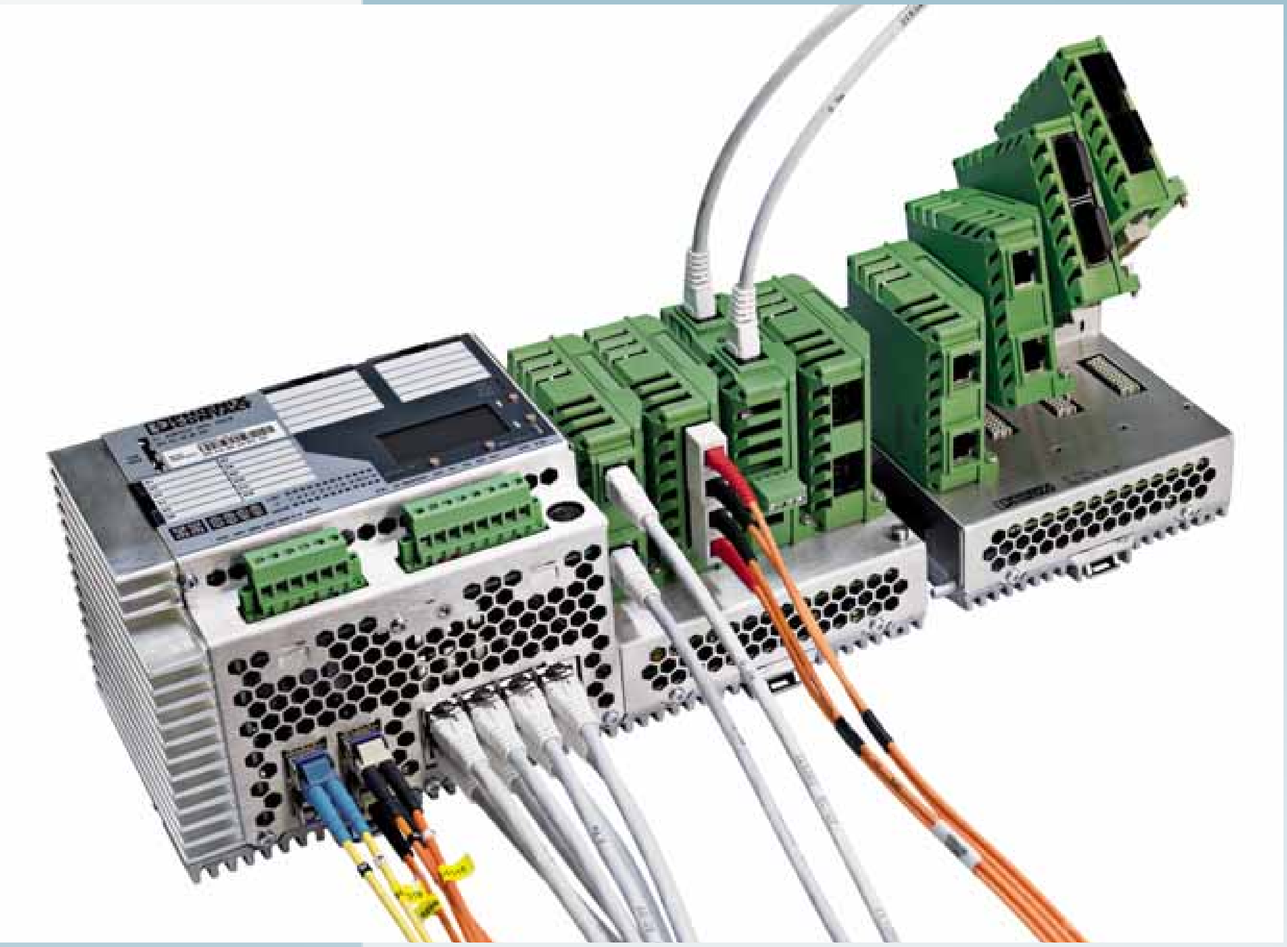
AUTOMATION



User manual

UM EN FL SWITCH GHS for

FL SWITCH GHS 12G/8(-L3)

FL SWITCH GHS 4G/12(-L3)

Gigabit Modular Switch

Order No.: -

PHOENIX CONTACT
INSPIRING INNOVATIONS

AUTOMATION

User manual

Description of the hardware and software functions of Gigabit Modular Switches

05/2011

Designation: UM EN FL SWITCH GHS

Revision: 01

Order No.: —

This user manual is valid for:

Designation	Revision	Order No.
FL SWITCH GHS 12G/8		2989200
FL SWITCH GHS 4G/12		2700271
FL FXT		2989307
FL SWITCH GHS 4G/12-L3		2700786
FL SWITCH GHS 12G/8-L3		2700787

Please observe the following notes

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

User group of this manual

The use of products described in this manual is oriented exclusively to qualified electricians or persons instructed by them, who are familiar with applicable national standards and other regulations regarding electrical engineering and, in particular, the relevant safety concepts.

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

Explanation of symbols used and signal words

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

⚠

DANGER

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

⚠

WARNING

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

⚠

CAUTION

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

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

❗

NOTE

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

ℹ

This symbol and the accompanying text provide the reader with additional information, such as tips and advice on the efficient use of hardware and on software optimization. It is also used as a reference to other sources of information (manuals, data sheets) on the the subject matter, product, etc.

General terms and conditions of use for technical documentation

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

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

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

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

Statement of legal authority

How to contact us

Internet

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

www.phoenixcontact.com

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

www.phoenixcontact.net/download

Subsidiaries

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

Published by

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
DEUTSCHLAND
Telefon +49 - (0) 52 35 - 3-00
Telefax +49 - (0) 52 35 - 3-4 12 00

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

tecdoc@phoenixcontact.com

Table of contents

1 Gigabit Modular Switches

Unless otherwise expressly stated, all information provided in this user manual always applies to both the FL SWITCH GHS 12G/8 and the FL SWITCH GHS 4G/12.

1.1 Properties

The Gigabit Modular Switch is a high-performance managed switch, which covers the port requirements of industrial applications in a modular and flexible way. It also supports all popular Gigabit and Fast Ethernet transmission standards, IT standard protocols, and the PROFINET and Ethernet/IP automation protocols.

The main elements are the two alternative head stations, FL SWITCH GHS 12G/8 and FL SWITCH 4G/12, and the FL FXT extension module.

The switches connect the IT backbone to the automation cells that are to be networked in the production environment via their Gigabit ports.

For cost-effective networking, the head stations already have twelve or four integrated Gigabit ports and support modular extension to up to 28 or 24 ports.

FL SWITCH GHS 12G/8

On the FL SWITCH GHS 12G/8, the twelve Gigabit ports are divided into four Gigabit fiber optic interfaces with SFP modules and eight twisted pair Gigabit ports. In addition, a further eight 100 Mbps ports can be connected using FL IF... interface modules. An FL FXT extension module can be used to create a configuration with up to 28 ports.

FL SWITCH GHS 4G/12

The FL SWITCH GHS 4G/12 has four integrated Gigabit ports, which can either be used as fiber optic interfaces with SFP modules or as twisted pair ports (combo ports). In addition, there are a further four integrated Fast Ethernet twisted pair ports. A further eight 100 Mbps ports can also be connected on this device using FL IF... interface modules. An FL FXT extension module can be used to create a configuration with up to 24 ports.

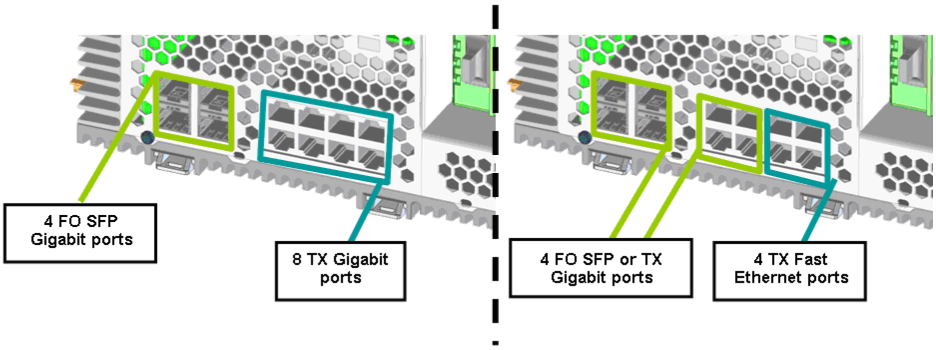


Figure 1-1 Assignment of the Gigabit ports (left: GHS 12G/8, right: GHS 4G/12)

Assignment of the Gigabit ports on the FL SWITCH GHS 4G/12

Gigabit port A: SFP slot X1 or RJ45 port X5

Gigabit port B: SFP slot X2 or RJ45 port X6

Gigabit port C: SFP slot X3 or RJ45 port X7

Gigabit port D: SFP slot X4 or RJ45 port X8

When an RJ45 port is automatically disabled by an SFP module, the Link LED on the RJ45 port lights up orange.

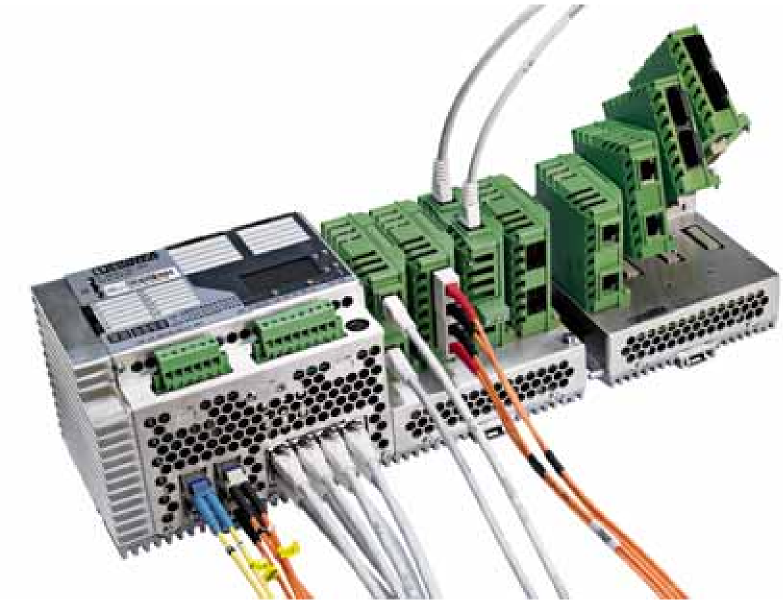


Figure 1-2 Gigabit Modular Switch including extension module and interface modules

1.2 New performance class for future-proof networks

Maximum flexibility - connection of various interfaces

- Flexible connection for IT and automation networks
- Gigabit for the backbone connection in all popular fiberglass standards and twisted pair
- TX, various FX standards, and media polymer fiber, POF SCRJ or HCS fiber that can be assembled in the field can be connected for automation cells
- Power over Ethernet (PoE) enables the integration of easy-to-install termination devices such as cameras, access points or scanners

Maximum performance and port trunking

The new performance class for industrial networks offers:

- Up to 12 integrated Gigabit ports for high-performance use in the backbone
- Support of redundant Gigabit backbones
- Link aggregation according to IEEE 802.3ad/port trunking can be used as an option to further increase the available bandwidth by bundling two to eight cables to create a single logical connection.

