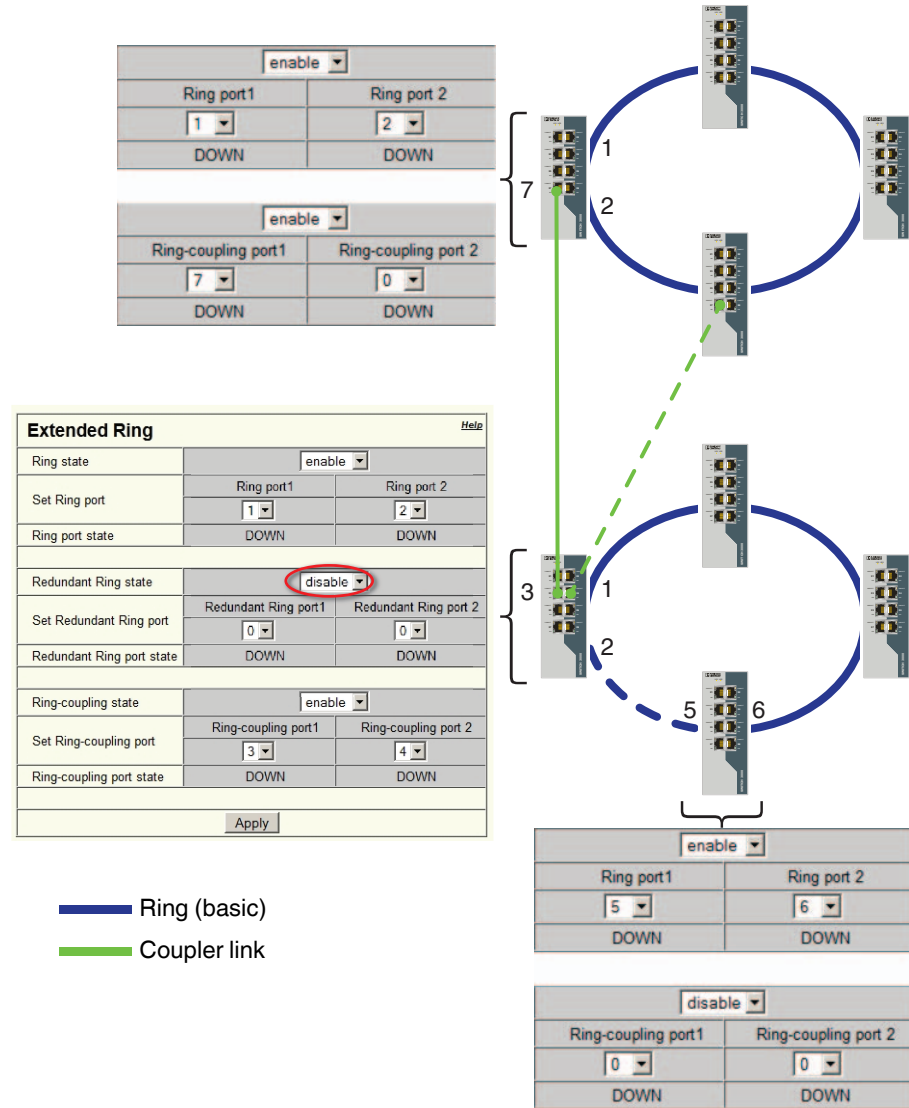
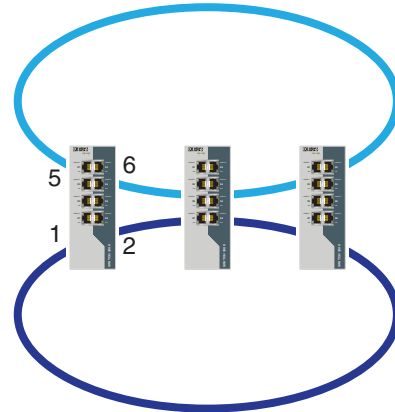
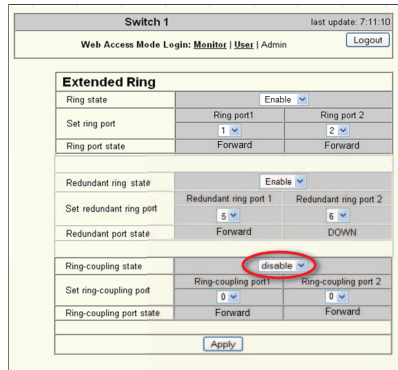


Figure 5-49 Single ring and ring coupling setup



- Ring (basic)
- Redundant

Figure 5-50 Setup of dual ring functionality

- Ring (basic)
- Redundant
- Coupler link

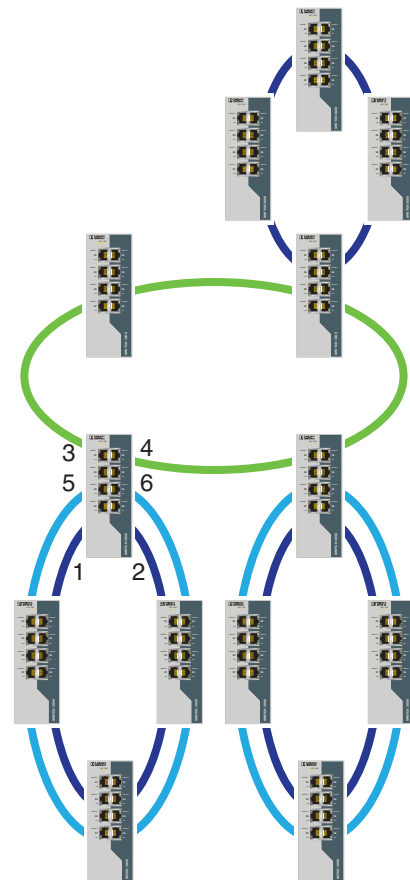
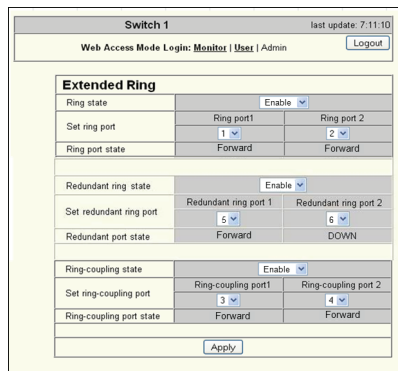


Figure 5-51 Setup of dual ring functionality with ring coupling

5.6.11 Path control

For some applications it is beneficial to define a preferred primary path for the ring. Possible reasons include:

- Consistent and predictable topology to ease troubleshooting.
- Use of different media capacity or bandwidth types in the ring with one being preferred over another.
- Easier accessibility of switches or cabling based on location.

If there is a failure in the primary path, communication automatically reverts to the backup path. When the primary path failure is corrected, communication automatically reverts back to the primary path.

A preferred path can be defined for both rings and the coupling between the rings.

The use of the preferred path function is based on the following constraints.

- The path control function is only available in firmware revision 1.30 and higher.
- The path control function may not be used in combination with the dual ring function.
- For path control to operate, all switches in the ring must have the path control function enabled.
- The application must be able to tolerate a 30 ms recovery time when communications over the backup path automatically reverts back to the primary path after the primary path is repaired.

A preferred path is defined by selecting a specific switch (called a path control ring master) and by setting one of its two ring ports (or coupling ports) to be on the primary path. Upon power up, the ring (or coupling) port of the primary path is active while the other ring (or coupling) port is always blocked, which defines the backup path. If the path control master switch becomes disabled, the other switches in the ring will continue communicating, though the path control function will not be operational.

Automatic switchback

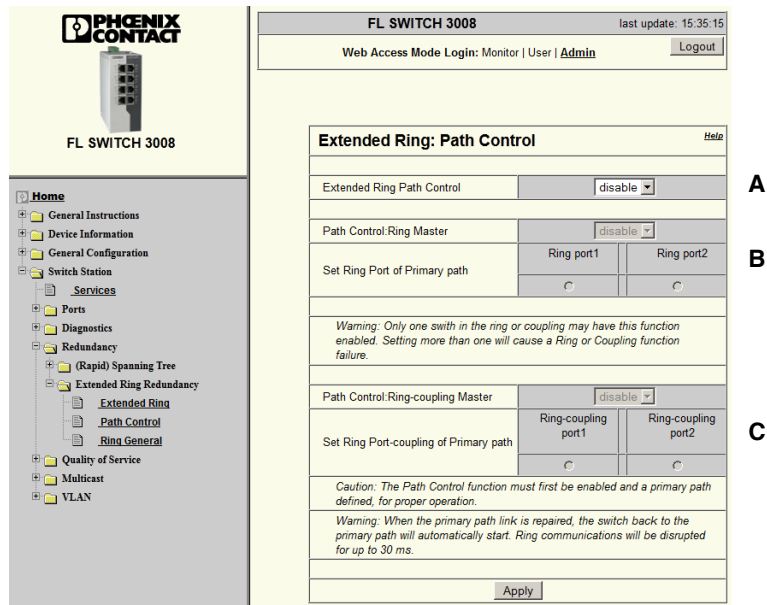
The path control function includes an automatic switchback capability. If there is a failure in the primary path, the switch automatically changes to use the backup path, in 15 ms. When the primary path fault is repaired, the switch will wait one second (default), and then automatically switch back to use the primary path. The automatic switchback recovery will result in stopped ring communication for up to 30 ms. The user may choose to delay the final primary path repair until a time when the 30 ms switchback time is allowable in the application.

As stated earlier, there is a one second time delay from when the switch detects the repaired primary path and when the 30 ms switchback operation starts. This one second delay provides “hysteresis,” which allows the repair to fully settle, preventing a premature switchback which could trigger a primary failure and an oscillating communication disruption. In very special or advanced applications this one second “ring recovery delay” may be changed via SNMP (0-99 seconds). The SNMP recovery delay time is independently set for path control ring recovery versus path control coupling recovery.

Configuration

The path control function is configured from the “Switch Station/Redundancy/Extended Ring Redundancy/Path Control” page.

The “Extended Ring” page must be configured first before the “Extended Ring: Path Control” page is configured. The “Extended Ring: Path Control” page is divided into three sections.



A	Configures an extended ring path.
B	Configures the ring port of the primary path.
C	Configures the coupling port of the primary path.

Figure 5-52 “Extended Ring: Path Control” page

Group A: Extended ring path configuration

- **Extended Ring Path Control:** Select **Enable** from the “Extended Ring Path Control” drop-down menu to enable the path control function. All switches in a path-controlled ring must have the path control function enabled.

Group B: Extended ring port path configuration

- **Path Control: Ring Master:** Select **Enable** from the “Path Control: Ring Master” drop-down menu to define this switch as the path control master.



NOTE:
Only one switch in the ring may be the master. Setting more than one will cause the extended ring redundancy function to fail.

- **Set Ring Port of Primary path:** Click the control button for either “Ring port1” or “Ring port2” to place it in the primary path.

Group C: Extended ring-coupling master configuration

- **Path Control: Ring-coupling Master:** Select **Enable** from the “Path Control: Ring-coupling Master” drop-down menu to enable the extended ring path control as a ring-coupling master.

**NOTE:**

Only one switch in the ring may be the master. Setting more than one will cause the extended ring redundancy function to fail.

- **Set Ring Port-coupling of Primary path:** Click the control button for either “Ring-coupling port1” or “Ring-coupling port2” to place it in the primary path.
- **Apply:** Click the “Apply” button to save the settings to volatile memory (see “Configuration management” on page 59).

5.7 Quality of service

The Quality of service (QoS) functionality contains several options for maximizing the overall network capacity (bandwidth) by prioritizing or filtering out traffic.

Traffic prioritization

When traffic utilization grows, various prioritization methods may be used to give priority handling to time-critical control messages over less time-critical supervisory or general status-related messages. The QoS functions all relate to various ways of setting priorities to outgoing messages and defining how incoming prioritized messages are handled.

Flow control

Flow control defines how the switch reacts when incoming traffic is excessive. In most cases, flow control is used to send “pause 802.3x” messages to other switches to prevent dropped packets in overload conditions. In certain unique network fault conditions and applications, dropped packets may be preferred, and the disabling of flow control is beneficial.

Traffic filtering

The storm control and traffic shaping functions set limits on the level of traffic the switch forwards. This provides pre-defined actions for potentially excessive traffic situations.

5.7.1 Configuring quality of service

Time-critical data, such as voice and video or real-time data, can be set to high priority to ensure the data is transmitted with minimum delay. The FL SWITCH 30..., 40... and 48... can read both IEEE 802.1p and differentiated services (DiffServe) traffic marking or DiffServe code point (DSCP) coded packets.

FL SWITCH 30..., 40... and 48... switches have four internal queues (0, 1, 2, 3). The highest priority messages are placed in queue 3, while the lowest priority messages are placed in queue 0.

There are two types of prioritization approaches that are supported by the switch.

- **Class of Service [IEEE 802.1p (also Q)]:** Manages priority within a subnetwork. This approach maps the eight-level VLAN priority tag into the switch’s four queues.

- **Type of Service/Differentiated Services:** Manages message priorities within and between subnetworks. If message priorities are to be maintained when passing through routers, DiffServe-based prioritization must be used. DiffServe-based services have 64 levels of prioritization (0-63).

Both of these prioritization schemes can be active in the switch at the same time, since different types of switches and control equipment can be mixed in the same overall system.

Configure the QoS functions from the “Quality of Service General” page.

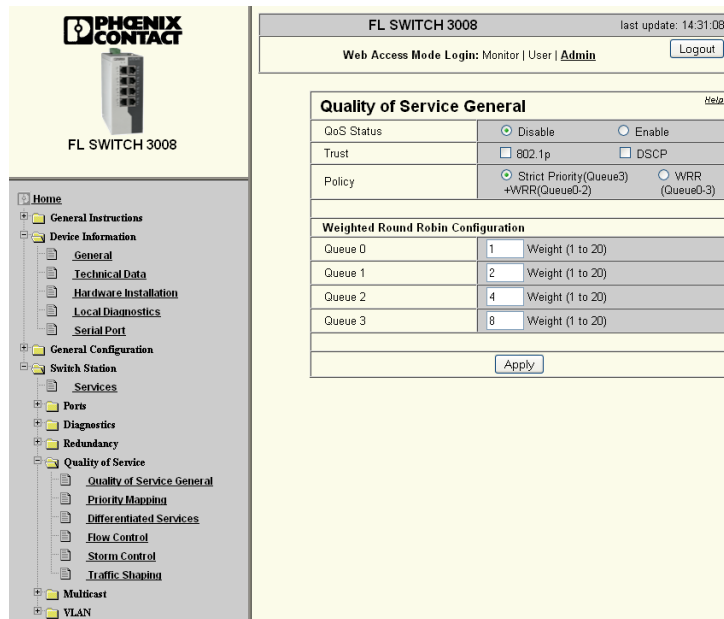


Figure 5-53 “Quality of Service General” page

- **QoS Status:** Click the radio button to “Enable” or “Disable” any of the QoS functions.
- **Trust** (Tagging mode only): Click the check box to define the type of incoming pre-prioritized messages the switch should read and act on. For Class of Service-based (eight priority levels) systems, select **802.1P**.



For firmware versions 1.30 and later, the default type of incoming pre-prioritized message is Class of Service-based (802.1P) when the QoS Status function is enabled.

For outgoing messages from the switch, use the Priority Mapping page (see “Priority mapping” on page 122). For incoming DiffServe prioritized messages, select **DSCP**. For Diffserve-based outgoing messages, use the Differentiated Services page (see “Differentiated services” on page 123). If neither is used, priority is ignored. If both are used, DSCP preempts 802.1p. Port priority will override both.