Security according to IEEE 802.1X

- Authentication server (RADIUS): Limited network access for external users
- Security in the automation network and protection against sabotage in the network
- Security is controlled centrally instead of being based on MAC addresses and is easier to configure

Display/operator interface for easy diagnostics

- Important parameters can be read and configured quickly and easily without external tools
- Smart operating modes such as PROFINET or Ethernet/IP can be set during the startup phase
- Considerable time savings for servicing
- The IP address, operating modes, link status, etc. can be called and easily read on the display by means of four soft keys

Command line interface

- Fast configuration using the favored command language of IT specialists as an alternative to proven management interfaces such as SNMP and PROFINET
- Offline configuration possible

Slim design width

- With a design width of 285 mm, this is the most compact modular system for DIN rails of its class
- Cost-effective control cabinet integration

Integrated control cabinet monitoring

- Control cabinet monitoring by means of integrated, digital inputs; reduces the number of components required

Port-specific storm control

- Reliable network availability in the event of an error (e.g., broadcast storms)
- Elimination of sources of interference; broadcast, multicast, and unicast bandwidth limits
- Port-specific thresholds can be configured (and can therefore be used selectively)

Easy backup

- Firmware download during runtime operation without shutting down the network
- Easy to switch between two firmware images without the need for time-consuming reinstallation
- Backup image in addition to the current runtime image ensures network availability

Easy assembly

- Flexibility and cost savings thanks to connection media that can be assembled in the field, such as POF, SCRJ, and GI HCS for distances up to 2000 m (with GI HCS)

PROFINET

- The switches can be operated in PC WorX and Step 7 environments as conformance class B PROFINET IO devices. Connections to PLC systems can be easily implemented for diagnostic and communication applications.

Ethernet/IP

- In the Ethernet/IP environment the switches support the IGMP snooping function and multicast filtering.

Smart mode

- For easy configuration, the switches feature Smart mode in which it is possible to change the operating state without additional tools or user interfaces such as CLI, web-based management or SNMP.

Routing Support of numerous routing methods; the additional FL SD Flash/L3/MRM license (Order No. 2700607) is required to activate them.

PROFIenergy Support of the PROFIenergy function.

Additional product properties

- Alternative redundancy mechanisms
  - Rapid Spanning Tree Protocol (RSTP)
  - Optional fast ring detection (FRD) (now also available for 1000 Mbps)
  - Optional large tree support
- Media Redundancy Protocol (MRP) function
- Ethernet IP, support of IGMP snooping
- 256 multicast groups
- 2 alarm contacts
- Backwards compatibility with existing IF modules
- Configuration can be saved on SD Flash cards
- SNMP v1, v2, v3
- User and access management

1.2.1 GHS device view

1.2.1.1 Elements of the head station

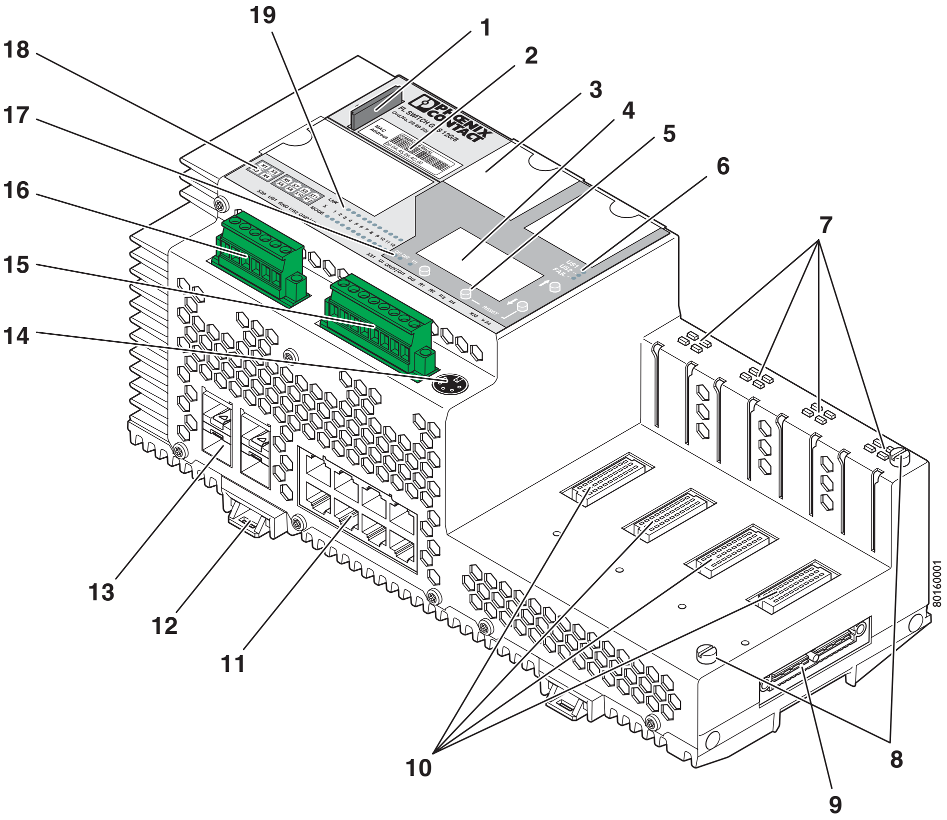


Figure 1-3 Elements of the head station

Table 1-1 Elements of the head station

No.	Function
1	SD card for saving the GHS configuration
2	MAC address in plain text and as a barcode
3	Labeling field for the GHS ports
4	Display for GHS configuration and diagnostics
5	Pushbuttons for operating the display
6	Status indicator for the supply voltage and Fail LED
7	Status indicators for the ports of the interface modules
8	Mounting screws for the extension module
9	Outgoing interface for the extension module
10	Slots for interface modules

Table 1-1 Elements of the head station

No.	Function
11	Ethernet ports of the head station in RJ45 format
12	Fixing clips for snapping onto the DIN rail
13	SFP slots of the head station
14	RS-232 interface in Mini-DIN format for configuration
15	Connection for digital sensors and alarm contacts
16	Supply voltage connection for the device and sensor supply
17	Status indicators for the sensors and sensor supply
18	Diagram of port numbering
19	Status indicators for the ports of the Ethernet ports

1.2.2 Dimensions of the Gigabit Modular Switch

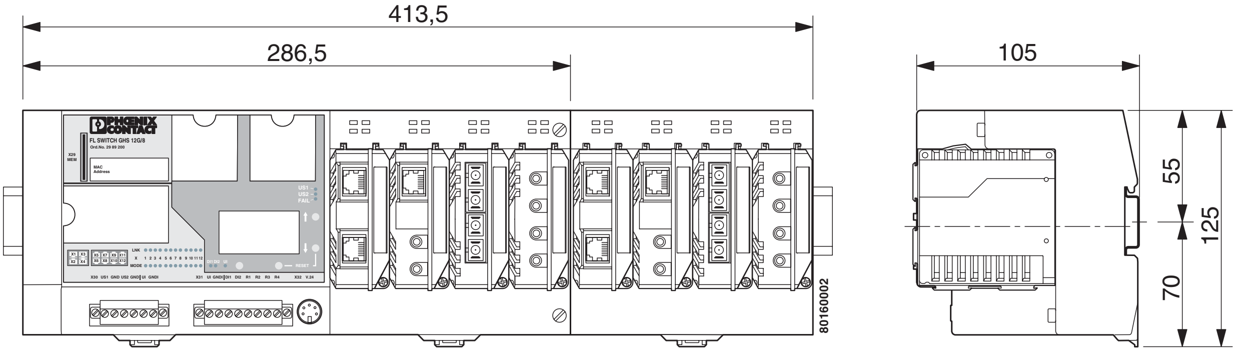


Figure 1-4 GHS housing dimensions in millimeters

1.2.3 View of the interface modules (example)

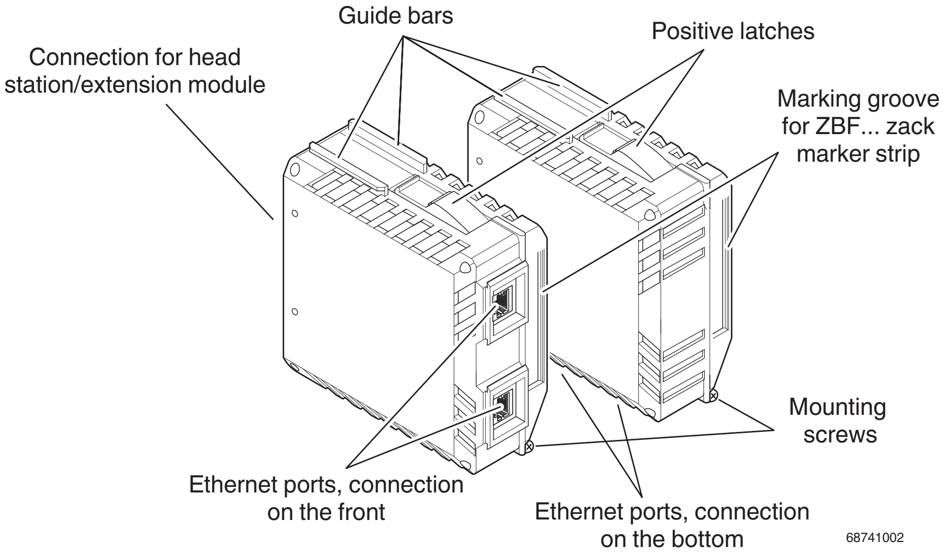

Guide bars
Positive latches
Connection for head station/extension module
Marking groove for ZBF... zack marker strip
Mounting screws
Ethernet ports, connection on the front
Ethernet ports, connection on the bottom
68741002

Figure 1-5 View of the interface modules (example)

- Connection for extension module/head station
  This connector is used to connect the interface module and the extension module or the head station.
- Guide bars
  These bars aid installation and hold the interface modules securely in place.
- Positive latches
  These latches must be pressed in order to remove the interface module (previous versions used mounting screws).
- Ethernet ports
  These are the ports for the various interfaces and connection directions.
- Marking groove for ZBF ... zack marker strip
- Mounting screws to lock the interface modules in place.