- **Policy:** Click either the “Strict Priority (Queue 3)” or “WRR” radio button. This sets how the switch services the four different priority queues to ensure that lower priority traffic will be sent and not effectively shut down the switch due to high volumes of high-priority traffic.
 - **WRR** (Weighted Round Robin): In this mode, the switch scans all four priority queues and decides how many packets it sends from any particular queue per scan. A weight of **1** means that, during each scan, that queue will send out only one packet. A weight of **8** means that up to eight packets will be sent from that queue during each internal scan. A weight of 20 means that 20 packets from that queue

will be sent every internal scan. The IEEE default settings are used most often, but these can be customized using the **Weighted Round Robin Configuration** portion of the page. The higher the weight, the faster that queue is emptied of messages.

As an example, consider Q0: 1, Q1: 2, Q2: 4, Q3: 8. In terms of bandwidth, $Q0 = 1/1+2+4+8 = 6\%$, $Q1 = 2/1+2+4+8 = 13\%$, $Q2 = 4/1+2+4+8 = 27\%$ and $Q3 = 8/1+2+4+8 = 53\%$. From a packet perspective, for every single packet emptied from Q0, two will be emptied from Q1, four will be emptied from Q2 and eight will be emptied from Q3 per scan.

- **Strict Priority (Queue 3) + WRR (Queue 0-2):** This maximizes sending of the highest priority packets from “Queue 3”. During each scan, the switch sends all the highest priority “Queue 3” messages. When “Queue 3” is empty, it proceeds to process “Queue 0,” “Queue 1” and “Queue 2” using the weighted round-robin approach. When more “Queue 3” traffic arrives, it stops the weighted round-robin handling and goes back to clear out “Queue 3” messages. When “Queue 3” is clear of messages, it resumes the WRR scanning of the remaining queues.

As an example, consider Q0: 1, Q1: 2, Q2: 4. In terms of bandwidth, $Q0 = 1/1+2+4 = 14\%$, $Q1 = 2/1+2+4 = 29\%$, $Q2 = 4/1+2+4 = 57\%$. From a packet perspective, as long as Q3 is empty, for every single packet emptied from Q0, two will be emptied from Q1 and four will be emptied from Q2 per round. If Q3 contains packets, Q3 will be emptied first until no packets remain. When Q3 is once again empty, the aforementioned scheme resumes.

- **Weighted Round-Robin Configuration:** Enter a value between 1 and 20, setting each queue to send that number of packets per internal queue scan.
As an example: Enter a weight from 1 to 20. This weight is translated to the percent bandwidth each queue will receive (ex.: $Q1/Q1+Q2+Q3+Q4$ for WRR or $Q1/Q1+Q2+Q3$ for WRR+SP[Q3]) or, in other words, the number of packets that will be emptied out of a queue per round with respect to the three other queues.
3. To enter the configuration data, click the “Apply” button (see “Configuration management” on page 59).

5.7.2 Priority mapping

The priority mapping function assigns the value of 802.1p Class of Service (CoS) priority information of a data packet to the four priority queues in the switch. This Class of Service type of prioritization is used by switches to manage priorities within a single network (subnetwork).

The desired assignment can be configured from the “Switch Station/Quality of Service/Priority Mapping” page.

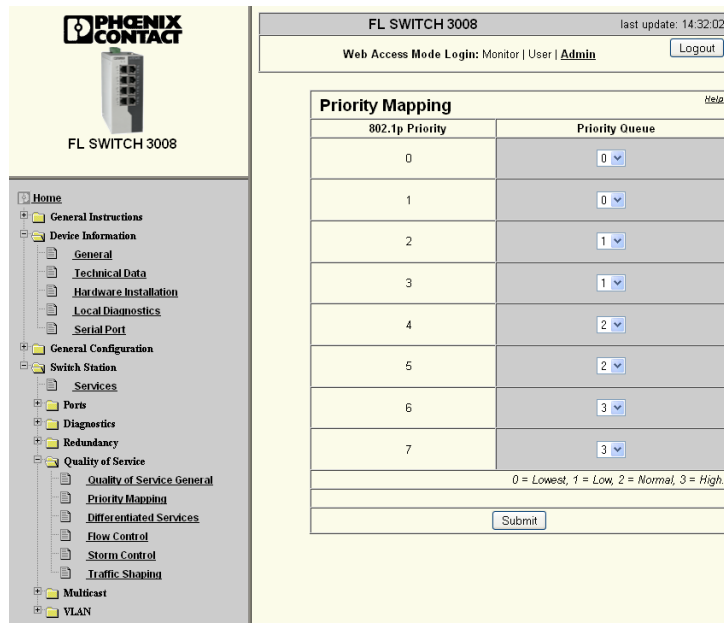


Figure 5-54 “Priority Mapping” page

- **802.1p Priority:** The Class of Service (CoS) values specified by the 3-bit field in Ethernet header when 802.1Q is in use.
- **Priority Queue:** Use the drop-down menu to select one of four QoS priority queues. The lowest priority queue is 0, while the highest priority queue is 3.
- **Submit:** Click the “Submit” button to save the settings to volatile memory (see “Configuration management” on page 59).

5.7.3 Differentiated services

The differentiated services function assigns the priority information of a data packet to the four priority queues in the switch. This DiffServe type of prioritization is used by switches to manage priorities across several subnetworks. If priorities need to be maintained after passing through a router, this type of prioritization must be used.

The desired correlation between the 64 levels of DiffServe priorities and the switch's four queues are configured from the "Differentiated Services" page.

The screenshot shows the web interface for an FL SWITCH 3008. The main content area is titled "Differentiated Services" and contains a table with 8 columns: DSCP Value, Priority Queue, DSCP Value, Priority Queue, DSCP Value, Priority Queue, DSCP Value, and Priority Queue. Each cell in the table contains a numerical value and a drop-down menu showing '0'. The table rows are numbered from 0 to 59 in increments of 4.

DSCP Value	Priority Queue	DSCP Value	Priority Queue	DSCP Value	Priority Queue	DSCP Value	Priority Queue
0	0	1	0	2	0	3	0
4	0	5	0	6	0	7	0
8	0	9	0	10	0	11	0
12	0	13	0	14	0	15	0
16	0	17	0	18	0	19	0
20	0	21	0	22	0	23	0
24	0	25	0	26	0	27	0
28	0	29	0	30	0	31	0
32	0	33	0	34	0	35	0
36	0	37	0	38	0	39	0
40	0	41	0	42	0	43	0
44	0	45	0	46	0	47	0
48	0	49	0	50	0	51	0
52	0	53	0	54	0	55	0
56	0	57	0	58	0	59	0

Figure 5-55 "Differentiated Services" page

- **DSCP Value:** The decimal values associated with PHBs (Per-Hop Behaviors) described by RFC 2475.
- **Priority Queue:** Use the drop-down menu to select one of four QoS priority queues. The lowest priority queue is 0, while the highest priority queue is 3.
- **Submit:** Click the "Submit" button to save the settings to volatile memory (see "Configuration management" on page 59).

5.7.4 Flow control

Flow control is normally enabled up to firmware version 1.21. With firmware version 1.22 and later, the flow control is globally disabled. When the incoming traffic of a switch becomes high enough to fill the internal packet buffers of a port, the flow control function sends pause frames to the connected device to stop sending more packets. When the buffer is able to accept more messages, the pause frames stop, and normal communication resumes. This approach guards against dropped packets in a traffic overload condition.

In unusual conditions, a hardware fault can cause a device to continuously send pause frame command packets that can fill buffers of one switch, cascade into other affected switches and cause a shutdown in a section of the network. For certain critical applications, it is better to have dropped packets than have the unlikely possibility of a partial network shutdown. For these critical applications, flow control may be disabled on the links between switches, and packets will be dropped when a port's buffer fills.

Flow control is activated/deactivated in the “Switch Station/Quality of Service/Flow Control” page.

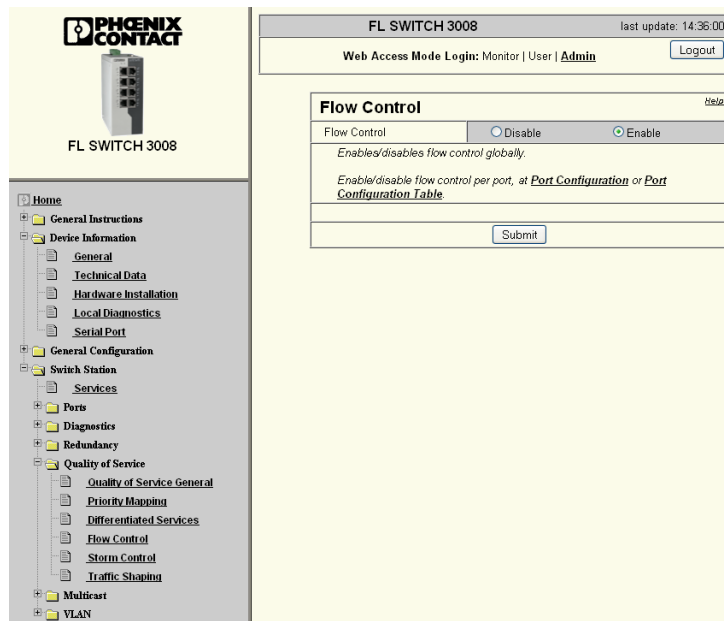


Figure 5-56 “Flow Control” page

- **Flow Control:** Click the radio button to “Disable” or “Enable” the function. Enabled is the default.
- **Submit:** Click the “Submit” button to save the settings to volatile memory (see “Configuration management” on page 59).



It is recommended that flow control be disabled on switch-to-switch links.

5.7.5 Storm control

The storm control function allows the filtering of broadcast, multicast and unicast Ethernet packets for each port. Each port can have a different filtering configuration. The purpose is to stop excessive amounts of different traffic types from entering the switch and proliferating through the network. For each port, or only for certain application-critical ports, the maximum percentage of allowable bandwidth is defined.

The choice of which parameter to set is based on both the type of traffic and whether the traffic was previously learned by the switch, i.e., multicasts learned using IGMP snooping, normal unicast learning or if the excess traffic is unlearned (switch has not seen it before). Unlearned traffic can come from different sources, such as other parts of the manufacturing facility or the office environment. It can also come as a temporary result of redundancy reconfigurations.

The unicast selection filters out both unicast and multicast unlearned traffic. The multicast selection, by itself, only filters out previously learned multicast traffic. In order to filter out all multicast traffic, both the unicast and multicast functions must be selected. The broadcast option filters out all broadcast traffic.

- For FL SWITCH 30... and FL SWITCH 40... switches, the unicast selection filters out both unlearned unicast and unlearned multicast traffic. The multicast selection, by itself, only filters out previously learned multicast traffic. In order to filter out all multicast traffic, both the unicast and multicast functions must be selected. The broadcast option filters out all broadcast traffic.
- For FL SWITCH 48...E... switches, the unicast selection filters out unlearned unicast traffic. The multicast selection filters out all multicast traffic. The broadcast option filters out all broadcast traffic.

The desired function can be configured from the “Switch Station/Quality of Service/Storm Control” page.

The screenshot shows the web interface for a Phoenix Contact FL SWITCH 3008. The top left features the Phoenix Contact logo and the device name 'FL SWITCH 3008'. Below this is a navigation menu with categories like 'Home', 'General Instructions', 'Device Information', 'General Configuration', 'Switch Station', 'Services', 'Parts', 'Diagnostics', 'Redundancy', 'Quality of Service', 'Multicast', and 'VLAN'. The 'Quality of Service' section is expanded to show 'Storm Control'. The main content area displays the 'Storm Control' configuration for 'port-1'. It includes three rows of radio buttons: 'Broadcast Storm Control' (Disable selected), 'Multicast Storm Control' (Disable selected), and 'Unicast Storm Control' (Disable selected). Below these is a 'Threshold level' input field set to '0.1-100 %' and a 'Submit' button.

Figure 5-57 “Storm Control” page

- **Port:** Select the desired port from the drop-down menu.

- **Broadcast Storm Control:** Click the radio button to “Enable” or “Disable” the function.
- **Multicast Storm Control:** Click the radio button to “Enable” or “Disable” the function.
- **Unicast Storm Control:** Click the radio button to “Enable” or “Disable” the function.
- **Threshold level:** Enter the maximum level, as a percentage, for bandwidth. Note that the same threshold level is used for all enabled message types.
 The value entered should be the maximum bandwidth for the most critical message type. For example, if all three control types are enabled, limiting the threshold to 33% for each message type creates a total network load of 99% utilization. If only two message types are used but the maximum threshold for one message type is 40%, both message types are limited to 40%.
 In networks with broadcast traffic above 800 Ethernet frames per second, enter 0.4% or lower in the “Threshold level” field.
- **Submit:** Click the “Submit” button to save the settings to volatile memory (see “Configuration management” on page 59).

5.7.6 Traffic shaping

Traffic shaping allows definition of the maximum allowable level of traffic (bandwidth used) for ingress traffic (incoming packets) and egress traffic (outgoing packets) for each individual port. Traffic shaping sets a maximum transfer rate, as a percentage, for all traffic, regardless of the type. For each port, the maximum ingress and egress rates are 100% for ingress and 100% for egress.

The desired assignment can be configured from the “Switch Station/Quality of Service/Traffic Shaping” page.

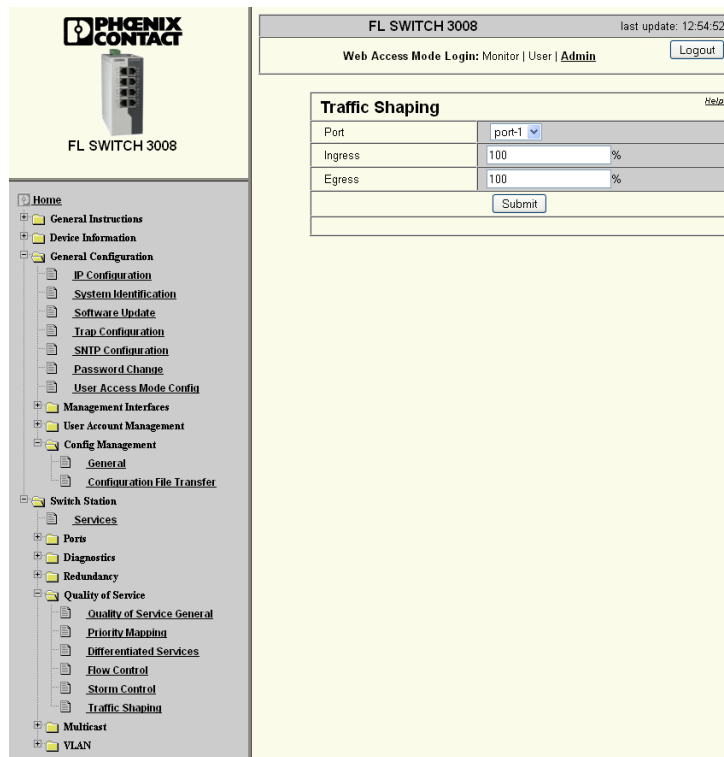


Figure 5-58 “Traffic Shaping” page

- **Port:** Select the desired port from the drop-down menu.
- **Ingress:** Enter the maximum incoming transfer rate for the selected port as a percentage.
- **Egress:** Enter the maximum outgoing transfer rate for the selected port as a percentage.
- **Submit:** Click the “Submit” button to save the settings to volatile memory (see “Configuration management” on page 59).

5.8 Multicast control

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.

Advantages:

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



A maximum of 256 multicast groups can be created automatically for IGMP snooping. In addition, a maximum of 20 static groups can be created.

5.8.1 Procedure for creating a multicast group

Gain an overview of the multicast applications available within the network and the multicast addresses used. Create a group for every multicast application or for the multicast address used, and for each switch add the ports to which a device of the appropriate group is directly connected or via which the device can be accessed.

Example: In Table 5-3 there are various switches connected to multicast transmitters (like PLCs) and multicast receivers (like I/O stations). Typically, PLCs are sending unicast heartbeats to I/O, which is producing multicast so multiple PLCs can listen. The ports (for each switch) to which the receivers of the multicast data are connected are indicated with an “X”.