2 Mounting and installation

2.1 Mounting and removal

NOTE: Always switch off the supply voltage when mounting/removing the head station and extension modules.

Mount the head station on a clean DIN rail according to DIN EN 50 022 (e.g., NS 35 ... from Phoenix Contact). To avoid contact resistance only use clean, corrosion-free DIN rails. To avoid impermissible loads on the switch in the event of high mechanical strain (strong vibrations or shocks), the DIN rail used should be secured tightly to prevent it turning. In the event of high loads when using "NS 35..." rails, the rails should be screwed/secured every 75 mm.

Before mounting the modules, mount an end clamp (E/AL-NS 35, Order No. 1201662) on the left-hand side next to the head station to stop the modules from slipping on the DIN rail. Once completely installed, mount an end clamp on the right-hand side of the station.

Mounting:

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

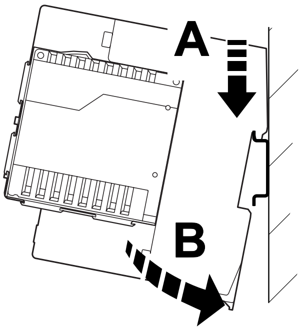


Figure 2-1 Snapping the head station onto the DIN rail

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

Removal:

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

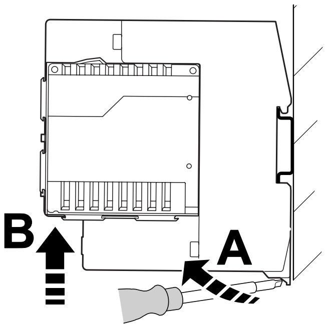


Figure 2-2 Removing the head station

2.2 Mounting and removing the extension module

NOTE: Always switch off the supply voltage when mounting/removing the extension module.

Mounting:

1. Place the module onto the DIN rail from above (A). The upper holding keyway must be hooked onto the top edge of the DIN rail. Push the module from the front towards the mounting surface (B). Check that the positive latches have snapped on properly.

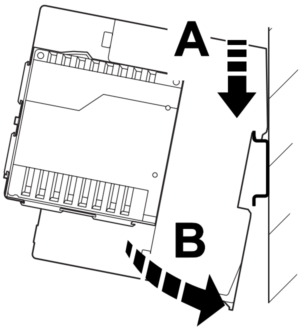


Figure 2-3 Mounting extension modules

2. Now that the extension module is snapped onto the DIN rail, push it along the DIN rail towards the head station (A), until the male connector/female connector of the modules are interlatched and the sides of the modules lie flush with one another. Secure the connection using the two screws (C).

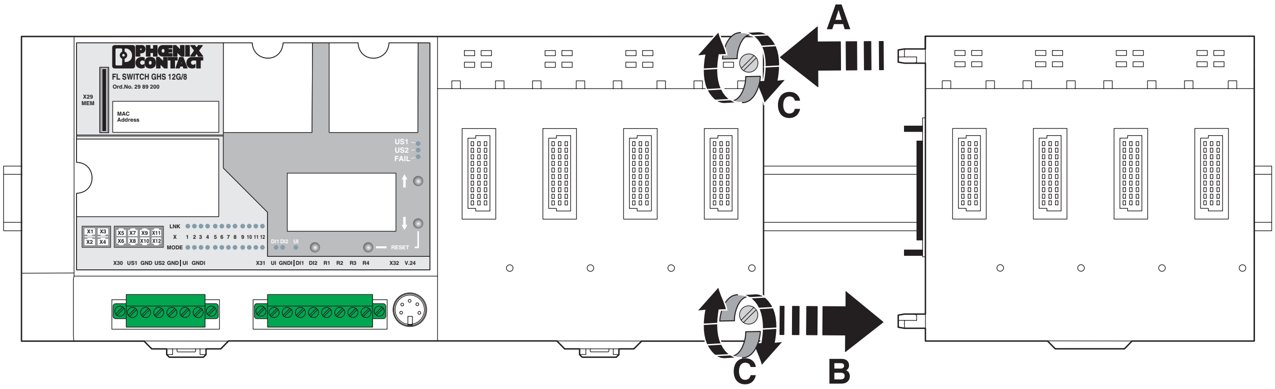


Figure 2-4 Mounting/removing extension modules

Removal:

NOTE: Switch off the supply voltage before removing the extension modules.

1. Remove all plug-in connections or interface modules.
2. Remove the two screws - see (C) in Figure 2-4.
3. Push the right-hand extension module along the DIN rail to the right until the plug-in contact is completely free - see (B) in Figure 2-4.
4. Pull down the holding latches using a suitable tool (e.g., screwdriver).
5. Then swivel the bottom of the module away from the DIN rail slightly (A). Next, lift the module upwards away from the DIN rail.

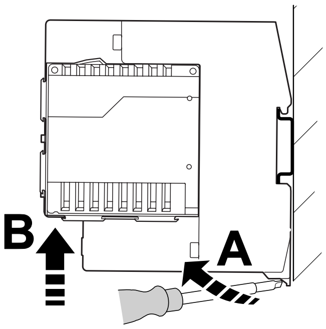


Figure 2-5 Removing extension modules

2.3 Installing the GHS

2.3.1 Connecting the supply voltage to the GHS

24 V DC

The system is operated using a 24 V DC nominal voltage, which can be supplied from separate power supply units if required.

The following connections are available and can be supplied separately if required:

- Supply voltage US1 (terminal blocks US1/GND)
- Supply voltage US2 (terminal blocks US2/GND)
- Sensor supply - here connection for the sensor power supply (terminal blocks UI/GNDI to connector X30, internally to connector X31, terminal blocks UI/GNDI bridged)

Connections are also available for:

- Sensor supply - here connection for the sensor (sensor power supply, terminal blocks UI/GNDI to connector X31, internally to connector X30, terminal blocks UI/GNDI bridged)
- Sensor signals DI1/DI2
- Floating alarm contact 1 (terminal blocks R1/R2)
- Floating alarm contact 2 (terminal blocks R3/R4)

> If redundant power supply monitoring is active (default setting), an error is indicated if only one voltage is applied. A bridge between US1 and US2 prevents this error message. It is also possible to deactivate monitoring via the management interfaces.

2.3.1.1 Example: Supplying the device from one voltage source

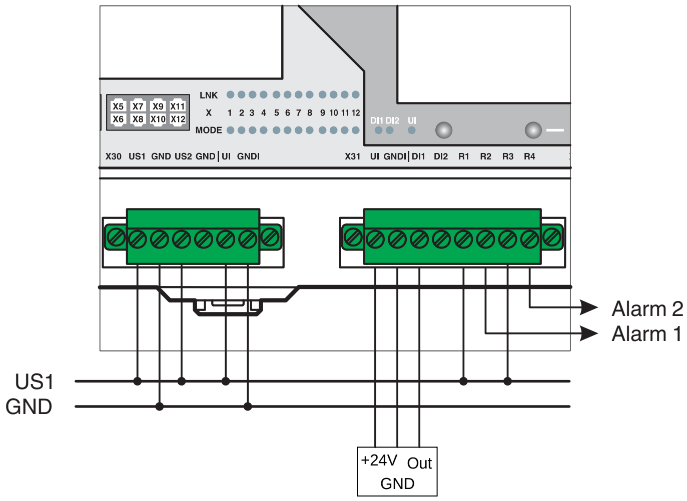

X5 X7 X9 X11
X6 X8 X10 X12
LNK
X 1 2 3 4 5 6 7 8 9 10 11 12
MODE
DI1 DI2 UI
X30 US1 GND US2 GND UI GNDI
X31 UI GNDI DI1 DI2 R1 R2 R3 R4
Alarm 2
Alarm 1
US1
GND
+24V Out
GND

Figure 2-6 Supplying the system using one voltage source

2.3.1.2 Example: Supplying the device from multiple voltage sources

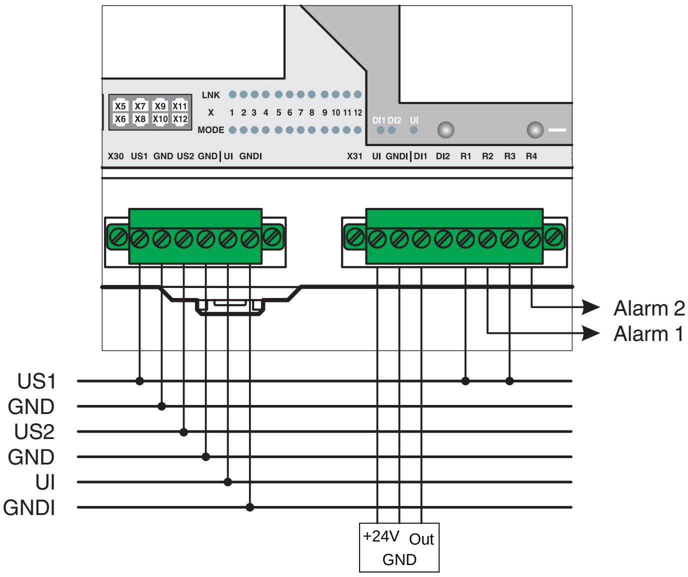


Figure 2-7 Supplying the system using multiple voltage sources

2.4 Mounting and removing the interface modules

NOTE: Ensure that the surface of the head station or extension module housing is clean.

Hot plugging
When inserting and removing interface modules, you do **not** have to switch off the supply voltage. The interface modules are detected automatically and logged to the network management.

Mounting:

1. Insert the interface modules in the slots of the basic modules. The guide bars on the top of the interface modules must be pushed into the guide slots of the basic module without tilting them.