Table 5-3 Multicast port assignment to the switches

	Switch 1	Switch 2	Switch 3	Switch 4	Switch 5	Switch 6	Switch 7
Port 1							
Port 2	X	X	X	X		X	X
Port 3							
Port 4					X		X
Port 5				X			
Port 6						X	
Port 7	X						
Port 8			X		X		



Possible redundant paths resulting from rapid spanning tree must be taken into consideration for multicast group creation.

5.8.2 General multicast configuration

There are two methods of defining multicast groups that are then managed by the switch.

- Static multicast groups are created manually where all configuration information is entered manually by the user.
- Dynamic multicast groups use Internet Group Management Protocol (IGMP) Snooping and Query functions to automatically learn the multicast groups.
- Group Multicast Registration Protocol (GMRP) may be used with dynamic multicast groups to automatically share multicast group information between switches.

IGMP snooping can be configured from the “Switch Station/Multicast/General” page.

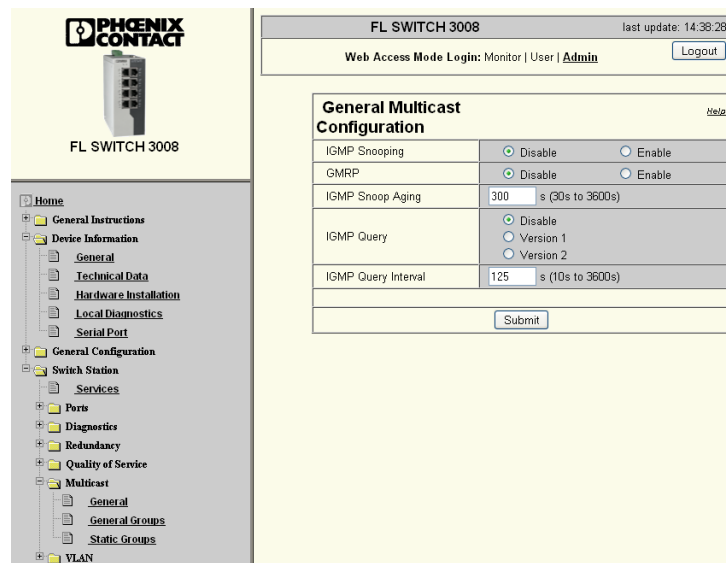


Figure 5-59 “General Multicast Configuration” page

- **IGMP Snooping:** Click the radio button to “Enable” or “Disable” IGMP snooping. In IGMP snooping, the switch passively listens in on the IGMP messages 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.
- **GMRP:** Click the radio button to “Enable” or “Disable” GMRP.
- **IGMP Snoop Aging:** Enter a value, from **30** to **3600** seconds, to maintain the membership reports. 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:** Click the radio button to select “Disable”, “Version 1” or “Version 2” IGMP queries. A switch with activated query function actively sends queries of the version selected under “IGMP Query” and evaluates the received reports. The switch only sends IGMP query reports if IGMP snooping is enabled and only in the management VLAN.
- **IGMP Query Interval:** Enter a value from **10** to **3600** seconds. This is the interval between IGMP queries.
- **Submit:** Click the “Submit” button to save the settings to volatile memory (see “Configuration management” on page 59).

5.8.3 Static multicast groups

Static multicast groups must be created manually on every switch, and all ports that are used to contact group members need to be added. The advantages of static groups are:

1. Easy specification of network paths on which the multicast data traffic of known groups is limited.
2. No querier required (see “Querying port states” on page 79).

The following marginal conditions must be observed:

- Precise network documentation for path specification is required.
- Possible redundant paths due to spanning tree must be taken into account during port assignment.
- For network modifications and during servicing or expansion, the multicast data paths must be restored.

The “Static Groups” page is used to create and manage statically configured multicast groups. In order to create a multicast group, enter the MAC address for the multicast group in the “Multicast Group Address” field, add the ports of the data paths to the group members and confirm these entries by entering a valid password. If a group address is entered as an IP address, the IP address is converted into a multicast MAC address according to the specifications of IEEE 802.1D/p.

Overwriting a dynamic group with a static configuration means that a new port assignment for this group cannot be created dynamically. Port assignments for this group can only be started dynamically once the group has been deleted.

The guidelines for converting a multicast IP address into a multicast MAC address require the mapping of different IP groups to the same MAC group. Avoid the use of IP groups:

- that do not differ in the first and second byte from the right.
- that differ by 128 in the third byte from the right.
- where the fourth byte from the right is always replaced by 01:00:5e during conversion. See example below:



Because of the conversion from IP to MAC addresses, avoid using IP addresses that differ by 128 in the third byte from the right. Example:

Third byte
from right
↓

First multicast IP address	228. 30.117.216
Second multicast IP address	228.158.117.216
Difference	128

Both multicast IP addresses are converted into the multicast MAC address 01:00:5e:1e:75:d8.

The group is added to the list of existing static multicast groups. This list, which is displayed in a list box, is referred to as “dot1qStaticMulticastTable” in SNMP.



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

Port assignment

After entering a new group in the “Multicast Group Address” field, add the ports of the group members by selecting the corresponding check boxes.

Modifying assignment

Select the corresponding group in the “Select Group” list box to modify or delete the port assignment. The group members are indicated by check boxes and can be modified, if required. Click the “Submit” or “Delete” button to complete the action.

The screenshot shows the web interface for a Phoenix Contact FL SWITCH 3008. The page title is "Static Multicast Groups". On the left is a navigation tree with categories like "General Instructions", "Device Information", "Switch Station", and "Multicast". The main content area has a "Select Group" dropdown menu and a "Create Filter" button. Below these are input fields for "VLAN ID", "Multicast Group Address", and "Ports 1-8". There are also instructions for entering MAC and IP addresses and "Submit" and "Delete" buttons.

Figure 5-60 “Static Multicast Groups” page

Checking group assignment

In order to check which ports are assigned to which group, select one of the existing groups. The corresponding MAC address is then displayed in the “Multicast Group Address” text field. The members of the group are indicated by the activated check boxes.

Multicast addresses

Do not use multicast MAC addresses that are in the range from 01:00:5e:80:00:00 to 01:00:5e:ff:ff:ff.

Incorrect format

An incorrect MAC address format and the entry of “non-multicast addresses” is indicated, and the entry is not permitted.



Please note that in multicast MAC addresses the bytes are separated by a colon (:), and in IP multicast addresses, the bytes are separated by a decimal (.).

5.8.4 Dynamic multicast groups

5.8.4.1 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 the IP level (Layer 3).

When starting a multicast application, a network device transmits an IGMP membership report, thus announcing its membership to a specific multicast group. A router collects these membership reports and 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. Please note that the FL SWITCH 30..., 40... and 48... only operates as the IGMP querier in the management VLAN.

IGMP snooping

A switch that 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).

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.

5.8.5 “General Multicast Configuration” page

The “General Multicast” page provides global settings for multicast support. Here, IGMP snooping can be activated and an aging time specified for IGMP snooping information.

The screenshot shows the web interface for an FL SWITCH 3008. The main content area is titled 'General Multicast Configuration' and contains the following settings:

Setting	Value
IGMP Snooping	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
GMRP	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
IGMP Snoop Aging	300 s (30s to 3600s)
IGMP Query	<input checked="" type="radio"/> Disable <input type="radio"/> Version 1 <input type="radio"/> Version 2
IGMP Query Interval	125 s (10s to 3600s)

A 'Submit' button is located at the bottom of the configuration table.

Figure 5-61 “General Multicast Configuration” page

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 query

The FL SWITCH 30..., 40... and 48... with activated query function actively sends queries at “query intervals” and evaluates the received reports. The FL SWITCH 30..., 40... and 48... only sends IGMP query reports if IGMP snooping is enabled and only in the management VLAN.

- **IGMP Snooping:** Click the radio button to “Disable” or “Enable” IGMP snooping.
- **GMRP:** Click the radio button to “Disable” or “Enable” GMRP.
- **IGMP Snoop Aging:** Enter the time for Enter a value between **30** and **3600** seconds. The default is **300** seconds.
- **IGMP Query:**
 - Click the “Disable” radio button to disable the query function.
 - Click the “Version 1” radio button to enable queries using IGMP version 1.

- Click the "Version 2" radio button to enable queries using IGMP version 2.
- **IGMP Query Interval:** Enter the time between query requests. Enter a value between **10** and **3600** seconds. The default is **300** seconds.
- **Submit:** Click the "Submit" button to save the settings to volatile memory (see "Configuration management" on page 59).

5.8.6 Current multicast groups

The table on this page provides an overview of the current multicast groups created on the FL SWITCH 30..., 40... and 48... switch. These include multicast groups assigned as a result of IGMP snooping and groups that are statically created.

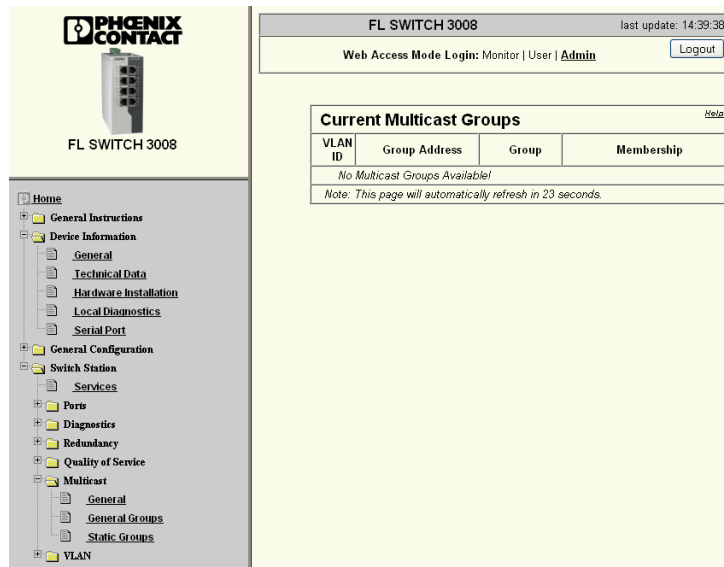


Figure 5-62 "Current Multicast Groups" page

Multicast groups are listed in a row with the VLAN ID, Group Address and Group. In the "Membership" column are check boxes. Each check box corresponds to a port on the switch to indicate membership. Ports are numerically arranged from port 1 on the left to port 5 or 8 on the right. The group column indicates which group of up to eight ports the membership relates to. For larger port capacity switch versions, each group membership may consist of two or more groups, i.e., for a 16-port switch group 1-8 and group 9-16.



All multicast groups that are known to the switch, including the dynamically detected groups that were not created manually, are shown on this page.

- **Membership:** Click the check box to join or remove the port from the group.

5.9 VLAN

A VLAN is a closed network that 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.

VLANs work by taking the traffic from normal industrial devices, I/O, PLC, etc., and assigning a VLAN ID number to the traffic. Switches use the VLAN IDs to determine which devices can talk to each other. Only devices on the same VLAN can communicate with each other. The VLAN ID is also known as a **Tag**. When VLAN functions are disabled, the switch is said to be in transparent mode – the traffic passes through the switch without being modified or filtered. Each VLAN contains all the traffic from its devices like a separate network cable would. Devices on one VLAN can be spread between different switches. Configuration information for a new VLAN is entered manually for that switch the first time. When connecting many VLAN switches together, the VLAN information from the other switches can be created either **statically** (manually) or **dynamically** (automatically).

There are two approaches where VLAN IDs may be added to an Ethernet packet and controlled within the network: “port-based VLANs” and “tagging”.

Port-based VLANs

The port-based VLAN approach is optimized to manage traffic between devices connected to a single switch or a small group of switches. One or more VLAN IDs are assigned to each port on the switch. This means all traffic coming into that port is assigned VLAN IDs and can belong to one or more VLANs. This approach is also used when connecting to legacy switches that do not support the newer IEEE 802.1Q “Tagging” standard. The setup for any single port is easy, but as more switches are added, overall system configuration may become difficult. VLAN trunks also contain all VLAN information – there is no ability to restrict certain VLAN information in the main trunk lines.

Tagging-based VLANs

Tagging-based VLANs are based on the IEEE 802.1Q standard. With this method, some ports are defined as edge ports, connected to devices, and some ports are defined as trunk ports, for main backbone communications. For edge ports, any single device is only assigned one VLAN ID. However, when many switches are connected together, the GVRP option can be used, where switches automatically learn the VLAN setups in each other (no manual entry is required for switch-to-switch interfacing). There are also additional security-oriented filtering functions to control which VLAN traffic is allowed on the main trunk lines. Compared with port-based VLANs, there are more traffic control options, but tagging-based VLANs require more setup parameters. Table 5-4 summarizes the differences between the two approaches.

Table 5-4 Port-based VLANs vs. Tagging-based VLANs

Function	Port-based VLAN	Tagging-based VLAN
Maximum number of VLANs per switch	16	64
Scope of control	One or a few switches is ideal	Multiple switches
Configuration complexity (number of options)	Lower	Higher
Automatic switch-to-switch VLAN configuration (GVRP)	No	Yes
Filters VLAN traffic between sections of the main backbone	No	Yes
VLANs per port	Can be many	1 (typically)

GVRP protocol

The GVRP protocol (GARP VLAN Registration Protocol) can be activated in “VLAN Tagging” mode for dynamic registration of the VLANs at the relevant neighbor. The GVRP switch indicates the selected user setting or enables the setting. GVRP is used to dynamically create VLANs across several switches. If GVRP is set to **Disable**, the switch is transparent for GVRP BPDUs (GVRP data packets). If GVRP is set to **Enable**, the switch sends GVRP BPDUs every 10 seconds. If the VLAN assignment of a port to a specified VLAN is changed, the adjacent switches will be informed of this change within the next 10 seconds.

When the GVRP is disabled, the adjacent switches also remove the dynamically learned ports within the next 10 seconds. If GVRP packets are missing, the learned group assignments are rejected after approximately 20 seconds. If a static VLAN is installed on a switch, a port can be added to this VLAN via GVRP. The port is listed in the Current VLANs Table (see Figure 5-66). However, only statically created group members are saved.

VLAN page references

The following can be used as a guide when configuring VLANs:

General configuration page

Disable (transparent mode) or enable VLANs

Select either port-based or tag-based VLAN

Enable the GVRP option (tagging mode only)

For a port-based VLAN, use the following pages:

Current VLANs for status and diagnostic information

Port-based VLAN configuration

For a tagging VLAN, use the following pages:

Current VLANs for status and diagnostic information

Static VLAN configuration

Advanced static VLAN configuration (optional)

Native VLAN port configuration (optional)

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 then use the same switches/infrastructure components. Alternatively, termination devices that support VLAN tags can also be used.

5.9.1 VLAN ID management

The management of the switch and all ports are assigned to VLAN 1 by default. This ensures that the network-supported management functions can be accessed via all ports.



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



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



If the VLAN in which the FL SWITCH 30..., 40... and 48... is managed is deleted, 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.

5.9.1.1 Configuration in transparent mode

Figure 5-63 To configure the switch to operate in transparent mode: "IP Configuration" page

1. Enable the pages for VLAN configuration (see "Login and user accounts" on page 54).
2. Create the required VLANs (see "Static VLAN example" on page 143).

3. On the “Port Based VLAN Configuration” page (see Figure 5-65), assign the ports for incoming packets to individual VLANs using the VLAN ID (see “Port-based VLAN configuration” on page 140).
4. On the “IP Configuration” page, the desired management VLAN ID can now be set (see “Individual port configuration” on page 65).
5. On the “General VLAN Configuration” page, set the switch to “Tagging” VLAN mode (see “General VLAN configuration” on page 138).
6. Click the “Submit” button to save the configuration (see “Configuration management” on page 59).

5.9.1.2 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. 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.
3. From the “IP Configuration” page (see Figure 5-63), set the desired VLAN ID as the management VLAN.
4. Connect a PC to the switch via port B and save the configuration. Make sure that the FL SWITCH 30..., 40... and 48... is always managed in an accessible VLAN.

5.9.2 General VLAN configuration

The use of VLANs can be activated/deactivated from the “Switch Station/VLAN/General Configuration” page.

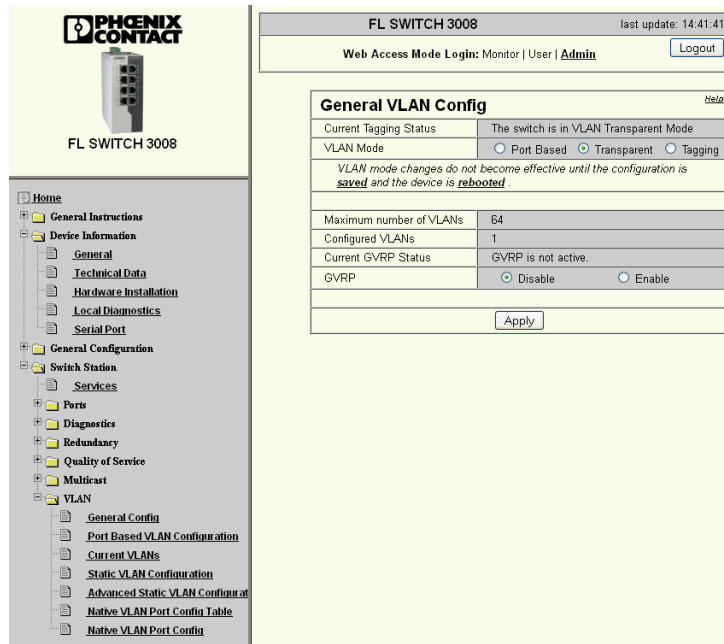


Figure 5-64 “General VLAN Configuration” page

Current Tagging Status: Displays the current switch status.

VLAN Mode: Click the radio button to select the VLAN mode.

- **Transparent:** No VLAN functions are enabled. Ethernet traffic passes transparently through the switch without modification.
- **Port-based:** Used to select the port-based VLAN operating mode. Port-based VLANs are optimized for one or a few switches. They are also used when connecting to legacy switches that do not support IEEE 802.1Q. In port-based VLAN mode, VLAN IDs are assigned to all traffic coming into a port. Previously tagged VLAN traffic is sent only to the output ports that are members of that VLAN. The switch supports a maximum of 16 port-based VLANs.
- **Tagging:** Used to select the VLAN tagging (IEEE 802.1Q) mode. VLAN tagging is optimized for networks with medium to large numbers of switches, or where control of backbone VLAN traffic is needed. 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 switch supports a maximum of 64 VLANs in tagging mode.
- **Maximum number of VLANs:** Displays the number of VLANs that can be managed. Dependent upon the type of VLAN mode.
- **Configured VLANs:** Displays the number of currently configured VLANs.
- **Current GVRP Status:** Displays the GVRP status.
- **GVRP:** Click the radio button to “Enable” or “Disable” GVRP. GVRP is only available in **VLAN Tagging** mode and **Transparent** mode.

GVRP allows the dynamic (automatic) registration of the VLANs from the relevant neighbors. GVRP is used to dynamically create VLANs across several switches. If GVRP is set to **Disable**, the switch is transparent for GVRP BPDUs (GVRP data packets). The management VLAN ID specifies the VLAN that the switch can be accessed by, if it is operating in Tagging VLAN mode.
- **Apply:** Click the “Apply” button to save the configuration (see “Configuration management” on page 59). After switching the VLAN mode from **Tagging** or **Port Based** 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 observed in the “Current Tagging Status” field.

5.9.3 Port-based VLAN configuration

Port-specific VLAN settings can be made from the “Switch Station/VLAN/Port Based VLAN Configuration” page.

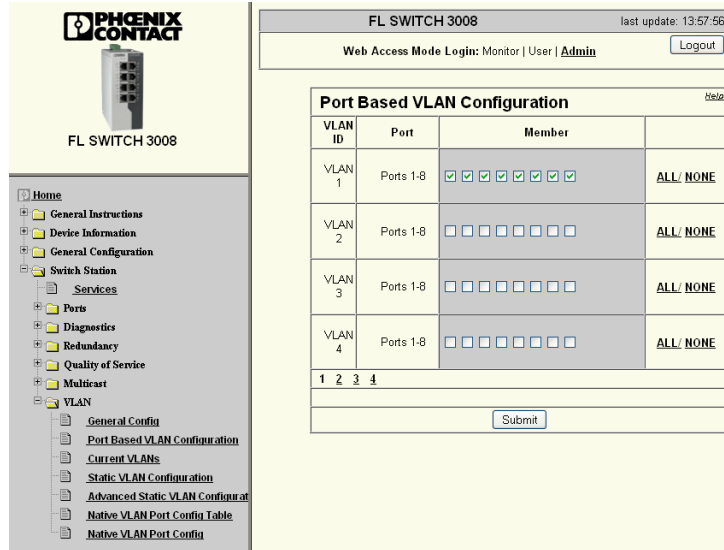


Figure 5-65 “Port Based VLAN Configuration” page

Configuration is in a table format. Each VLAN is listed in the first column. Click the check box of each port that is to be assigned to that VLAN. Alternatively, click either “ALL” or “NONE” to place a check in the check boxes. After assigning the ports to the VLANs, click the “Submit” button.

- **Submit:** Click the “Submit” button to save the settings to volatile memory (see “Configuration management” on page 59).

5.9.4 Current VLANs

The “Current VLANs” page provides an overview of the VLANs currently existing in the switch. All VLANs are listed here. In addition, refer to the “Static VLAN Configuration” pages where the VLANs were created.

FL SWITCH 3008 last update: 14:42:43
Web Access Mode Login: Monitor | User | **Admin** Logout

Current VLANs <small>table</small>			
VLAN ID	Type	Group	Membership
1	static / Management VLAN	Ports 1-8	U U U U U U U U

(T=Tagged, U=Untagged, -=Non Member)
This table indicates out of which ports each VLAN's data will be sent using static (Static VLANs) or dynamic (GVRP) configuration data.
Note: This page will automatically refresh in 28 seconds.

Figure 5-66 “Current VLANs” page

All VLANs are listed, along with the type, number of ports and the type of membership. Membership is displayed as **T** (tagged), **U** (untagged) and **-** (non-members). VLAN 1 is always created statically, and all ports are added to it as untagged members.

5.9.5 Tagging-based VLANs: Static VLANs

Tagging-based VLAN systems are configured statically (manually) or dynamically (automatically via GVRP). The static configuration of VLANs is used to define which ports on a switch have which VLAN configuration. Once a switch's own VLAN ports are configured via the “Static VLANs” page, then VLAN information from other switches must be added to that switch. This can be done statically (any other switch's VLAN information that passes through this switch is statically configured into this switch) or dynamically via the GVRP feature.

The “Static VLAN Configuration” page allows static VLANs to be created one at a time. The “Advanced Static VLAN Configuration” page has the additional ability to quickly create groups of VLANs

5.9.5.1 Configuring static VLANs

VLAN 1 is always created statically (IEEE standard), and all ports are added to it as untagged members. With Tagging VLAN mode activated, network-based management interfaces (WBM, Telnet and SNMP) are only available from VLAN 1 (default). This means

that in order to access the management interfaces, users must either implement data traffic in tagged mode without the VLAN tag, where the switch is accessed via ports using the VLAN ID, or use data traffic with a VLAN ID of 1.

Up to 64 “tagging based” VLANs can be created using VLAN IDs in the range of 2-4096. If more than 64 VLANs are created, an error message is displayed.

Static VLANs are created from the “Static VLAN Configuration” page.

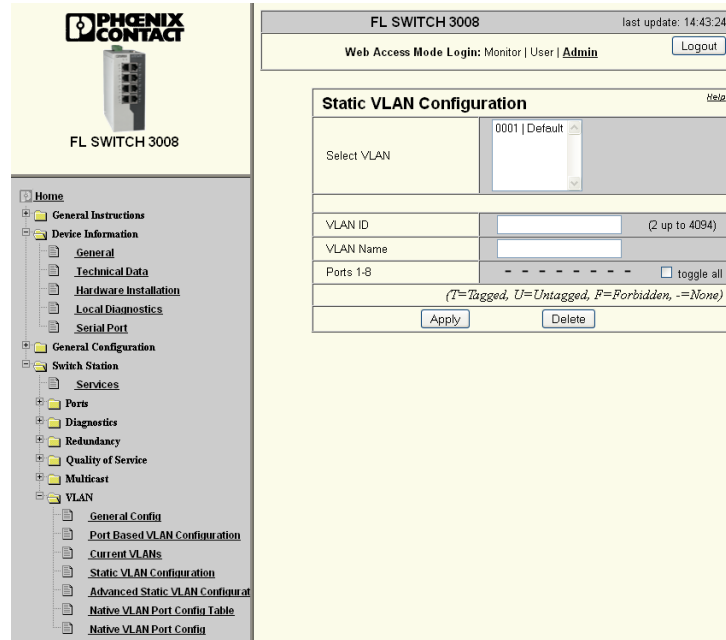


Figure 5-67 “Static VLAN Configuration” page

- **Select VLAN:** Click the desired VLAN from the list displayed.
- **VLAN ID:** Enter an ID between 2 and 4096.
- **VLAN Name:** Enter a name between 8 and 16 characters long.
- **Ports 1-8:** Click the “-” to select a port to be a member of the selected VLAN.
 - **T (Tagged):** Ports with **T** status belong to the selected VLAN, and packets are sent to this port with VLAN tag.
 - **U (Untagged):** Ports with **U** 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).
 - **F (Forbidden):** Ports with **F** status do not belong to the selected VLAN and cannot be added dynamically to this VLAN via GVRP.
 - **- (None):** Ports with - status are not integrated into the VLAN.
- **Apply:** Click the “Apply” button to save the settings to volatile memory (see “Configuration management” on page 59).

5.9.5.2 Static VLAN example



Instead of using VLAN 1 for management, it is recommended that a new, separate VLAN be created for management. Ensure that the administrator has access to this VLAN.

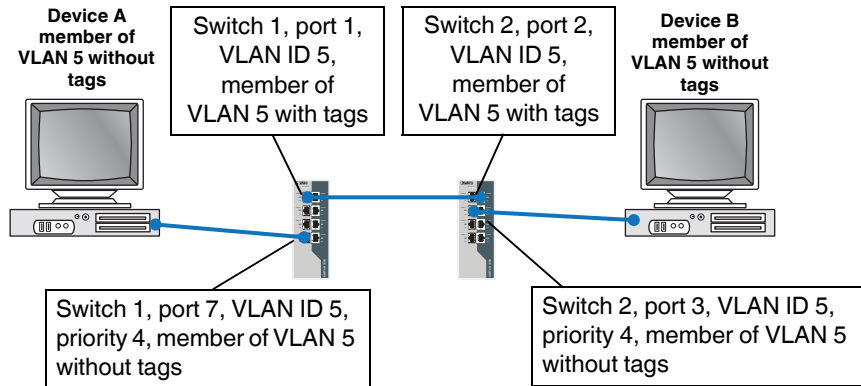


Figure 5-68 Communication between termination devices via VLAN

Switch configuration

1. Set both switches to **VLAN Tagging** mode, save and restart devices.
2. Create VLAN 5 on switch 1, specify port 7 as an **untagged** member and port 1 as a **tagged** member.
3. For port 7 on switch 1, set the priority to 4.
4. On switch 2, create port 2 as a tagged member and port 3 as an untagged member of VLAN 5.
5. For port 3 on switch 2, set the priority to 4.

Both termination devices now communicate via the network path shown in Figure 5-68 without other switch ports forwarding the broadcast packets for both termination devices, for example.

If additional infrastructure components are located between switch 1 and switch 2, there are two options to ensure communication between the termination devices:

- The infrastructure is also operated in “VLAN Tagging” mode, and VLAN 5 is created based on the relevant devices. Result: high configuration and maintenance costs.
- GVRP is activated in “VLAN Tagging” mode on all infrastructure components, and the information about the created VLANs is transmitted within the network via switch 1 and switch 2. Result: bidirectional data exchange is ensured between termination device A and B.

5.9.5.3 Advanced VLAN configuration

The “Advanced Static VLAN Configuration” page is used to enter groups of VLANs in a single step instead of one by one. The page can also be used to enter or modify VLANs individually. To enter a group of VLANs, check the box in the “VLAN ID-Range” field. To enter individual VLAN information, check the box in the “VLAN ID-Individual” field.

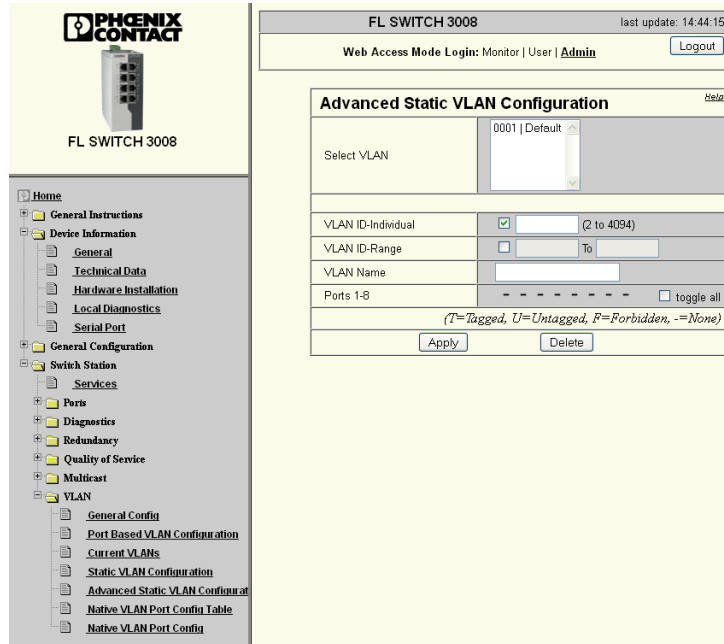


Figure 5-69 “VLAN Advanced Configuration” page

- **Select VLAN:** Click the desired VLAN from the list displayed.
- **VLAN ID-Individual:** Click the check box to use this function and enter an ID between 2 and 4096.
- **VLAN ID-Range:** Click the check box to use this function and enter a range for the automatically created IDs. The range must be between 2 and 4096, must be sequential and must not exceed 64 VLAN ID values.
- **VLAN Name:** Enter a name for the VLAN. The field accepts names between 2 and 10 characters.
- **Ports 1-8:** Click the “–” to select a port to be a member of the selected VLAN.
 - **T (Tagged):** Ports with **T** status belong to the selected VLAN, and packets are sent to this port with VLAN tag.
 - **U (Untagged):** Ports with **U** 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).
 - **F (Forbidden):** Ports with **F** status do not belong to the selected VLAN and cannot be added dynamically to this VLAN via GVRP.
 - **– (None):** Ports with – status are not integrated into the VLAN.
- **Apply:** Click the “Apply” button to save the settings to volatile memory (see “Configuration management” on page 59).

The automatically created VLANs will have default names such as VLANxxxx. To customize the names:

1. Check the box in the “VLAN ID-Individual” area and uncheck the “VLAN ID-Range” check box.
2. From the list of VLANs in the “Select VLAN” field, click the desired VLAN. Enter the desired name in the “VLAN Name” field.
3. If desired, modify the “Ports1-8” field for the desired state of each port.
4. Click the “Apply” button (see “Configuration management” on page 59).

5.9.6 Native VLAN configuration

The “Native VLAN Configuration” pages are used to define what default VLAN ID and priority tags will be added to any untagged data coming into the ports on a switch. By default, all devices use VLAN 1 as the default native VLAN, which is the same as the default management VLAN for the switch. These pages allow the default native VLAN to be changed. As an example of use, switch-to-switch VLAN trunk lines (defined using the static pages or GVRP), which were originally supposed to carry only VLAN trunk data, may need to carry industrial device data due to a plant change. In this case, changing the native VLANs from 1 to another VLAN on the trunk ports may be needed. Similar to port-based VLANs, the manipulation of native VLAN numbers between ports can help communication between devices.