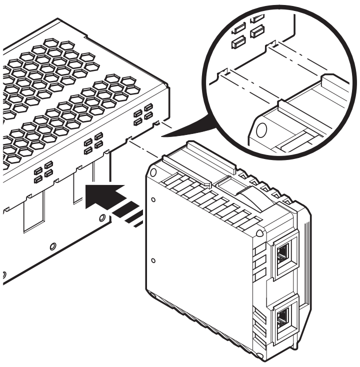


Figure 2-8 Mounting interface modules

2. Now push the interface modules towards the basic module until the connector and the holding clamp are snapped into place.
3. Secure the interface module using the screw on the bottom right-hand side of the interface module.

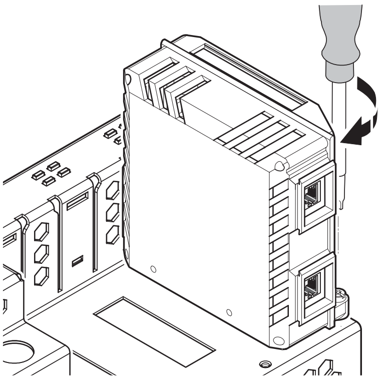


Figure 2-9 Securing the interface module

Removal:

1. Remove the mounting screw.

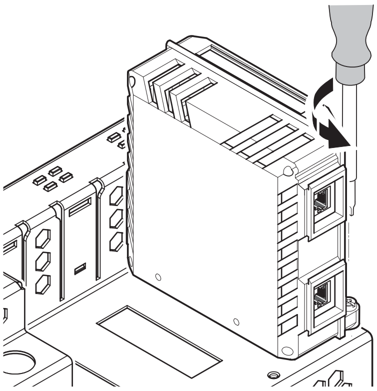


Figure 2-10 Removing the mounting screw on interface modules

2. Press the positive latch (A) and pull out the module (B).

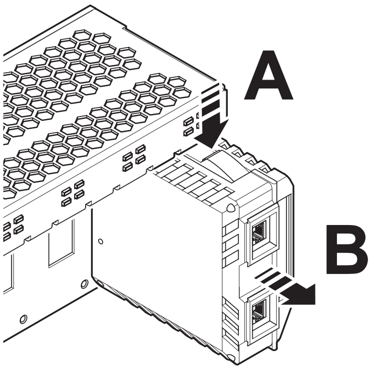


Figure 2-11 Removing the interface module

2.5 Use of SFP slots

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

The SFP modules are available separately as accessories, see Unknown source of cross-reference.

Phoenix Contact only recommends using SFP modules listed in the ordering data on Unknown source of cross-reference.

2.5.1 Elements of the SFP modules

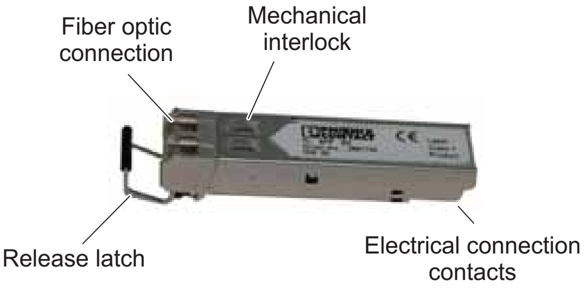


Figure 2-12 Elements of the SFP modules

2.5.2 Mounting the SFP modules (example)

Inserting the SFP modules

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

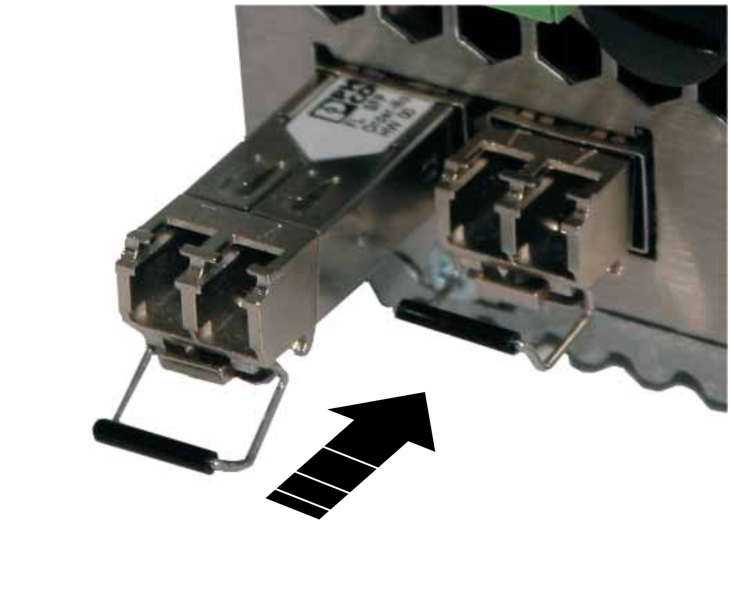


Figure 2-13 Inserting the SFP modules

FL SWITCH GHS 4G12: Inserting an SFP module disables the corresponding RJ45 port. When an RJ45 port is automatically disabled by an SFP module, the Link LED on the RJ45 port lights up orange.

Connecting the fiber optic cable

- When inserting the fiber optic connectors, ensure correct mechanical alignment according to the mechanical recess on the SFP module.

Removing the fiber optic connectors

- Press the arresting latch (A) and pull out the connector (B).

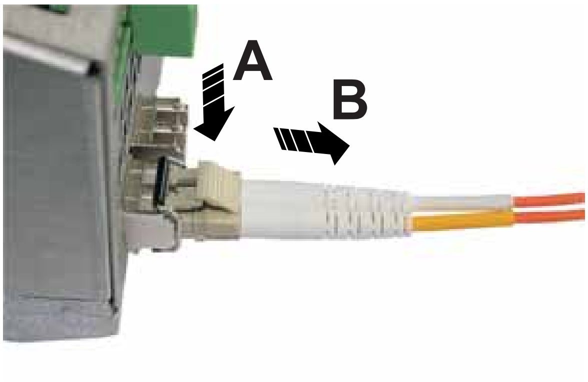


Figure 2-14 Removing the fiber optic connectors

Removing the SFP modules

- Remove the fiber optic connector before removing the SFP module.
- Flip down the release latch (A) and pull out the SFP module (B).

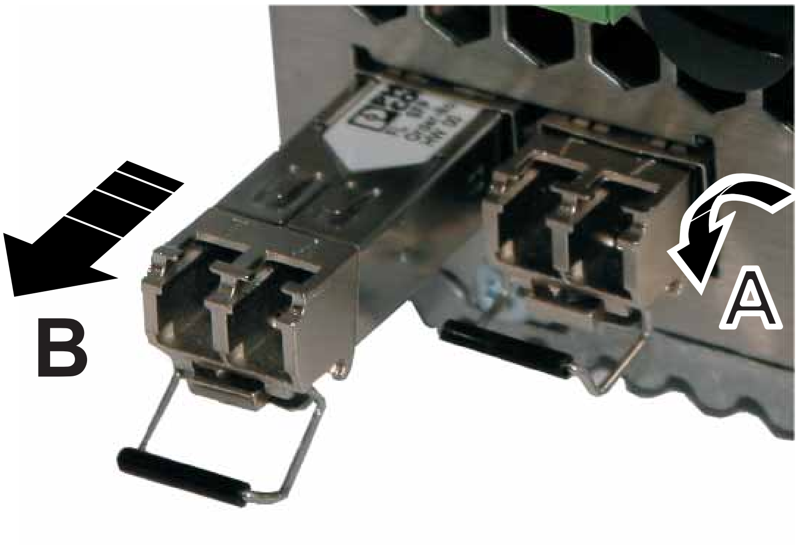


Figure 2-15 Removing the SFP modules

2.6 Starting up the interface modules

2.6.1 FL IF 2TX VS-RJ ...

2.6.1.1 Default upon delivery

When the interface modules are inserted, the auto negotiation and autocrossing functions are activated. Link monitoring for the twisted pair ports is not activated.

If an interface module is inserted in a GHS that has already been parameterized, the existing configuration remains active.

2.6.1.2 Functions

- Auto negotiation
  Auto negotiation is a method whereby the switch automatically detects the operating parameters for the connected network and sets the corresponding parameters (10 Mbps or 100 Mbps data transmission rate and half or full duplex transmission mode) for its RJ45 ports. Automatic port setting eliminates the need for manual intervention by the user. The auto negotiation function can be activated/deactivated via the web interface.
- Autocrossing
  There is no need to distinguish between 1:1 and crossover cables, as the transmit and receive cables are crossed automatically. Autocrossing is only available if auto negotiation is activated.
- Auto polarity
  The polarity is changed automatically by the switch if a pair of twisted pair receive cables (RD+ and RD-) are connected incorrectly.
- Line monitoring/link monitoring
  The switch uses link test pulses according to standard IEEE 802.3 at regular intervals to monitor the connected TP/TX cable segments for short circuits and interrupts.

Ports that are not being used are considered cable interrupts. In addition, a TP/TX path to a deactivated termination device is also considered a cable interrupt, as the connected device cannot send a link test pulse because it is switched off.

2.6.2 FL IF 2FX SC .../FL IF 2FX SM SC .../FL IF 2FX ST-D/FL IF 2POF SCRJ-D

ℹ If the FL IF 2FX (SM) SC... interface is removed and another interface type is inserted in its place, the ports are set to auto negotiation.

2.6.2.1 Default upon delivery

When the interface modules are inserted, they are preset with a data transmission rate of 100 Mbps and full duplex mode, and link monitoring is not activated for the fiber optic ports.

ℹ If a fiber optic interface module is inserted in a GHS that has already been parameterized, the existing configuration remains active with the following exceptions:

- The data transmission rate is set to 100 Mbps
- The duplex method is set to full duplex

If the module is removed, auto negotiation is enabled.

2.6.2.2 Functions

- Line monitoring
  According to standard IEEE 802.3, the switch monitors the connected fiber optic cables for interrupts.

ℹ Ports that are not being used are considered cable interrupts. In addition, a fiber optic path to a deactivated termination device is also considered a cable interrupt, as the connected device cannot send a link test pulse because it is switched off.

- Far End Fault Detection indicates that the connection in the direction of the partner is not OK (the partner does not indicate a link) and therefore at least one fiber within the fiber optic cable is faulty or has not been assembled correctly.

2.6.2.3 Connecting the SC-D connectors

> To prevent dirt from entering the connectors, do not remove the dust protection caps until just before connecting the plug-in connectors. The same applies for the protective caps on the plug-in connectors.