The “Native VLAN Port Config Table” page allows the quick change of basic native VLAN ID and priority configurations for all ports on the switch. The “Native VLAN Port Config” page allows configuration of basic native VLAN ID and priority one port at a time, and has additional native port GVRP and egress configuration settings.

The screenshot displays the web interface for a Phoenix Contact FL SWITCH 3008. The main content area is titled "Native Vlan Port Config Table" and contains a table with the following data:

Port	Native VLAN	Priority
1	1	0
2	1	0
3	1	0
4	1	0
5	1	0
6	1	0
7	1	0
8	1	0

Below the table, there is a note: "This table indicates what Port VLAN ID and Priority will be assigned to any untagged data coming in each port." and a "Submit" button.

Figure 5-70 “Native VLAN Port Config Table” page

The table allows the easy and fast change of basic native VLAN ID and basic QoS priority configurations for all ports on the switch. Click on the relevant port number to open the “VLAN Port Configuration” page where the settings can be modified. This table can be used to assign incoming packets to the created VLANs if the packets reached the port without a VLAN tag.

- **Submit:** Click the “Submit” button to save the settings to volatile memory (see “Configuration management” on page 59).

The “Native VLAN Port Configuration” page allows the port-by-port configuration of the native VLAN of the switch. In addition to the native VLAN ID and basic QoS Priority, the Egress tagging and GVRP settings for the port may also be made. Select which port is to be configured via the “Port Number” drop-down menu. Then enter the native VLAN ID and any priority settings.

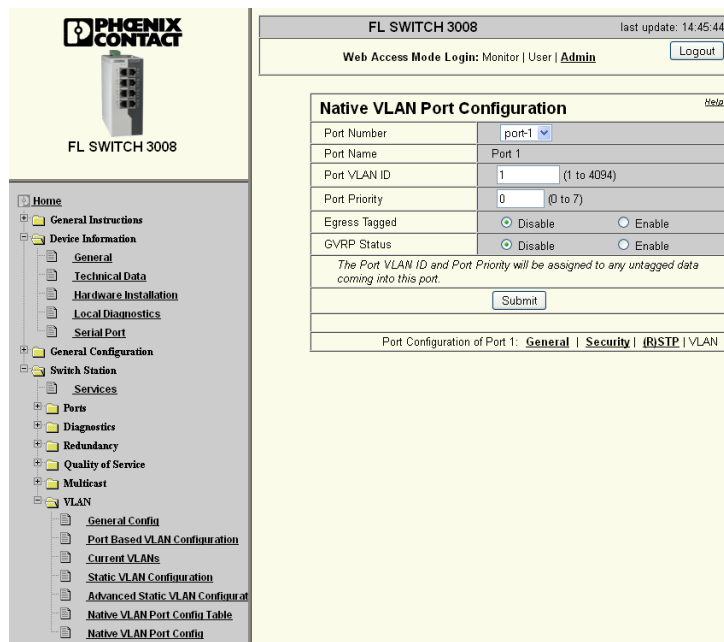


Figure 5-71 “Native VLAN Port Configuration” page

- **Port Number:** Port being referenced.
- **Port Name:** Name assigned to the port.
- **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. Only IDs of existing VLANs can be set as the port VLAN ID.
- **Port Priority:** A corresponding tag indicating the priority is added to packets without tags.
- **Egress Tagged:** Defines whether the VLAN ID is to be added to traffic exiting (egressing) from this port. For normal native VLAN applications the outgoing traffic from the port is not tagged. This setting is for special cases.
- **GVRP Status:** Defines whether this port will accept GVRP dynamic VLAN configuration data.
- **Submit:** Click the “Submit” button to save the settings to volatile memory (see “Configuration management” on page 59).

5.9.7 Tagging-based VLANs: Dynamic GVRP configuration

Dynamic VLAN configurations using GVRP can be set for transmission between infrastructure components. Here, every switch with static- or dynamic-created VLANs transmits information within the network via VLAN IDs. The adjacent switches with activated GVRP then create the same VLANs and add the receiver ports of the GVRP BPDUs as “tagged” ports. A BPDU receiver then distributes its own BPDUs to all ports via the dynamically learned VLAN.

1. All switches must be set to **VLAN Tagging** mode. After saving the configuration, a restart is required.
2. GVRP must be activated on all switches (see “General VLAN configuration” on page 138).

Since termination devices usually do not support VLAN tags, port-specific settings must be made at the termination device ports for the infrastructure. The switch then adds the corresponding tags to every data packet received at the relevant port. If a data packet is to be sent from the termination device port to the termination device, the switch removes the VLAN tag first.

5.9.8 VLAN and RSTP

When using RSTP and VLAN simultaneously, please note the following:

- RSTP is not based on VLANs. Standard RSTP packets will cross between VLANs. To isolate RSTP action within one or more VLANs, use MST (see “MST” on page 99).
- RSTP 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 RSTP, every VLAN can be accessed by every switch.

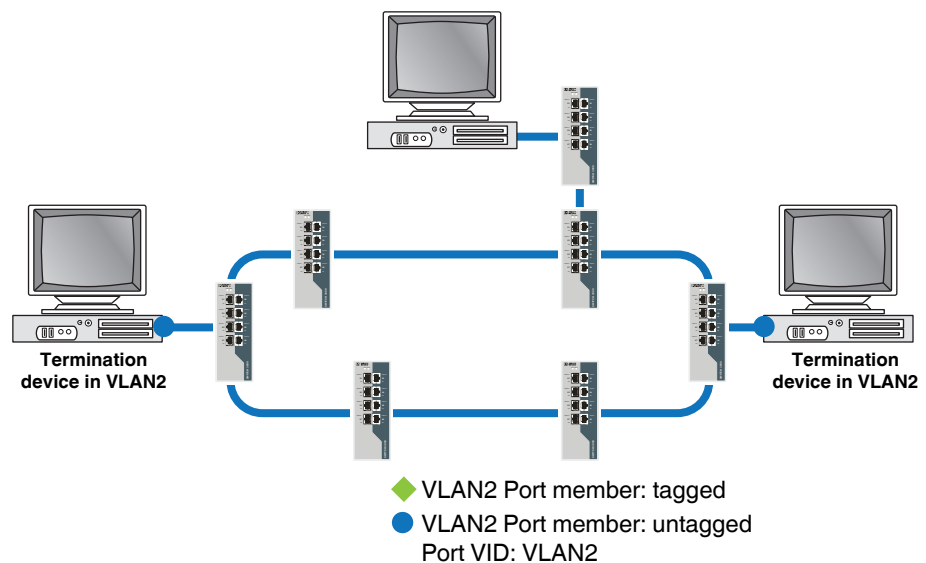


Figure 5-72 Typical configuration for VLAN and RSTP

5.10 Link aggregation

Link aggregation (also known as “Trunking”) allows up to four ports to be combined into a larger capacity link. It is mainly used to increase the bandwidth capacity of a switch to a server/PC or tightly couple two managed switches without having to replace switches with gigabit class switches. The trunking function uses link aggregation control protocol to manage the load across the individual links that make up the trunk line. Failure of a link results in the switch re-apportioning the traffic across the remaining links. The link aggregation load balancing works by analyzing the MAC addresses of the traffic.

All links that make up the trunk must be of the same data rate and duplex.

5.10.1 Configuring link aggregation

Link aggregation is managed from the “Switch Station/Ports/Ext. Port Configuration/Link Aggregation” page.

The screenshot shows the web interface for a Phoenix Contact FL SWITCH 3008. The page title is "Link Aggregation" and it includes a "Help" link. The configuration area contains the following fields:

Select Trunk	Create
Link Aggregation	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Trunking	<input checked="" type="radio"/> 802.1ax <input type="radio"/> 802.3ad
STP Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Load Balance	[Dropdown menu]

Below the configuration fields, there is a note: "NOTE: Connecting Link aggregation to a device NOT supporting 802.3ad would cause a loop." The "Link Name" field is empty, and the "Link Status" is "Not Connected". The "Member Ports" section shows "Ports 1-8" with eight checkboxes, all of which are unchecked. A "Submit" button is located at the bottom of the form.

Figure 5-73 “Link Aggregation” page

- **Select Trunk:** Use the drop-down menu to select an already defined trunk name for deletion or modification, or select “Create” a new trunk. Only one trunk can be defined per switch.
- **Link Aggregation:** Click the radio button to “Enable” or “Disable” the function.
- **Trunking:** Click the “802.1ax” or “802.3ad” radio button to choose the trunking management function. IEEE 802.3ad was released in 2000 and 802.1ax in 2008. The default is 802.1ax. The 802.3ad approach is used when connecting a switch to an older legacy switch.

- **STP Mode:** Click the radio button to “Enable” or “Disable” the flow of IEEE STP or RSTP redundancy protocols across the trunk line. Please note that the extended ring protocol packets are not transferred across any of the link aggregation controlled links.
- **Load Balance:** Use the drop-down menu to select the distribution method of the traffic across the separate links. The choices are “Source address”, “Destination address” or “Mix of source/destination addresses”. The choice is based on the dominant direction of data flow. If the data flow between switches is relatively equal, then “Mix of source/destination addresses” should be used. If there is a particularly heavy concentration of traffic to a single area, for example, an alarm-gathering HMI, then “Destination address” may be used. If control devices are sending commands to many slave devices, then “Source address” may be used.
- **Link Name:** Enter a name for the aggregated link. The name is important in order to change or delete the link in the future.
- **Link Status:** Displays the status of the link system as connected and operational.
- **Ports 1-8:** Click the check box to select the member ports that form the aggregated link. A maximum of four ports can be selected.
- **Submit:** Click the “Submit” button to save the settings to volatile memory (see “Configuration management” on page 59).

A Technical appendix – MIB objects

A 1 SNMP MIB objects

This appendix categorizes the SNMP MIB objects and associates them with the corresponding WBM page. Note that the table is a subset of the SNMP objects available. The device-specific MIB files for FL SWITCH 30..., 40... and 48... switches can be downloaded from the device via the "Technical Data" page (see "Private MIBs" on page 3-30).

Table A-1 Device information

	WBM page	MIB file	SNMP object	Full path/OID
	SERIAL PORT	FL-SWITCH-3000_V131-MIB.mib	flWorkFWCtrlSerial	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlSerial(6)

FL SWITCH 30..., 40... and 48...

Table A-2 General configuration

WBM page	MIB file	SNMP object	Full path/OID
IP CONFIGURATION	FL-SWITCH-3000_V131-MIB.mib	flWorkNetIfParameter	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkNet(4).flWorkNetIfParameter(1)
SYSTEM IDENTIFICATION	SNMPv2-MIB	system	iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).system(1)
SOFTWARE UPDATE	FL-SWITCH-3000_V131-MIB.mib	flWorkFWCtrlUpdate	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlUpdate(4)
TRAP CONFIGURATION	FL-SWITCH-3000_V131-MIB.mib	flWorkFWCtrlTrapDest	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlTrapDest(2)
SNTP CONFIGURATION	FL-SWITCH-3000_V131-MIB.mib	flWorkTimeSynchSntp	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkTimeSynch(21).flWorkTimeSynchSntp(1)
PASSWORD CHANGE	FL-SWITCH-3000_V131-MIB.mib	flWorkFWCtrlPasswd	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlPasswd(3)
MANAGEMENT INTERFACES	FL-SWITCH-3000_V131-MIB.mib	flWorkFWCtrlBasic	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlBasic(1)

Table A-2 General configuration (continued)

	WBM page	MIB file	SNMP object	Full path/OID
User account				
	USER ACCOUNT	FL-SWITCH-3000_V131-MIB.mib	flWorkFWCtrlUserConfigTable	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlUserConfigGroup(14).flWorkFWCtrlUserConfigTable(2)
	LOGIN SESSION	FL-SWITCH-3000_V131-MIB.mib	flWorkFWCtrlLoginSessionTable	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlUserConfigGroup(14).flWorkFWCtrlLoginSessionTable(3)
	RADIUS AUTHENTICATION	radius_auth_client.mib	radiusAuthServerTable	iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).radiusMIB(67).radiusAuthentication(1).radiusAuthClientMIB(2).radiusAuthClientMIBObjects(1).radiusAuthClient(1).radiusAuthServerTable(3)
	CONFIGURATION MANAGEMENT	FL-SWITCH-3000_V131-MIB.mib	flWorkFWCtrlConf	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlConf(5)

FL SWITCH 30..., 40... and 48...

Table A-3 Switch station

	WBM page	MIB file	SNMP object	Full path/OID
Ports				
	PORT MIRRORING	FL-SWITCH-3000_V131-MIB.mib	flSwitchPortMirr	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flSwitch(15).flSwitchPortMirr(2)
Ports/Ext.				
	GENERAL - PORT SECURITY	FL-SWITCH-3000_V131-MIB.mib	flWorkFWCtrlSecurityPortEnable	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlSecurity(8).flWorkFWCtrlSecurityPort(2).flWorkFWCtrlSecurityPortEnable(5)
	GENERAL - 802.1X	dot1x.mi2	dot1xPaeSystemAuthControl	iso(1).std(0).iso8802(8802).ieee802dot1(1).ieee802dot1mibs(1).ieee8021paeMIB(1).paeMIBObjects(1).dot1xPaeSystem(1).dot1xPaeSystemAuthControl(1)
	802.1X CONFIGURATION	dot1x.mi2	dot1xAuthConfigTable	iso(1).std(0).iso8802(8802).ieee802dot1(1).ieee802dot1mibs(1).ieee8021paeMIB(1).paeMIBObjects(1).dot1xPaeAuthenticator(2).dot1xAuthConfigTable(1)
	MAC-BASED SECURITY: PER PORT	FL-SWITCH-3000_V131-MIB.mib	flWorkFWCtrlSecurityPort	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).fl
	MAC-BASED SECURITY: GLOBAL DISCARD	rfc4188-BRIDGE-MIB.mi2	dot1dStaticTable	iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).dot1dBridge(17).dot1dStatic(5).dot1dStaticTable(1)
	LINK AGGREGATION	FL-SWITCH-3000_V131-MIB.mib	flSwitchLagConfig	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flSwitch(15).flSwitchLagConfig(8)

Table A-3 Switch station (continued)

	WBM page	MIB file	SNMP object	Full path/OID
Diagnostics				
	ALARM CONTACT	FL-SWITCH-3000_V131-MIB.mib	flWorkFWCtrlAlarmContact	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlAlarmContact(7)
	UTILIZATION	FL-SWITCH-3000_V131-MIB.mib	flSwitchUtilPortTable	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flSwitch(15).flSwitchUtil(14).flSwitchUtilPortTable(1)
	EVENT TABLE	FL-SWITCH-3000_V131-MIB.mib	flWorkFWInfoEvent	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWInfo(1).flWorkFWInfoEvent(14)
	MAC ADDRESS TABLE	rfc2674q-Q-BRIDGE-MIB.mi2	std mib (depends on tagged-based vlan enabled?) dot1qTpFdbTable in 1q-mib,	iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).dot1dBridge(17).dot1dTp(4).dotqTpFdbTable(3)
	LLDP GENERAL	LLDP MIB.mi2	lldpConfiguration	iso(1).std(0).iso8802(8802).ieee802dot1(1).ieee802dot1mibs(1).lldpMIB(2).lldpObjects(1).lldpConfiguration(1)
	LLDP TOPOLOGY	LLDP MIB.mi2	lldpRemoteSystemsData	iso(1).std(0).iso8802(8802).ieee802dot1(1).ieee802dot1mibs(1).lldpMIB(2).lldpObjects(1).lldpRemoteSystemsData(4)
Redundancy/(rapid) spanning tree				
	SPANNING-TREE	rfc4188-BRIDGE-MIB.mi2	dot1dStp	iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).dot1dBridge(17).dot1dStp(2)
	MST	IEEE8021-MSTP-MIB.mi2	IEEE8021-MSTP-MIB	iso(1).org(3).ieee(111)Standards-association-numbers-series-standards(2).lan-man-stds(802).ieee802dot1(1).ieee802dot1-1(1).ieee8021MstpMib(6)
	EXTENDED RING REDUNDANCY	FL-SWITCH-3000_V131-MIB.mib	flSwitchExtendedRing	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flSwitch(15).flSwitchRedundancy(4).flSwitchExtendedRing(5)

FL SWITCH 30..., 40... and 48...

Table A-3 Switch station (continued)

	WBM page	MIB file	SNMP object	Full path/OID
Quality of service				
	QUALITY OF SERVICE - GENERAL	FL-SWITCH-3000_V131-MIB.mib	flSwitchQoSMechanism, flSwitchQoSSchedulingControl	1. flSwitchQoSMechanism iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flSwitch(15).flSwitchQoSMechanism(10) 2. flSwitchQoSSchedulingControl iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flSwitch(15).flSwitchQoSSchedulingCo
	PRIORITY MAPPING	pBridgeMIB	dot1dTrafficClassTable	iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).dot1dBridge(17).pBridgeMIB(6).pBridgeMIBObjects(1).dot1dPriority(2).d
	DIFFERENTIATED SERVICES	FL-SWITCH-3000_V131-MIB.mib	flSwitchQoSDiffservExtend	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flSwitch(15).flSwitchQoSDiffservExtend(12)
	FLOW CONTROL	FL-SWITCH-3000_V131-MIB.mib	flSwitchDot3FlowControlMode	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flSwitch(15).flSwitchRateCtrl(6).flSwitchDot3FlowControlMode(4)
	STORM CONTROL	FL-SWITCH-3000_V131-MIB.mib	flSwitchStormCtrlTable	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flSwitch(15).flSwitchRateCtrl(6).flSwitchStormCtrlTable(11)
	TRAFFIC SHAPING	FL-SWITCH-3000_V131-MIB.mib	flSwitchTrafficShapingTable	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flSwitch(15).flSwitchTrafficShaping(7).flSwitchTrafficShapingTable(1)

Table A-3 Switch station (continued)

	WBM page	MIB file	SNMP object	Full path/OID
Multicast				
	MULTICAST - GENERAL	FL-SWITCH-3000_V131-MIB.mib, rfc2674p-P-BRIDGE-MIB.mi2	flSwitchIgmP_Snoop, dot1dGmrpStatus, flSwitchIgmP_Query	A).flSwitchIgmP_Snoop iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flSwitch(15).flSwitchIgmP(3).flSwitchIgmP_Snoop(1) B).dot1dGmrpStatus iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).dot1dBridge(17).pBridgeMIB(6).pBridgeMIBObjects(1).dot1dExtBase(1).dot1dGmrpStatus(3) C).flSwitchIgmP_Query iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flSwitch(15).flSwitchIgmP(3).flSwitchIgmP_Query(2)
	CURRENT MULTICAST GROUPS	FL-SWITCH-3000_V131-MIB.mib	flSwitchIgmP_SnoopTable	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flSwitch(15).flSwitchIgmP(3).flSwitchIgmP_Snoop(1).flSwitchIgmP_SnoopTable(4)
	STATIC GROUPS	rfc2674q-Q-BRIDGE-MIB.mi2	dot1qStaticMulticastTable	iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).dot1dBridge(17).qBridgeMIB(7).qBridgeMIBObjects(1).dot1qStatic(3).dot1qStaticMulticastTable(2)
VLAN				
	GENERAL CONFIG - VLAN MODE	FL-SWITCH-3000_V131-MIB.mib	flSwitchCtrlVlanTagMode	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flSwitch(15).flSwitchCtrl(1).flSwitchCtrlVlanTagMode(5)
	GENERAL CONFIG - GVRP	rfc2674q-Q-BRIDGE-MIB.mi2	dot1qGvrpStatus	iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).dot1dBridge(17).qBridgeMIB(7).qBridgeMIBObjects(1).dot1qBase(1).dot1qGvrpStatus(5)
	PORT-BASED VLAN CONFIGURATION	FL-SWITCH-3000_V131-MIB.mib	flSwitchVlanPortBasedTable	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flSwitch(15).flSwitchPortBasedVlan(13).flSwitchVlanPortBased(1).flSwitchVlanPortBasedTable(1)

FL SWITCH 30..., 40... and 48...

Table A-3 Switch station (continued)

WBM page	MIB file	SNMP object	Full path/OID
CURRENT VLANS	rfc2674q-Q-BRIDGE-MIB.mi2	dot1qVlanCurrentTable	iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).dot1dBridge(17).qBridgeMIB(7).qBridgeMIBObjects(1).dot1qVlan(4).dot
STATIC VLAN CONFIGURATION	rfc2674q-Q-BRIDGE-MIB.mi2	dot1qVlanStaticTable	iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).dot1dBridge(17).qBridgeMIB(7).qBridgeMIBObjects(1).dot1qVlan(4).dot
ADVANCED STATIC VLAN CONFIGURATION	rfc2674q-Q-BRIDGE-MIB.mi2	dot1qVlanStaticTable	iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).dot1dBridge(17).qBridgeMIB(7).qBridgeMIBObjects(1).dot1qVlan(4).dot1qVlanStaticTable(3)
NATIVE VLAN PORT CONFIGURATION	rfc2674q-Q-BRIDGE-MIB.mi2, rfc2674p-P-BRIDGE-MIB.mi2	dot1qPortVlanTable	iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).dot1dBridge(17).qBridgeMIB(7).qBridgeMIBObjects(1).dot1qVlan(4).dot1qPortVlanTable(5)
AGING TIME	rfc4188-BRIDGE-MIB.mi2	dot1dTpAgingTime	iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).dot1dBridge(17).dot1qVlan(4).dot1dTpAgingTime(2) MIB object (OID 1.3.6.1.2.1.17.4.2).The available setting range is 10 - 1000000 seconds. For static configuration, an aging time of 300
IP CONFIGURATION	FL-SWITCH-3000_V131-MIB.mib	flWorkNetIfParamIpAddress	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkNet(4).flWorkNetIfParameter(1)flWorkNetIfParamIpAddress.(2)

Table A-4 Management interfaces

	WBM page	MIB file	SNMP object	Full path/OID
	TELNET	FL-SWITCH-3000_V131-MIB.mib	flWorkFWCtrlTelnet	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlBasic(1).flWorkFWCtrlTelnet
	HTTP	FL-SWITCH-3000_V131-MIB.mib	flWorkFWCtrlHTTP	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlBasic(1).flWorkFWCtrlHTTP
	HTTPS	FL-SWITCH-3000_V131-MIB.mib	flWorkFWCtrlSNMP	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlBasic(1).flWorkFWCtrlHTTP
	SNMP	FL-SWITCH-3000_V131-MIB.mib	flWorkFWCtrlSNMP	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlBasic(1).flWorkFWCtrlSNMP
	SNMPv3	FL-SWITCH-3000_V131-MIB.mib	flWorkFWCtrlSNMPv3	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlBasic(1).flWorkFWCtrlSNMPv3

B Technical appendix

B 1 Ordering data

Products

Description	Type	Order No.	Pcs./Pkt.
Managed Ethernet switch with five RJ45 ports at 10/100 Mbps and operating temperature of -10°C ... +60°C	FL SWITCH 3005	2891030	1
Managed Ethernet switch with five RJ45 ports at 10/100 Mbps and operating temperature of -40°C ... +75°C	FL SWITCH 3005T	2891032	1
Managed Ethernet switch with eight RJ45 ports at 10/100 Mbps and operating temperature of -10°C ... +60°C	FL SWITCH 3008	2891031	1
Managed Ethernet switch with eight RJ45 ports at 10/100 Mbps and operating temperature of -40°C ... +75°C	FL SWITCH 3008T	2891035	1
Managed Ethernet switch with 16 RJ45 ports at 10/100 Mbps and operating temperature of -10°C ... +60°C	FL SWITCH 3016	2891058	1
Managed Ethernet switch with 16 RJ45 ports at 10/100 Mbps and operating temperature of -40°C ... +75°C	FL SWITCH 3016T	2891059	1
Managed Ethernet switch with four RJ45 ports at 10/100 Mbps, one 100 Mbps SC format fiber optic port and operating temperature of -40°C ... +75°C	FL SWITCH 3004T-FX	2891033	1
Managed Ethernet switch with four RJ45 ports at 10/100 Mbps, one 100 Mbps ST format fiber optic port and operating temperature of -40°C ... +75°C	FL SWITCH 3004T-FX ST	2891034	1
Managed Ethernet switch with six RJ45 ports at 10/100 Mbps, one 100 Mbps SC format fiber optic port and operating temperature of -40°C ... +75°C	FL SWITCH 3006T-2FX	2891036	1
Managed Ethernet switch with six RJ45 ports at 10/100 Mbps, one 100 Mbps ST format fiber optic port and operating temperature of -40°C ... +75°C	FL SWITCH 3006T-2FX ST	2891037	1
Managed Ethernet switch suitable for substation applications, with 12 RJ45 ports at 10/100 Mbps, two SC-D MM fiber optic ports and operating temperature of -40°C ... +70°C	FL SWITCH 3012E-2FX	2891120	1
Managed Ethernet switch suitable for substation applications, with 12 RJ45 ports at 10/100 Mbps, two SC-D SM fiber optic ports and operating temperature of -40°C ... +70°C	FL SWITCH 3012E-2FX SM	2891119	1
Managed Ethernet switch with six RJ45 ports at 10/100 Mbps, two 100 Mbps SC format, single-mode fiber optic ports and operating temperature of -40°C ... +75°C	FL SWITCH 3006T-2FX SM	2891060	1
Managed Ethernet switch suitable for substation applications, with 12 RJ45 ports at 10/100 Mbps, two 100 Mbps SFP slots and operating temperature of -40°C ... +70°C	FL SWITCH 3012E-2SFX	2891067	1
Managed Ethernet switch suitable for substation applications, with 16 RJ45 ports at 10/100 Mbps and operating temperature of -40°C ... +70°C	FL SWITCH 3016E	2891066	1
Managed Ethernet switch with eight RJ45 ports at 10/100 Mbps, two RJ45 ports at 10/100/1000 Mbps, four 100 Mbps SC format, single-mode fiber optic ports and operating temperature of -40°C ... +75°C	FL SWITCH 4008T-2GT-4FX SM	2891061	1
Managed Ethernet switch with eight RJ45 ports at 10/100 Mbps, two RJ45 ports at 10/100/1000 Mbps, three 100 Mbps SC format, single-mode fiber optic ports and operating temperature of -40°C ... +75°C	FL SWITCH 4008T-2GT-3FX SM	2891160	1
Managed Ethernet switch with 12 RJ45 ports at 10/100 Mbps, two RJ45 ports at 10/100/1000 Mbps, two 100 Mbps ST format, multimode fiber optic ports and operating temperature of -40°C ... +75°C	FL SWITCH 4012T-2GT-2FX ST	2891161	1

FL SWITCH 30..., 40... and 48...

Description	Type	Order No.	Pcs./Pkt.
Managed Ethernet switch with 12 RJ45 ports at 10/100 Mbps, two RJ45 ports at 10/100/1000 Mbps, two 100 Mbps SC format, multimode fiber optic ports and operating temperature of -40°C ... +75°C	FL SWITCH 4012T-2GT-2FX	2891063	1
Managed Ethernet switch with eight RJ45 ports at 10/100 Mbps, two 1000 Mbps SFP module slots and operating temperature of -40°C ... +75°C	FL SWITCH 4008T-2SFP	2891062	1
Managed Ethernet switch suitable for substation applications, with 24 RJ45 ports at 10/100 Mbps, four RJ45/FO ports (10/100/1000 Mbps RJ45 connection; 1000 Mbps fiber optic connection requires 1000 Mbps SFP modules) and operating temperature of -40°C ... +70°C	FL SWITCH 4824E-4GC	2891072	1
Managed Ethernet switch suitable for substation applications, with eight RJ45 ports at 10/100 Mbps, 16 LC-MM fiber optic ports at 100 Mbps, four RJ45/FO ports (10/100/1000 Mbps RJ45 connection; 1000 Mbps fiber optic connection requires 1000 Mbps SFP modules) and operating temperature of -40°C ... +70°C	FL SWITCH 4808E-16FX LC-4GC	2891073	1
Managed Ethernet switch suitable for substation applications, with eight RJ45 ports at 10/100 Mbps, 16 LC-SM fiber optic ports at 100 Mbps, four RJ45/FO ports (10/100/1000 Mbps RJ45 connection; 1000 Mbps fiber optic connection requires 1000 Mbps SFP modules) and operating temperature of -40°C ... +70°C	FL SWITCH 4808E-16FX SM LC-4GC	2891074	1
Managed Ethernet switch suitable for substation applications, with eight RJ45 ports at 10/100 Mbps, 16 SC-MM fiber optic ports at 100 Mbps, four RJ45/FO ports (10/100/1000 Mbps RJ45 connection; 1000 Mbps fiber optic connection requires 1000 Mbps SFP modules) and operating temperature of -40°C ... +70°C	FL SWITCH 4808E-16FX-4GC	2891079	1
Managed Ethernet switch suitable for substation applications, with eight RJ45 ports at 10/100 Mbps, 16 SC-SM fiber optic ports at 100 Mbps, four RJ45/FO ports (10/100/1000 Mbps RJ45 connection; 1000 Mbps fiber optic connection requires 1000 Mbps SFP modules) and operating temperature of -40°C ... +70°C	FL SWITCH 4808E-16FX SM-4GC	2891080	1
Managed Ethernet switch suitable for substation applications, with eight RJ45 ports at 10/100 Mbps, 16 ST fiber optic ports at 100 Mbps, four RJ45/FO ports (10/100/1000 Mbps RJ45 connection; 1000 Mbps fiber optic connection requires 1000 Mbps SFP modules) and operating temperature of -40°C ... +70°C	FL SWITCH 4808E-16FX ST-4GC	2891085	1
Managed Ethernet switch suitable for substation applications, with eight RJ45 ports at 10/100 Mbps, 16 ST-SM fiber optic ports at 100 Mbps, four RJ45/FO ports (10/100/1000 Mbps RJ45 connection; 1000 Mbps fiber optic connection requires 1000 Mbps SFP modules) and operating temperature of -40°C ... +70°C	FL SWITCH 4808E-16FX SM ST-4GC	2891086	1
Managed Ethernet switch suitable for substation applications, with 24 SC-D MM fiber optic ports at 100 Mbps, four RJ45/FO ports (10/100/1000 Mbps RJ45 connection; 1000 Mbps fiber optic connection requires 1000 Mbps SFP modules) and operating temperature of -40°C ... +70°C	FL SWITCH 4800E-24FX-4GC	2891102	1
Managed Ethernet switch suitable for substation applications, with 24 SC-D SM fiber optic ports at 100 Mbps, four RJ45/FO ports (10/100/1000 Mbps RJ45 connection; 1000 Mbps fiber optic connection requires 1000 Mbps SFP modules) and operating temperature of -40°C ... +70°C	FL SWITCH 4800E-24FX SM-4GC	2891104	1