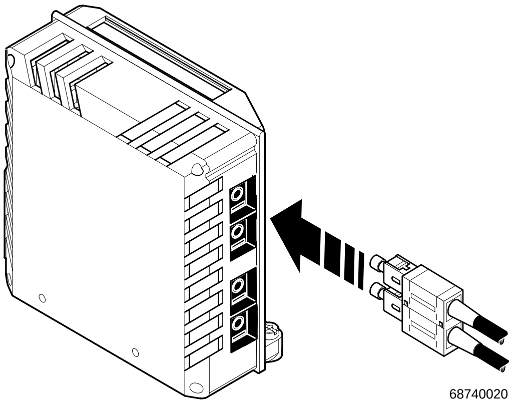


Figure 2-16 Connecting the SC-D connectors

2.6.2.4 Connecting the ST connectors

> To prevent dirt from entering the connectors, do not remove the dust protection caps until just before connecting the plug-in connectors. The same applies for the protective caps on the plug-in connectors.

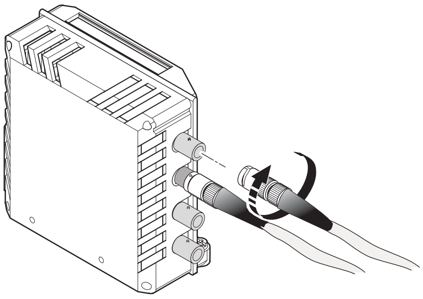


Figure 2-17 Connecting the ST connectors

2.6.2.5 Fiber optic connection between devices

When connecting two fiber optic interface modules, note the signal direction of the fiber optics. The fiber connection is always from the transmitter to the receiver. The SC-D/SCRJ connectors, which are connected using a support, are keyed to ensure that the assignment of the transmit and receive direction is correct.

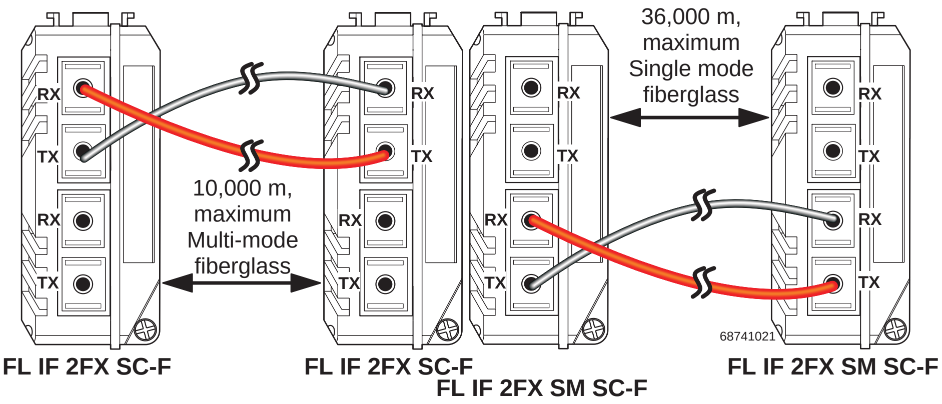


Figure 2-18 Fiber optic connection between devices

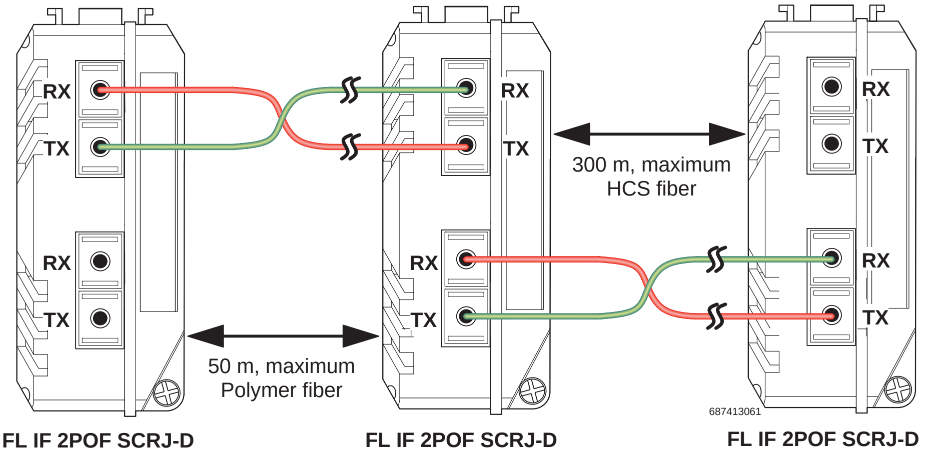


Figure 2-19 Connections with polymer and GI HCS fiber between devices

The maximum length of the fiber optic cables depends on the interface module/fiber type used.

2.6.2.6 SCRJ modules in WBM

Very detailed information about the SCRJ modules is available in WBM, e.g., the port system reserve, alarms or port states are displayed.

The following states can be displayed under "Transceiver status":

- "System hardware does not support diagnosable POF modules" (this hardware does not support POF-SCRJ diagnostics)
- "No POF-SCRJ Interface modules present" (no POF-SCRJ module is plugged in)
- "POF-SCRJ Interface module is present and OK" (the system reserve is greater than 2 dB and is displayed under "RX system reserve")
- "POF-SCRJ Interface module is present, but the system reserve is low" (the system reserve is less than 2 dB, but greater than 0 dB)
- "POF-SCRJ Interface module is present, but the system reserve is exhausted" (no system reserve available - the received optical power is below the required minimum value)

2.6.3 FL IF MEM 2TX-D/FL IF MEM 2TX-D/MRM

ℹ The configuration memory or redundancy manager function of the FL IF MEM 2TX-D/FL IF MEM 2TX-D/MRM is not available when using the GHS and is implemented instead by means of the SD Flash card. The RJ45 ports of the modules can still be used.

2.6.3.1 Network connection

See "FL IF 2TX VS-RJ ..." on page 2-11 and onwards.

2.6.4 FL IF 2PSE-F

ℹ PoE management and PoE information are only available if the 48 V supply is connected to the relevant PoE interface module. The ports can be used as standard RJ45 ports if there is no connected supply.

Properties of PoE mode

- Up to eight PoE interface modules with a total of 16 ports can be operated at the same time on a GHS.
- Configuration is still possible if the interface module is not plugged in or the 48 V supply is not connected.
- PoE management and PoE information are only available if the interface module is plugged in and there is a connected 48 V supply.
- The following management functions are available:
  - Indicate error states for each port on the display and communicate via the alarm contact (yes/no)
  - Connect/disconnect voltage for each port
  - Switch current limitation on or off for loads classified as class 1 devices
- Send traps when the PoE status changes

– The following diagnostic information is displayed:
  - No error
  - Surge voltage/undervoltage
  - Thermal error
  - Overload
  - Disconnected load (current consumption at this port is less than 10 mA, the supply voltage is disconnected from the PoE module)
  - No 48 V supply
  - No PoE interface module detected at this port
  - Missing hardware support due to the system bus
  - Detected class of a connected termination device (class 0 to class 4)
  - Output voltage and output current

2.6.4.1 Default upon delivery

See "FL IF 2TX VS-RJ ..." on page 2-11 and onwards.

2.6.4.2 Connecting the 48 V PoE supply voltage

Connecting the PoE supply

The connector for the PoE supply is located on the bottom of the interface module. Please observe the keying on the connector when inserting it.
The module has a green LED for each port, which indicates the PoE mode. The LED is active if the PoE supply **and** a PD (powered device) are connected. The LED flashes if the module is supplied with less than 48 V.

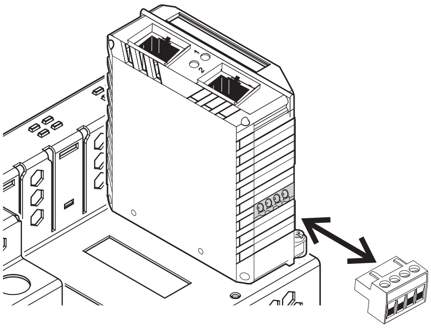


Figure 2-20 Connecting the PoE voltage connector

Connecting the PoE supply

Connect the 48 V PoE supply to terminal blocks 1 (+) and 2 (-). The terminal blocks are bridged within the module. The bridges are located between terminal blocks 1 and 3, and between terminal blocks 2 and 4. The bridges can be used to supply voltage to a **maximum** of three additional PoE interface modules. The supply voltage to additional PoE interface modules must be supplied by power supply units.