Accessories

Description	Type	Order No.	Pcs./Pkt.
SFP module, 1000 Mbps, multimode, 300/550 m	FL SFP SX	2891754	1
SFP module, 1000 Mbps, single mode, 30 km	FL SFP LX	2891767	1
SFP module, 1000 Mbps, long haul, 80 km	FL SFP LH	2989912	1
SFP module, 100 Mbps, multimode, 2 km	FL SFP FX	2891081	1
SFP module, 100 Mbps, single mode, 40 km	FL SFP FX SM	2891082	1
Lockable security element for RJ45 FL PATCH cables	FL PATCH GUARD	2891424	20
Lockable security element key	FL PATCH GUARD KEY	2891521	1
Patch cable, CAT5, pre-assembled, 0.3 m	FL CAT5 PATCH 0,3	2832250	10
Patch cable, CAT5, pre-assembled, 0.5 m	FL CAT5 PATCH 0,5	2832263	10
Patch cable, CAT5, pre-assembled, 1.0 m	FL CAT5 PATCH 1,0	2832276	10
Patch cable, CAT5, pre-assembled, 1.5 m	FL CAT5 PATCH 1,5	2832221	10
Patch cable, CAT5, pre-assembled, 2.0 m	FL CAT5 PATCH 2,0	2832289	10
Patch cable, CAT5, pre-assembled, 3.0 m	FL CAT5 PATCH 3,0	2832292	10
Patch cable, CAT5, pre-assembled, 5.0 m	FL CAT5 PATCH 5,0	2832580	10
Patch cable, CAT5, pre-assembled, 7.5 m	FL CAT5 PATCH 7,5	2832616	10
Patch cable, CAT5, pre-assembled, 10.0 m	FL CAT5 PATCH 10,0	2832629	10
Power supply for rack mounted switch, 48 V DC	FL SWITCH 4800E-P1	2891075	1
Power supply for rack mounted switch, 120/230 V AC/DC	FL SWITCH 4800E-P5	2891076	1
Mounting plate for FL SWITCH 30... and FL SWITCH 40... switches with eight ports	FL PA 3K4K 8	2891108	1
Mounting plate for FL SWITCH 30... and FL SWITCH 40... switches with 16 ports	FL PA 3K4K 16	2891109	1
Mounting kit for FL SWITCH 48...E... switches, for high-vibration and shock applications	FL RMB 4800E	2891054	1

B 2 Technical data

General data	
Mounting type	NS 35 (IEC 60715) DIN rail
Operating temperature	
FL SWITCH 3005, FL SWITCH 3008, FL SWITCH 3016	-10°C ... 60°C
FL SWITCH 3...E	-40°C ... 70°C
All other switches	-40°C ... 75°C
Ambient temperature (storage/transport)	-40 °C ... 85 °C
Permissible humidity (operation)	5% ... 95% (no condensation)
Permissible humidity (storage/transport)	5% ... 95% (no condensation)
Air pressure (operation)	57 kPa ... 108 kPa (up to 4850 m above mean sea level)
Air pressure (storage/transport)	57 kPa ... 108 kPa (up to 4850 m above mean sea level)
Degree of protection	IP20
Protection class	III, VDE 0106, IEC 60536

FL SWITCH 30..., 40... and 48...

Weight and dimensions	Weight	Width	Height	Depth
FL SWITCH 3005, FL SWITCH 3005T	920 g	54.4 mm	146.4 mm	125 mm
FL SWITCH 3008, FL SWITCH 3008T	940 g	54.4 mm	146.4 mm	125 mm
FL SWITCH 3004-FX	920 g	54.4 mm	146.4 mm	125 mm
FL SWITCH 3004-FX ST	930 g	54.4 mm	146.4 mm	125 mm
FL SWITCH 3006-2FX	960 g	54.4 mm	146.4 mm	125 mm
FL SWITCH 3006-2FX ST	955 g	54.4 mm	146.4 mm	125 mm
FL SWITCH 3016	1244 g	66 mm	173 mm	140 mm
FL SWITCH 3016T	1240 g	66 mm	173 mm	140 mm
FL SWITCH 3012E-2FX	1210 g	78.6 mm	146.4 mm	125 mm
FL SWITCH 3012E-2FX SM	1212 g	78.6 mm	146.4 mm	125 mm
FL SWITCH 3006T-2FX SM	970 g	54.4 mm	146.4 mm	125 mm
FL SWITCH 3012E-2SFX	1202 g	78.6 mm	146.4 mm	125 mm
FL SWITCH 3016E	1226 g	78 mm	144 mm	125 mm
FL SWITCH 4008T-2GT-4FX SM, FL SWITCH 4008T-2GT-3FX SM	1300 g	66 mm	173 mm	140 mm
FL SWITCH 4012T-2GT-2FX, FL SWITCH 4012T-2GT-2FX ST	1285 g	66 mm	173 mm	140 mm
FL SWITCH 4008T-2SFP	965 g	54.4 mm	146.4 mm	125 mm
FL SWITCH 4824E-4GC ¹	4494 g	442 mm	44 mm	375 mm
FL SWITCH 4808E-16FX LC-4GC ¹	4706 g	442 mm	44 mm	375 mm
FL SWITCH 4808E-16FX SM LC-4GC ¹	4700 g	442 mm	44 mm	375 mm
FL SWITCH 4808E-16FX-4GC ¹	4470 g	442 mm	44 mm	375 mm
FL SWITCH 4808E-16FX SM-4GC ¹	4680 g	442 mm	44 mm	375 mm
FL SWITCH 4808E-16FX ST-4GC ¹	4604 g	442 mm	44 mm	375 mm
FL SWITCH 4808E-16FX ST SM-4GC ¹	4710 g	442 mm	44 mm	375 mm
FL SWITCH 4800E-24FX-4GC ¹	4638 g	442 mm	44 mm	375 mm
FL SWITCH 4800E-24FX SM-4GC ¹	4696 g	442 mm	44 mm	375 mm

¹ Does not include power supply

Power

Connection method	Pluggable COMBICON screw connections
Conductor cross section, solid	0.2 mm ² ... 2.5 mm ²
Conductor cross section, stranded	0.2 mm ² ... 2.5 mm ²
Conductor cross section [AWG]	24 ... 12
Supply voltage	24 V DC
Supply voltage range	12 V DC ... 48 V DC
Residual ripple	3.6 V _{PP} (within the permitted voltage range)

Power (FL SWITCH 4800E-P1)

Connection method	Screw
Conductor cross section, solid	0.8 mm ² ... 6 mm ²
Conductor cross section, stranded	0.8 mm ² ... 6 mm ²
Conductor cross section [AWG]	18 ... 10
Supply voltage	48 V DC
Supply voltage range	36 V DC ... 75 V DC
Residual ripple	3.6 V _{PP} (within the permitted voltage range)

Power (FL SWITCH 4800E-P5)

Connection method	Screw
Conductor cross section, solid	0.8 mm ² ... 6 mm ²
Conductor cross section, stranded	0.8 mm ² ... 6 mm ²
Conductor cross section [AWG]	18 ... 10
Supply voltage, nominal	115/230 V AC 110/250 V DC
Supply voltage range	90 V AC ... 264 V AC 88 V DC ... 300 V DC
Frequency, AC	50/60 Hz
Residual ripple	3.6 V _{PP} (within the permitted voltage range)

Current

	Current draw	Inrush current
FL SWITCH 3004T-FX	230 mA (24 V DC)	9.2 A (2 ms)
FL SWITCH 3005	200 mA (24 V DC)	8.6 A (2 ms)
FL SWITCH 3005T	200 mA (24 V DC)	8.6 A (2 ms)
FL SWITCH 3008	210 mA (24 V DC)	8.6 A (2 ms)
FL SWITCH 3008T	210 mA (24 V DC)	8.6 A (2 ms)
FL SWITCH 3004T-FX ST	230 mA (24 V DC)	9.2 A (2 ms)
FL SWITCH 3006T-2FX	330 mA (24 V DC)	8.2 A (2 ms)
FL SWITCH 3006T-2FX ST	330 mA (24 V DC)	8.2 A (2 ms)
FL SWITCH 3016	312 mA (24 V DC)	6.4 A (2 ms)
FL SWITCH 3016T	312 mA (24 V DC)	6.4 A (2 ms)
FL SWITCH 3012E-2FX	713 mA (12 V DC) 354 mA (24 V DC) 190 mA (48 V DC)	5.3 A (271 μs) 12.4 A (141 μs) 30.8 A (77 μs)
FL SWITCH 3012E-2FX SM	636 mA (12 V DC) 320 mA (24 V DC) 169 mA (48 V DC)	5.7 A (305 μs) 12.6 A (149 μs) 40.8 A (75 μs)
FL SWITCH 3006T-2FX SM	330 mA (24 V DC)	8.6 A (2 ms)
FL SWITCH 3012E-2SFX	360 mA (24 V DC)	33.7 A (2 μs)
FL SWITCH 3016E	280 mA (24 V DC)	31.9 A (2 μs)
FL SWITCH 4008T-2GT-4FX SM, FL SWITCH 4008T-2GT-3FX SM	488 mA (24 V DC)	8.0 A (2 ms)
FL SWITCH 4012T-2GT-2FX, FL SWITCH 4012T-2GT-2FX ST	474 mA (24 V DC)	7.7 A (2 ms)
FL SWITCH 4008T-2SFP	278 mA (24 V DC)	7.8 A (2 ms)
FL SWITCH 4824E-4GC	451 mA (48 V DC) ¹ 359 mA (115 V AC) ² 243 mA (230 V AC) ² 107 mA (250 V DC) ²	18.8 A (290 μs) 20.7 A (757 μs) 21.9 A (1.95 μs) 67.0 A (95 μs)
FL SWITCH 4808E-16FX LC-4GC	745 mA (48 V DC) ¹ 553 mA (115 V AC) ² 348 mA (230 V AC) ² 160 mA (250 V DC) ²	19.0 A (290 μs) 18.7 A (757 μs) 22.0 A (1.95 μs) 66.6 A (95 μs)
FL SWITCH 4808E-16FX SM LC-4GC	630 mA (48 V DC) ¹ 476 mA (115 V AC) ² 370 mA (230 V AC) ² 138 mA (250 V DC) ²	19.2 A (290 μs) 18.2 A (757 μs) 22.6 A (1.95 μs) 67.2 A (95 μs)

FL SWITCH 30..., 40... and 48...

Current		
	Current draw	Inrush current
FL SWITCH 4808E-16FX-4GC	738 mA (48 V DC) ¹	19.7 A (290 µs)
	540 mA (115 V AC) ²	19.1 A (757 µs)
	341 mA (230 V AC) ²	22.9 A (1.95 µs)
	158 mA (250 V DC) ²	67.7 A (95 µs)
FL SWITCH 4808E-16FX SM-4GC	707 mA (48 V DC) ¹	20.2 A (290 µs)
	476 mA (115 V AC) ²	19.5 A (757 µs)
	307 mA (230 V AC) ²	23.1 A (1.95 µs)
	138 mA (250 V DC) ²	70.2 A (95 µs)
FL SWITCH 4808E-16FX ST-4GC	731 mA (48 V DC) ¹	19.2 A (290 µs)
	534 mA (115 V AC) ²	18.5 A (757 µs)
	338 mA (230 V AC) ²	22.1 A (1.95 µs)
	157 mA (250 V DC) ²	68.8 A (95 µs)
FL SWITCH 4808E-16FX ST SM-4GC	704 mA (48 V DC) ¹	19.9 A (290 µs)
	500 mA (115 V AC) ²	19.2 A (757 µs)
	331 mA (230 V AC) ²	22.8 A (1.95 µs)
	152 mA (250 V DC) ²	69.8 A (95 µs)
FL SWITCH 4800E-24FX-4GC	908 mA (48 V DC) ¹	19.6 A (610 µs)
	652 mA (115 V AC) ²	19.0 A (463 µs)
	410 mA (230 V AC) ²	22.3 A (483 µs)
	181 mA (250 V DC) ²	60.6 A (460 µs)
	127 mA (370 V DC) ²	66.6 A (470 µs)
FL SWITCH 4800E-24FX SM-4GC	840 mA (48 V DC) ¹	19.9 A (616 µs)
	602 mA (115 V AC) ²	19.6 A (480 µs)
	380 mA (230 V AC) ²	22.9 A (476 µs)
	186 mA (250 V DC) ²	63.2 A (470 µs)
	121 mA (370 V DC) ²	69.2 A (483 µs)

¹ FL SWITCH 4800E-P1

² FL SWITCH 4800E-P5

Ethernet (RJ45)

Connection method	RJ45 female connector, auto negotiation and autocrossing
Transmission speed	
FL SWITCH 4008T-2GT-4FX SM, FL SWITCH 4012T-2GT-2FX	1000 Mbps
All other switches	10/100 Mbps
Transmission length	100 m

Fiber optic interface

Connection method	
FL SWITCH...-FX	SC-Duplex multimode
FL SWITCH...-FX ST	ST multimode
FL SWITCH...-FX SM	SC-Duplex single mode
FL SWITCH 4008T-2SFP, FL SWITCH 3012E-2SFX, FL SWITCH 4824-4GC	SFP ports are dependent upon the SFP module
FL SWITCH 4808E-16FX LC-4GC	LC multimode; SFP ports are dependent upon the SFP module
FL SWITCH 4808E-16FX SM LC-4GC	LC single mode; SFP ports are dependent upon the SFP module
FL SWITCH 4808E-16FX-4GC, FL SWITCH 4800E-24FX-4GC	SC multimode; SFP ports are dependent upon the SFP module
FL SWITCH 4808E-16FX SM-4GC, FL SWITCH 4800E-24FX SM-4GC	SC single mode; SFP ports are dependent upon the SFP module
FL SWITCH 4808E-16FX ST-4GC	ST multimode; SFP ports are dependent upon the SFP module
FL SWITCH 4808E-16FX ST SM-4GC	ST single mode; SFP ports are dependent upon the SFP module
Transmission speed	
FL SWITCH 4008T-2SFP, FL SWITCH 4824E-4GC, FL SWITCH 48...E...	1000 Mbps SFP ports: 1000 Mbps; FX ports: 100 Mbps
All other switches	100 Mbps
Wavelength	
	1300/1310 nm
Transmission length, multimode	
	8.0 km (fiberglass with F-G 62.5/125 0.7 dB/km F1000) 3.3 km (fiberglass with F-G 62.5/125 2.6 dB/km F600) 9.6 km (fiberglass with F-G 50/125 0.7 dB/km F1200) 5.3 km (fiberglass with F-G 50/125 1.6 dB/km F800)
Transmission length, single mode	
	40 km (fiberglass with F-G 9/125 0.36 dB/km) 36 km (fiberglass with F-G 9/125 0.4 dB/km) 29 km (fiberglass with F-G 9/125 0.5 dB/km)

Alarm contact (except FL SWITCH 48...E...)

Voltage, maximum	
FL SWITCH ... T...	250 V AC
FL SWITCH 3005, FL SWITCH 3008	24 V DC
Current, maximum (includes inrush)	
	1 A

Electrical isolation/isolation of the voltage areas

Supply voltage/functional earth ground	500 V, 1 min
--	--------------

Mechanical tests

Shock test in acc. with IEC 60068-2-27	25g, 11 ms half-sine shock pulse
Vibration resistance in acc. with IEC 60068-2-6	5g, 150 Hz, Criterion 3
Free fall in acc. with IEC 60068-2-32	1 m

Conformance

FL SWITCH 3005(T), FL SWITCH 3008(T), FL SWITCH 3004T-FX (ST), FL SWITCH 3006T-2FX (ST), FL SWITCH 3006T-2FX SM, FL SWITCH 4008T-2SFP	NEMA TS 2-2003 2.1.2 (Operating voltage, 24 V DC power) NEMA TS 2-2003 2.8.1.3 and 2.1.7 (Transients, DC power) NEMA TS 2-2003 2.2.7.3 (Low temperature, low voltage test) NEMA TS 2-2003 2.2.7.4 (Low temperature, high voltage test) NEMA TS 2-2003 2.2.7.5 (High temperature, high voltage test) NEMA TS 2-2003 2.2.7.6 and 2.2.7.7 (Temperature, low voltage test) NEMA TS 2-2003 2.2.8.3 ... 2.2.8.5 (Resonant search) NEMA TS 2-2003 2.2.8.3 ... 2.2.8.5 (Vibration endurance test) NEMA TS 2-2003 2.2.9 (Shock)
---	--

FL SWITCH 30..., 40... and 48...