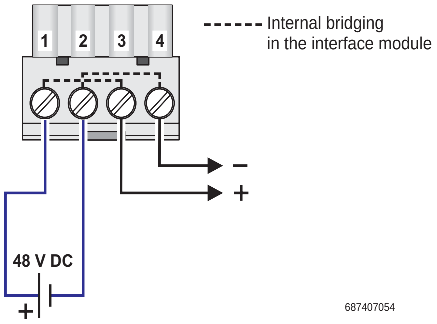


Figure 2-21 Connecting the 48 V PoE supply

Table 2-1 Pin assignment of PoE ports

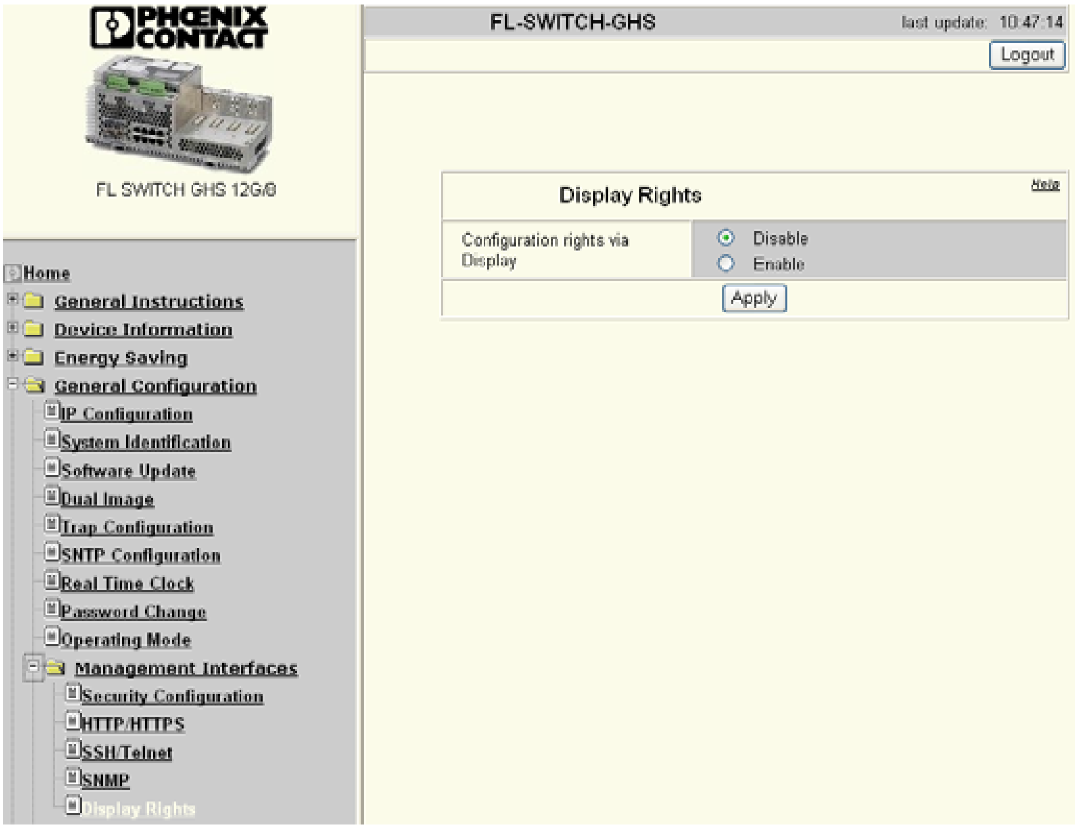
Pin	Assignment	Description	Pin	Assignment	Description
1	RX+/48 V DC	Data/PoE +	5	n. c.	-
2	RX-/48 V DC	Data/PoE +	6	TX-/0 V	Data/PoE -
3	TX+/0 V	Data/PoE -	7	n. c.	-
4	n. c.	-	8	n. c.	-

3 User interfaces

3.1 Display/operator interface

The head station has a display that can be used for both diagnostics and configuration. By default upon delivery (as shown in Figure 3-2), the "Mode" button can be used to select the function of the second port LED (see 3.1.3 "LEDs on the switch and the extension module"). The available functions are shown above the second line, the active function is displayed on a gray background ("ACT" in Figure 3-2). The "Menu" button can be used to select further display functions.

For extended configuration of the device to be supported, this function must be enabled on the "General Configuration/Management Interfaces/Display Rights" web page (default: Enable).



Display Rights

Configuration rights via Display: ● Disable ○ Enable

Figure 3-1 "Display Rights" web page

The structure of the configuration using the display is shown in Figure 3-4 on page 3-6.

3.1.1 Handling the display

There are four buttons for controlling the contents of the display. The selected information is displayed in white text on a gray background; "ACT" is activated in the figure below.

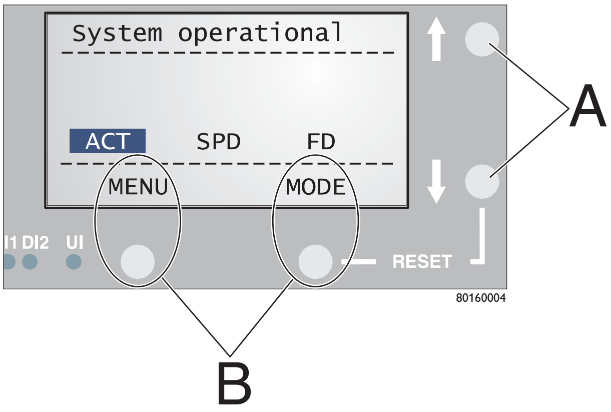


Figure 3-2 Display on the GHS

The "A" buttons are selection buttons (next/back) for the relevant information. The function of the "B" buttons varies; the current function of the button appears directly above the button in the display.

3.1.2 Meaning of the display contents

Messages in the first row

Display	Meaning
System operational (--)	Error-free standard operation
Configuration saved	The configuration has been saved
DCP Discovery	The device is operated as a PROFINET IO device and is waiting for startup using a PROFINET controller. The device cannot be accessed via an IP address.
Profinet Connection	PROFINET connection established
Profinet BusFailure	PROFINET communication connection faulty
PN-Config Diff	User configuration and PROFINET configuration differ
No IP assigned (01)	The GHS does not have an IP address
Upd. process (03)	Firmware update started
Write to Flash (04)	The firmware is saved in the Flash memory
Update finished(05)	Firmware update complete
System Reboot (rb)	Device is booting
TFTP upd. fail (17)	Firmware transfer via TFTP failed
Wrong upd. img.(19)	The transferred file is not a valid firmware file
0P	The configuration is being read from the card
Ec	The card and device configuration are identical
dC	The card and device configuration differ
0C	No valid configuration available on the card
1C	Cannot read the card
SD-Card write protected	The card is write-protected

Event messages

The middle section of the display can be used to indicate events in the form of a static display. Each event is indicated by a combination of three letters. When the cursor is positioned over the event using the selection buttons, explanatory text is displayed above the bottom line in the display.

Display	Meaning
MRP	MRP ring failure
LNK	Link monitor alarm
PN	PROFINET connection

3.1.3 LEDs on the switch and the extension module

Des.	Color	Status	Meaning
US1	Green	ON	Supply voltage 1 in the tolerance range
		OFF	Supply voltage 1 too low
US2	Green	ON	Supply voltage 2 in the tolerance range
		OFF	Supply voltage 2 too low
FAIL	Red	ON	Alarm contact open, i.e., an error has occurred
		OFF	Alarm contact closed, i.e., an error has not occurred
DI1/2	Green	ON	Digital input signal 1/2 present
		OFF	Digital input signal 1/2 not present
UI	Green	ON	Sensor supply voltage present
		OFF	Sensor supply voltage not present
A Link LED is located on the front of the housing or above the interface module slot for each port			
LNK (Link)	Green	ON	Link active
		OFF	Link not active
A Link LED is located on the front of the housing or above the interface module slot for each port. The function of the second LED (MODE) for each port can be selected using a switch on the device, which controls all ports (see also example below). There are three options:			
ACT (Activity)	Green	ON	Sending/receiving telegrams
		OFF	Not sending/receiving telegrams
SPD (Speed)	Green/ yellow	ON (yellow)	1000 Mbps
		ON (green)	100 Mbps
		OFF	10 Mbps if Link LED is active
FD (Duplex)	Green	ON	Full duplex
		OFF	Half duplex if Link LED is active
ACT and SPD and FD simultaneously	Green	Flashing	PROFINET device identification
ACT or SPD or FD (selected by mode switch)	Green	Flashing	No IP parameter present following restart

Example:

In Figure 3-3, the display shows that the mode LED means that "ACT - Activity" is selected. In conjunction with the LEDs for port 1 (X1) to port 12 (X12), the device now indicates the following information:

– Only port 1, port 3, and port 4 are connected and have a link
– Data is currently only being transmitted to port 1

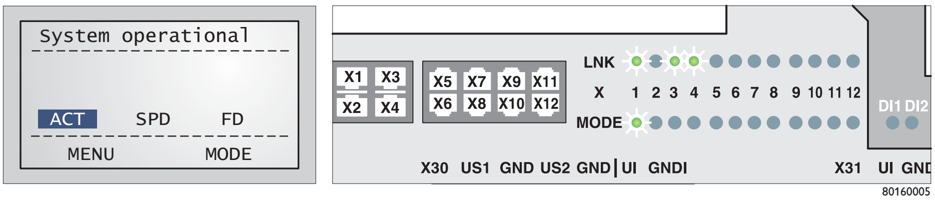


Figure 3-3 Example for status indicators

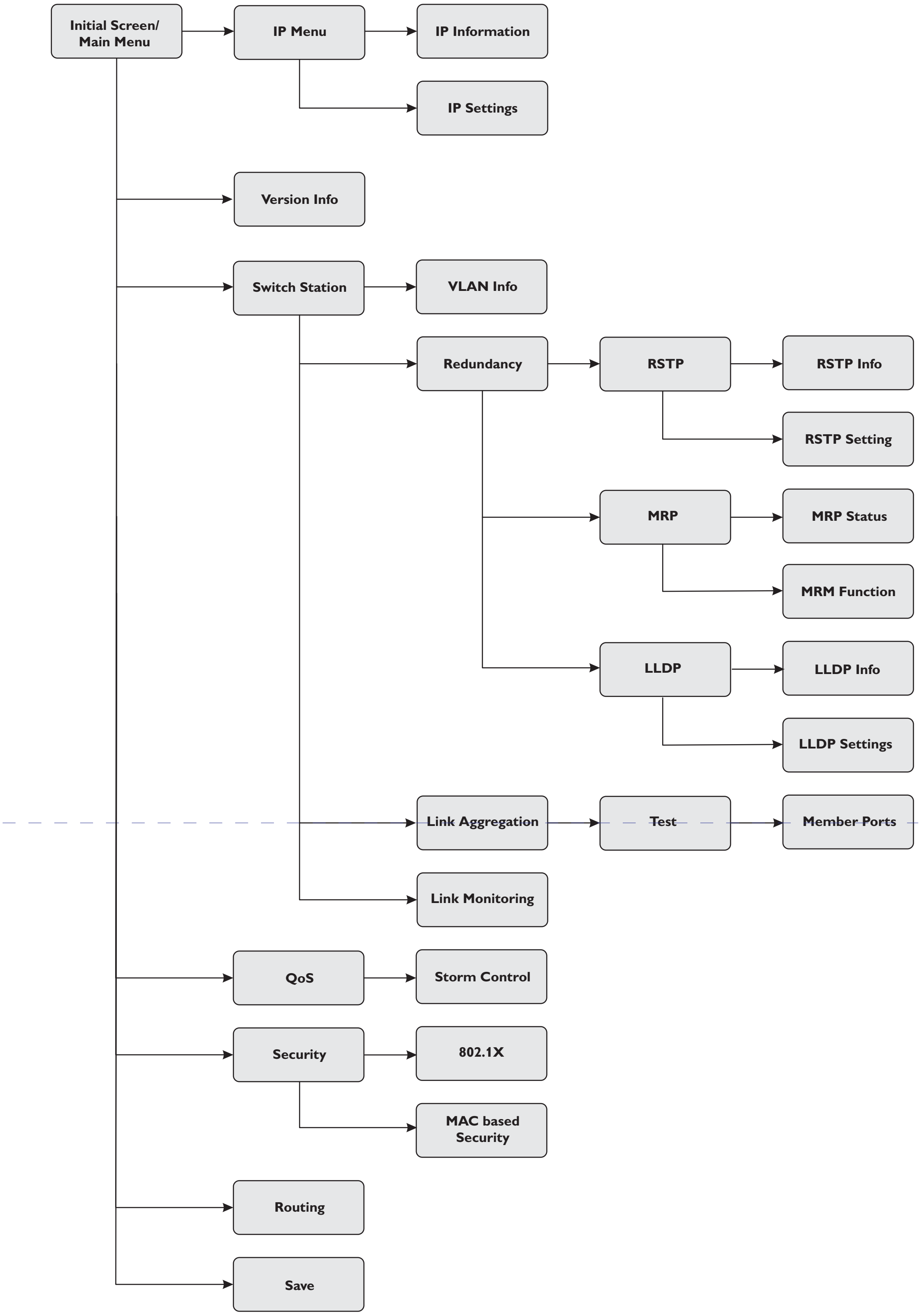


Figure 3-4 Structure of the display configuration

3.2 RS-232 interface for external management

The 6-pos. Mini-DIN female 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 (for an appropriate cable, please refer to Unknown source of cross-reference). Set the following transmission parameters:

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

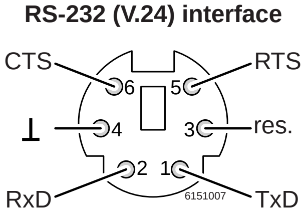


Figure 3-5	Transmission parameters and assignment of the RS-232 interface

3.3 CLI management

The command line interface (CLI) can be used to operate all the functions of the device via a local connection or a network connection. It enables secure administration of the GHS via V.24 (RS-232), Telnet or Secure Shell (SSH).

CLI provides IT specialists with the usual environment for configuring IT devices. The "Command Line Interface" reference manual provides detailed information about using the command line interface (CLI) and its commands. The commands in the CLI of the GHS are grouped logically.

The CLI (command line interface) enables device configuration in text mode. The commands are entered via the keyboard as character strings.

The CLI supports the following modes:

User mode - When you log into the CLI, you will automatically be in user mode. User mode has a limited range of commands. Prompt:

```
(FL SWITCH GHS) >
```

Privileged mode - In order to access the full scope of commands, switch to privileged mode (see 3.3.2.4 "Calling privilege mode"). In privileged mode, you can execute all exec commands. Prompt:

```
(FL SWITCH GHS) #
```

3.3.1 Calling commands/syntax

3.3.1.1 Syntax

When you log into the CLI, you will be in user mode. When you enter a command in the CLI and press <ENTER>, a search is carried out for the command in the command tree.
If the command is not found, the message that is output indicates the error.
The user wants to execute the "logout" command, but enters the command incorrectly and presses <ENTER>. The CLI then outputs an error message:

```
(FL SWITCH GHS) >logout Error[1]: Invalid command 'logout'
```

3.3.1.2 Command tree

The commands in the CLI are organized in a tree structure. The commands and any corresponding parameters are branched until the end point is reached. On each entry, the CLI checks whether the command and all parameters have been entered completely. Only then can the command be executed by pressing <ENTER>.

3.3.1.3 Keyboard entries for the CLI

Table 3-1 Description of keyboard shortcuts

Keyboard shortcut	Description
Ctrl+A	Go to start of line
Ctrl+B	Go back one character
Ctrl+D	Delete next character
Ctrl+E	Go to end of line
Ctrl+F	Go forward one character
Ctrl+K	Delete characters through to the end of the line
Ctrl+N	Switch to next line in memory
Ctrl+P	Switch to previous line in memory
Ctrl+Q	Enable serial flow
Ctrl+R	Rewrite line or insert contents
Ctrl+S	Disable serial flow
Ctrl+T	Replace previous character
Ctrl+U	Delete characters through to the start of the line
Ctrl+W	Delete previous word
Ctrl+X	Delete characters through to the start of the line
Ctrl+Y	Call from last deleted character
Ctrl+Z	Switch to origin
Del, BS	Delete last character
Tab, spacebar	Complete line
Exit	Switch to next level up
?	Display selection options

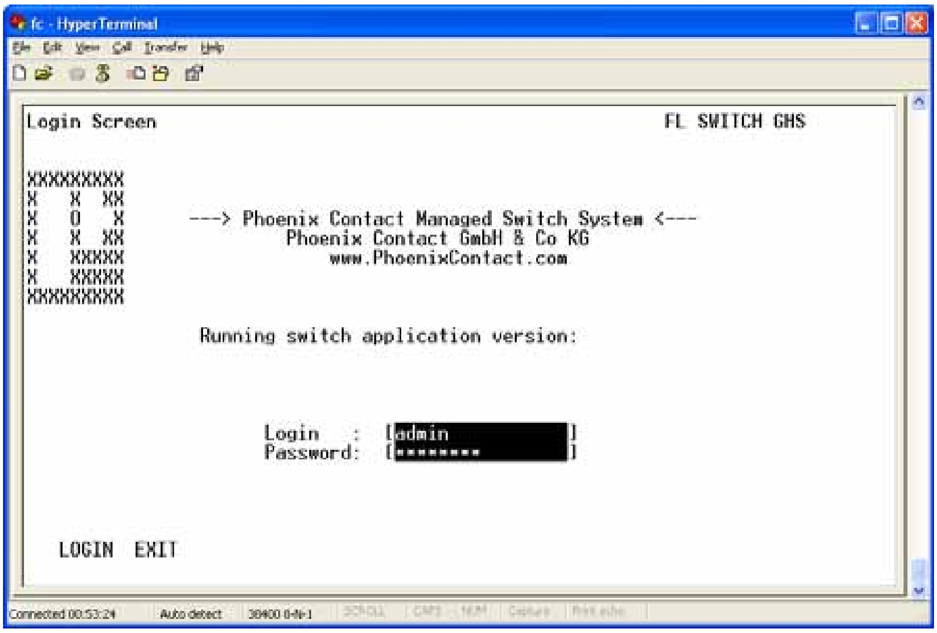
3.3.2 CLI via V.24 (RS-232) - General function

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

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

3.3.2.1 Calling the user interface

Connect the PC and the switch using a suitable cable (PRG CAB MINI DIN, Order No. 2730611) and start the terminal (e.g., HyperTerminal, PuTTY, etc.). Use the VT100 emulation. After establishing the connection, press ENTER on the PC. The screen contents are then requested by the switch and you have the option of choosing between the CLI and the serial configuration menu. Select "2" for the serial interface.



```
Login Screen                                              FL SWITCH GHS

XXXXXXXXX
X   X  XX
X   O   X        ---> Phoenix Contact Managed Switch System <---
X   X  XX              Phoenix Contact GmbH & Co KG
X   XXXXX                  www.PhoenixContact.com
X   XXXXX
XXXXXXXXX

                  Running switch application version:



                        Login   :  [admin          ]
                        Password:  [*********      ]



   LOGIN  EXIT
```

Figure 3-6 Serial screen

When the serial interface is called, you must log in. The default settings are:

User: **admin**

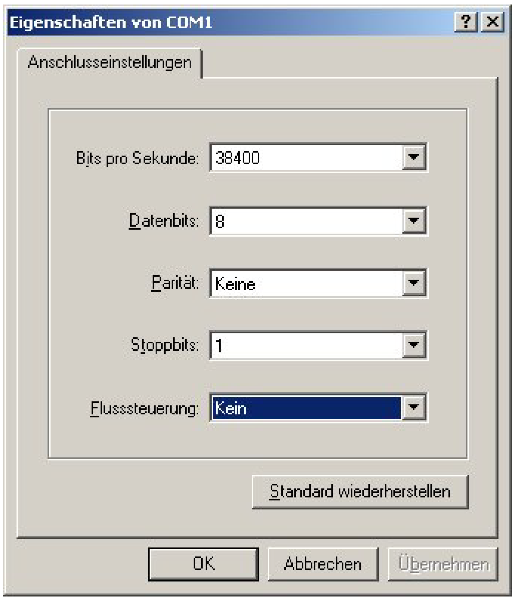
Password: **private**

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

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

3.3.2.2 Interface configuration

Make the following settings on your Windows PC.



Bits pro Sekunde: 38400

Datenbits: 8

Parität: Keine

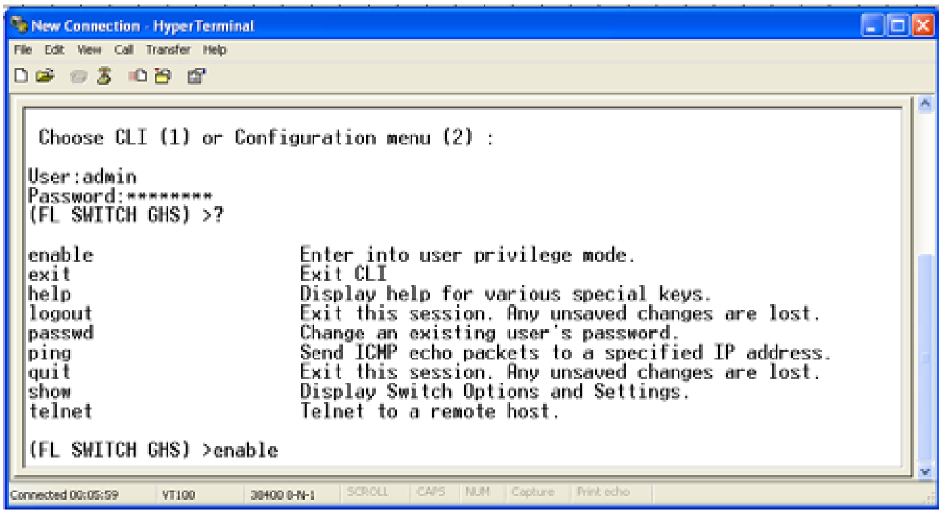
Stoppbits: 1

Flusssteuerung: Kein

Figure 3-7 HyperTerminal configuration

3.3.2.3 Calling the user interface

Connect the PC and the switch using a suitable cable (PRG CAB MINI DIN, Order No. 2730611) and start the terminal (e.g., HyperTerminal, PuTTY, etc.). Use the VT100 emulation. After establishing the connection, press ENTER on the PC. The screen contents are then requested by the switch and you have the option of choosing between the CLI and the serial configuration menu. Select "1" for the CLI.



```
 Choose CLI (1) or Configuration menu (2) :

User:admin
Password:********
(FL SWITCH GHS) >?

enable                          Enter into user privilege mode.
exit                            Exit CLI
help                            Display help for various special keys.
logout                          Exit this session. Any unsaved changes are lost.
passwd                          Change an existing user's password.
ping                            Send ICMP echo packets to a specified IP address.
quit                            Exit this session. Any unsaved changes are lost.
show                            Display Switch Options and Settings.
telnet                          Telnet to a remote host.

(FL SWITCH GHS) >enable
```