Conformance with EMC Directives

Developed according to IEC 61000-6-2

IEC 61000-4-2 (ESD)	Criterion B
IEC 61000-4-3 (radiated-noise immunity)	Criterion A
IEC 61000-4-4 (burst)	Criterion A
IEC 61000-4-5 (surge)	Criterion B
IEC 61000-4-6 (conducted noise immunity)	Criterion A
IEC 61000-4-8 (noise immunity against magnetic fields)	Criterion A
EN 55022 (noise emission)	Class A

Developed in accordance to IEC 61850-3 (FL SWITCH 30...E... and FL SWITCH 48...E...)

IEC 61000-4-2 (ESD)	Contact: ± 6 kV Air: ± 8 kV
IEC 61000-4-3 (radiated-noise immunity)	10 V/m
IEC 61000-4-4 (burst)	Ports: ± 4 kV DC power: ± 2 kV
IEC 61000-4-5 (surge)	Ports: ± 4 kV DC power: ± 2 kV
IEC 61000-4-6 (conducted noise immunity)	Ports: 10 V DC power: 10 V
IEC 61000-4-8 (noise immunity against magnetic fields)	100 A/m continuous 1000 A/m for 3 s
IEC 61000-4-10 (damped oscillatory magnetic field immunity)	30 A/m
IEC 61000-4-16 (immunity to conducted common mode disturbances)	Ports and DC power: 30 V _{rms} continuous 300 V _{rms} for 1 s (50 Hz)
IEC 61000-4-17 (ripple on DC power supply)	10%
IEC 61000-4-18 (oscillatory waves)	2.5 kV common mode (100 kHz, 1 MHz) 1 kV differential mode (100 kHz, 1 MHz)
IEC 61000-4-29 (voltage dips and voltage interruptions)	30% reduction 0.1 s 60% reduction (dips) 0.1 s ¹ 100% interruptions 0.05 s ¹
EN 55022 (radiated RF emissions)	Class A and B
EN 55022 (noise emission)	Class A and B

¹ Switch restarts at this level

Developed in accordance to IEEE 1613 (FL SWITCH 30...E... and FL SWITCH 48...E...)

IEEE C37.90.3 (ESD)	Contact: ± 8 kV Air: ± 15 kV
IEEE C37.90.2 (RF susceptibility)	Ports: 20 V/m
IEEE C37.90.1 SWC (fast transient)	Ports: ± 4 kV 2.5 kHz DC power: ± 4 kV
IEEE C37.90.1 SWC (oscillatory)	Ports: ± 2.5 kV common mode, 1 MHz DC power: ± 2.5 kV common mode, ± 2.5 kV differential mode, 1 MHz
IEEE C37.90 (dielectric power frequency test)	Ports: 2 kV DC power: 2 kV
IEEE C37.90 (impulse voltage test)	DC power: 5 kV
IEEE 1613 Clause 9 vibration	30 mm/s 1...150 Hz
IEEE 1613 Clause 9 shock	250 mm

IEEE standards

Common name	Original standard	Current standard	Brief description
10Base-T	802.3i	IEEE 802.3-2008 10BASE-T	10Mbps Ethernet over twisted pair
100Base-TX	802.3u	IEEE 802.3-2008 100BASE-TX	100Mbps Fast Ethernet over twisted pair (802.3u)
100Base-FX	802.3u	IEEE 802.3-2008 100BASE-FX	100Mbps Fast Ethernet over optical fiber
Auto-negotiation	802.3u	IEEE 802.3-2008 Clause 28	Auto-negotiate speed and duplex
Auto MDI-X	N/A (HP patented)	N/A	Auto crossover
RS-232	EIA RS-232	TIA-232-F	RS-232 serial interface
Flow Control	802.3x	IEEE 802.3-2008 Annex 31B	MAC control PAUSE (802.3x Flow control)
STP/RSTP	802.1D/802.1w	IEEE 802.1D-2004	Rapid spanning tree protocol
MSTP	802.1s	IEEE 802.1Q-2005	Multiple spanning tree protocol
Link aggregation	802.3ad	IEEE 802.1AX-2008	Link aggregation
VLAN	802.1Q	IEEE 802.1Q-2005	Virtual LAN
IGMP snooping/query	n/a	IETF RFCs 1112, 2236, 4541	IGMP snooping/query for versions 1 & 2
QoS:CoS	802.1Q	IEEE 802.1Q-2005	Class of Service QoS
QoS:DSCP	-	IETF RFC 2474	Differentiated services code point QoS
GVRP	-	IEEE 802.1Q-2005	GARP VLAN registration protocol
GMRP	-	IEEE 802.1D-2004	GARP multicast registration protocol
SNMPv1	IETF RFC 1067	IETF RFC 1157	Simple network management protocol version 1
SNMPv2	n/a	IETF RFC 1901	Simple network management protocol version 2
SNMPv3	n/a	IETF RFC 3411	Simple network management protocol version 3
Port authentication	802.1X	IEEE 802.1X-2010	Port-based network access control
LLDP	-	IEEE 802.1AB-2005	Link layer discovery protocol
DHCP/BootP	-	IETF RFC 2131, 951	Dynamically assigned ip address
SNTP	-	IETF RFC 4330	Simple network time protocol
HTTP	-	IETF RFC 2616	Web pages
IPv4	IETF RFC 760	IETF RFC 791	Internet protocol version 4
TFTP	IETF RFC 783	IETF RFC 1350	Trivial file transfer protocol

Approvals

See phoenixcontact.com for the latest approvals

Firmware updates

Version 1.00	Original release
Version 1.10	Added link layer discovery protocol Added extended management information base (MIB) for SNMP
Version 1.20	Added extended ring and dual ring capability, improved SNTP synchronization
Version 1.21	Added FL SWITCH 48...E... capability, ring operates when booting up in a linear topology, extended ring failure sends a trap message
Version 1.22	Open SSL library security update, selectable SSL support security update, native VLAN configuration (PVID) independent from the port setting in the static VLAN configuration
Version 1.30	Added extended-ring path control, native VLAN ID of the port can be modified when the port is tagged, changed default trust mode with QoS enabled, several bug fixes
Version 1.31	Added HTTPS web page connection with TLS 2048-bit group, extended ring failures are logged on the "Event Table" page, SNTP server functionality, FREAK security feature, enhanced SNTP web, and SNMP interfaces

C Appendices

C 1 List of figures

Section 1

Figure 1-1:	Structure of the FL SWITCH 3006T-2FX	8
Figure 1-2:	Structure of the FL SWITCH 3016	9
Figure 1-3:	Structure of the FL SWITCH 4008T-2GT	11
Figure 1-4:	Structure of the FL SWITCH 4824E-4GC	13
Figure 1-5:	Structure of the FL SWITCH 4808E-16FX...4GC	14

Section 2

Figure 2-1:	DIN rail installation	17
Figure 2-2:	19-inch rack mounting with standard mounting brackets	18
Figure 2-3:	19-inch rack mounting with optional FL RMB 4800E mounting brackets	19
Figure 2-4:	Removal from the DIN rail	20
Figure 2-5:	Power connections	21
Figure 2-6:	Power module installation	22
Figure 2-7:	Power connections for FL SWITCH 48...E...	23
Figure 2-8:	Alarm contact	23
Figure 2-9:	SFP module components	24
Figure 2-10:	SFP module installation	25

Section 3

Figure 3-1:	"Technical Data" page	30
Figure 3-2:	PuTTY login screen	31
Figure 3-3:	Prompt for user password	31
Figure 3-4:	Login parameters entered in PuTTY	32
Figure 3-5:	Switch configuration screen	32
Figure 3-6:	"Telnet" page	33
Figure 3-7:	Position of bits within the IP address	34
Figure 3-8:	Structure of IP addresses	35
Figure 3-9:	IPAssign splash screen	39
Figure 3-10:	Devices sending BootP requests in IPAssign	39

Figure 3-11:	IP parameter settings	40
Figure 3-12:	Completion screen	40
Figure 3-13:	Static assignment of the IP via the serial interface	41
Figure 3-14:	Web Access Mode selection	41
Figure 3-15:	Sign-in Administrative page	42
Figure 3-16:	“IP Configuration” page in Administrator mode	43
Figure 3-17:	IP address assignment via SNMP	44
Figure 3-18:	“Device Information” page	45
Figure 3-19:	“System Identification” page	46
Figure 3-20:	“Login Session” page	47
Figure 3-21:	“Software Update” page	48
Figure 3-22:	“Simple network time protocol configuration” page	50
Figure 3-23:	“Change Password” page	51

Section 4

Figure 4-1:	Mode display	54
Figure 4-2:	“User Accounts” page	55
Figure 4-3:	Select the user account type	56
Figure 4-4:	“User Access Mode Config” page	58
Figure 4-5:	“Configuration Management” page	59
Figure 4-6:	“Save” icon	60
Figure 4-7:	“Configuration File Transfer” page	60

Section 5

Figure 5-1:	“Services” page	63
Figure 5-2:	“Port Configuration Table” page	64
Figure 5-3:	“Port Configuration” page	65
Figure 5-4:	“HTTPS” page	67
Figure 5-5:	“SNMP” page with V1/V2 options	68
Figure 5-6:	“SNMP” page with V3 options	69
Figure 5-7:	“General Security Configuration” page	70
Figure 5-8:	“802.1x Configuration” page	72
Figure 5-9:	“802.1x Configuration Table” page	73
Figure 5-10:	“RADIUS Authentication Server” page	74
Figure 5-11:	“MAC Based Security: Per Port” page	75
Figure 5-12:	“MAC Based Security: Global Discard” page	77
Figure 5-13:	“Trap Configuration” page	78

Figure 5-14:	“Port Table” page	79
Figure 5-15:	“Port Statistics” page	80
Figure 5-16:	“Port Mirroring” page	82
Figure 5-17:	“Adding Source Ports” page	82
Figure 5-18:	“Display” page	83
Figure 5-19:	“Alarm Contact” page	84
Figure 5-20:	“Utilization” page	85
Figure 5-21:	“Event Table” page	86
Figure 5-22:	“MAC Address Table” page	87
Figure 5-23:	“Link Layer Discovery Protocol” page	89
Figure 5-24:	“LLDP Topology” page in IEEE mode	90
Figure 5-25:	“LLDP Topology” page in PROFINET mode	91
Figure 5-26:	“Spanning Tree General” page	93
Figure 5-27:	“Spanning-Tree Config” page	94
Figure 5-28:	“STP Port Table” page	95
Figure 5-29:	“STP Port Config Table” page	96
Figure 5-30:	“STP Port Config” page	97
Figure 5-31:	MSTP example network	99
Figure 5-32:	“MST Global Config” page	100
Figure 5-33:	“MST Config” page	101
Figure 5-34:	“MST Port Config” page	102
Figure 5-35:	Ring restructure process	104
Figure 5-36:	Basic ring	104
Figure 5-37:	Extended ring made from three single rings	105
Figure 5-38:	Incorrect extended ring structure with four coupling ports	105
Figure 5-39:	Two-ring extended ring coupling path with additional switches	106
Figure 5-40:	Extended ring coupling path example	107
Figure 5-41:	Joining rings with a single switch	108
Figure 5-42:	Dual ring topology	108
Figure 5-43:	Supervisory and field networks	109
Figure 5-44:	Improper use of redundant ring	110
Figure 5-45:	“Extended Ring” page	111
Figure 5-46:	Ring port and redundant ring port pairs	112
Figure 5-47:	Incorrect port pairings and connections	113
Figure 5-48:	“Ring General” screen	113
Figure 5-49:	Single ring and ring coupling setup	115
Figure 5-50:	Setup of dual ring functionality	116

Figure 5-51:	Setup of dual ring functionality with ring coupling	116
Figure 5-52:	“Extended Ring: Path Control” page	118
Figure 5-53:	“Quality of Service General” page	120
Figure 5-54:	“Priority Mapping” page	122
Figure 5-55:	“Differentiated Services” page	123
Figure 5-56:	“Flow Control” page	124
Figure 5-57:	“Storm Control” page	125
Figure 5-58:	“Traffic Shaping” page	126
Figure 5-59:	“General Multicast Configuration” page	128
Figure 5-60:	“Static Multicast Groups” page	131
Figure 5-61:	“General Multicast Configuration” page	133
Figure 5-62:	“Current Multicast Groups” page	134
Figure 5-63:	To configure the switch to operate in transparent mode: “IP Configuration” page	137
Figure 5-64:	“General VLAN Configuration” page	138
Figure 5-65:	“Port Based VLAN Configuration” page	140
Figure 5-66:	“Current VLANs” page	141
Figure 5-67:	“Static VLAN Configuration” page	142
Figure 5-68:	Communication between termination devices via VLAN	143
Figure 5-69:	“VLAN Advanced Configuration” page	144
Figure 5-70:	“Native VLAN Port Config Table” page	145
Figure 5-71:	“Native VLAN Port Configuration” page	146
Figure 5-72:	Typical configuration for VLAN and RSTP	147
Figure 5-73:	“Link Aggregation” page	148

C 2 List of tables

Section 1

Table 1-1:	Models.....	6
Table 1-2:	Structure of the FL SWITCH 3006T-2FX	8
Table 1-3:	Structure of the FL SWITCH 3016	10
Table 1-4:	Structure of the FL SWITCH 4008T-2GT	12
Table 1-5:	Structure of the FL SWITCH 4824E-4GC	13
Table 1-6:	Structure of the FL SWITCH 4808E-16FX...4GC	14

Section 2

Table 2-1:	D-SUB 9 connector pinout.....	24
Table 2-2:	RS-232 parameters	24

Section 3

Table 3-1:	Traps for the FL SWITCH 30..., 40... and 48...	29
------------	--	----

Section 5

Table 5-1:	Event table for LLDP.....	88
Table 5-2:	Path costs.....	98
Table 5-3:	Multicast port assignment to the switches	128
Table 5-4:	Port-based VLANs vs. Tagging-based VLANs	136

C 3 Index

A

Access modes	41
Viewing modes	41
Admin mode	53
Advanced VLAN	144
Alarm	84

C

Connections	20
Alarm contacts	23
Power	21
RS-232 (V.24) interface	23
Current multicast groups	134
Customization options	57

D

Default	37
Device information	45
Diagnostics	78
Alarm	84
Display	83
Events	86
LLDP	90
Port mirroring	81
Port statistics	80
Trap configuration	78
Utilization	85
Display	83
Dual ring	108
Dynamic multicast	132

E

Events	86
Extended ring redundancy	103

F

Factory default	37
Flow control	124

G

GVRP protocol	136
---------------------	-----

I

IGMP snooping	132, 133
IP address	34

L

Link aggregation	148
Link layer discovery protocol	87
LLDP	90
Log out	47
Login	30, 47, 53, 54

M

Monitor mode	53
Mounting	17
MST	99
Multicast control	127

N

Native VLAN	145
-------------------	-----

P

Port configuration	64
Port mirroring	81
Port security	70
Port statistics	80
Priority mapping	122
Private MIBs	30
PROFINET mode	91

Q

Quality of service	119
--------------------------	-----

R

RADIUS authentication	71
RADIUS server	73
Redundancy	92
Removal	20
Ring redundancy	103
RSTP	147

S

Saving the configuration	59
--------------------------------	----

FL SWITCH 30..., 40... and 48...

Security	70
Port security	70
Simple Network Management Protocol	28
SNMP	28
SNTP	49
Software update	48
Spanning tree	95
Static multicast groups	129
Static VLAN	141
Storm control	125
Subnet masks	36
System identification	46

T

Telnet	33
Traffic shaping	126
Trap configuration	78

U

User account	57
User accounts	54
User mode	53
User password	51
Utilization	85

V

Viewing modes	41
VLAN	135
VLAN ID management	137

W

Web server protocol	66
Web-based management	27