Figure 3-8 CLI screen

When the CLI is called, you must log in. The default settings are:

User: **admin**

Password: **private**

After logging in, you are at the top level in the CLI. Display:

```
(FL SWITCH GHS) >
```

If you now enter "?", a list of all other possible commands will be displayed. In this case:

```
enable
exit
logout ...
```

Enter the desired word with the corresponding arguments and confirm with ENTER. If you do not know the corresponding arguments for the desired command, add "?" to the command (see also Figure 3-9 on page 3-11). Example:

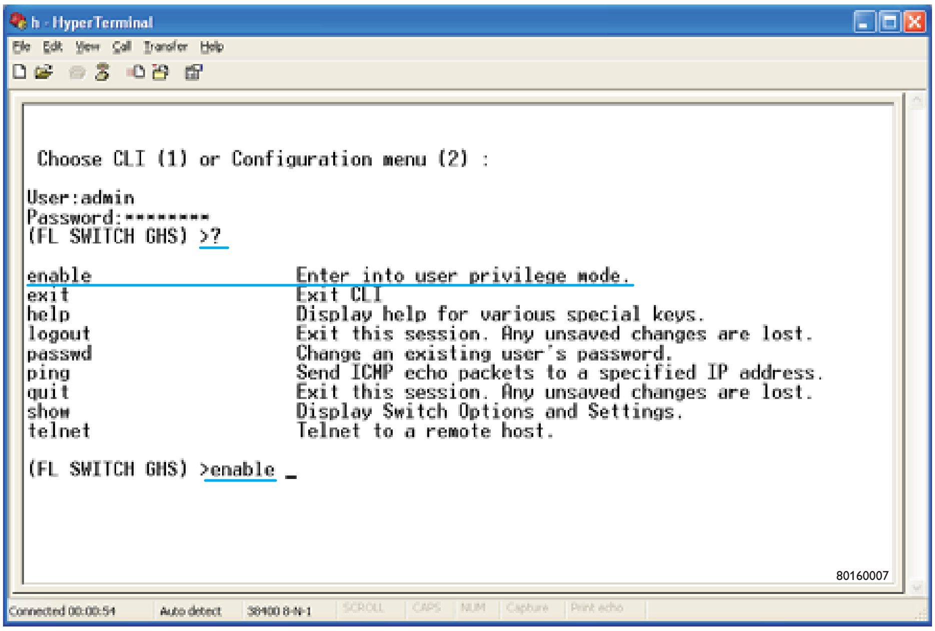
```
(FL SWITCH GHS) >show ?
```

3.3.2.4 Calling privilege mode

In privilege mode, you have access to all the CLI options. You can tell that you are in privilege mode, as the cursor in the CLI changes from ">" to "#".

Procedure:

- Call the CLI as described above.
- Log in.
- Enter "enable". Confirm the password prompt that then appears by pressing ENTER.



h - HyperTerminal
File Edit View Call Transfer Help
80160007
Connected 00:00:54 Auto detect 38400 8-N-1 SCROLL CAPS NUM Capture Print echo

```
 Choose CLI (1) or Configuration menu (2) :

User:admin
Password:********
(FL SWITCH GHS) >?

enable                    Enter into user privilege mode.
exit                      Exit CLI
help                      Display help for various special keys.
logout                    Exit this session. Any unsaved changes are lost.
passwd                    Change an existing user's password.
ping                      Send ICMP echo packets to a specified IP address.
quit                      Exit this session. Any unsaved changes are lost.
show                      Display Switch Options and Settings.
telnet                    Telnet to a remote host.

(FL SWITCH GHS) >enable _
```

Figure 3-9 Calling the list of arguments and privilege mode

3.3.3 CLI via SSH - General function

A SSH (Secure Shell) connection can be used to establish a communication connection with an external management station via the Ethernet network.

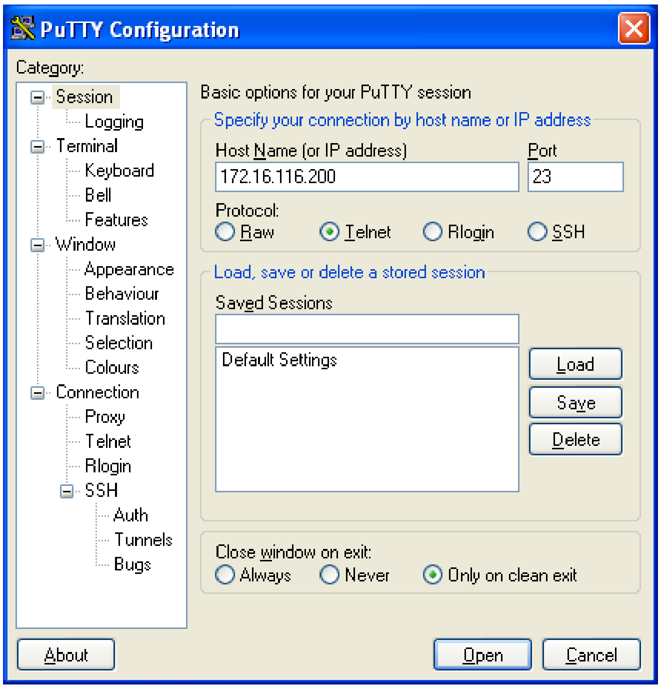
> SSH is deactivated by default upon delivery. It must be activated prior to use and a security context must be stored on the switch.

In order to use the SSH connection, the switch must already have an IP address. This IP address may, for example, have been set via the CLI or the serial connection or may have been assigned via the automatic BootP or DHCP mechanisms (see also 4.3.1 "Assigning IP parameters with IPAssign").

The communication connection is established using a corresponding SSH client between the switch and a PC (e.g., PuTTY) and enables access to the CLI user interface via a network connection.

3.3.3.1 Calling the CLI

- Start your SSH client (PuTTY in this example).
- In the "Host Name (or IP address)" input field, enter the current IP address of your device. The IP address comprises four decimal numbers ranging from 0 to 255. These four decimal numbers are separated by dots. Example: 172.16.116.200



Basic options for your PuTTY session

Specify your connection by host name or IP address

Host Name (or IP address): 172.16.116.200

Port: 23

Protocol: ○ Raw ● Telnet ○ Rlogin ○ SSH

Load, save or delete a stored session

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 3-10 SSH client screen

When the CLI is called, you must log in. The default settings are:

User: **admin**

Password: **private**

After logging in, you are at the top level in the CLI. Display:
`(FL SWITCH GHS) >`

If you now enter "?", a list of all other possible commands will be displayed. In this case:

```
enable
exit
logout ...
```

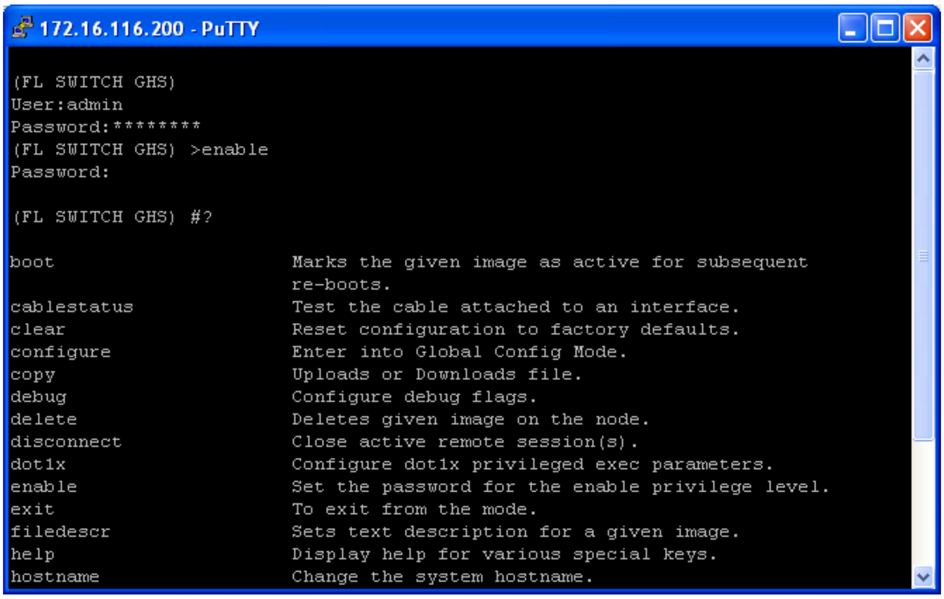
Enter the desired word with the corresponding arguments and confirm with ENTER. If you do not know the corresponding arguments for the desired command, add "?" to the command (see also Figure 3-9 on page 3-11). Example:
`(FL SWITCH GHS) >show ?`

3.3.3.2 Calling privilege mode

In privilege mode, you have access to all the CLI options. You can tell that you are in privilege mode, as the cursor in the CLI changes from ">" to "#".

Procedure:

- Call the CLI as described above.
- Log in.
- Enter "enable". Confirm the password prompt that then appears by pressing ENTER.



```
(FL SWITCH GHS)
User:admin
Password:********
(FL SWITCH GHS) >enable
Password:

(FL SWITCH GHS) #?

boot                     Marks the given image as active for subsequent
                         re-boots.
cablestatus              Test the cable attached to an interface.
clear                    Reset configuration to factory defaults.
configure                Enter into Global Config Mode.
copy                     Uploads or Downloads file.
debug                    Configure debug flags.
delete                   Deletes given image on the node.
disconnect               Close active remote session(s).
dot1x                    Configure dot1x privileged exec parameters.
enable                   Set the password for the enable privilege level.
exit                     To exit from the mode.
filedescr                Sets text description for a given image.
help                     Display help for various special keys.
hostname                 Change the system hostname.
```

Figure 3-11 Switching to privilege mode and calling the list of arguments

3.4 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. Comprehensive configuration and diagnostic functions are clearly displayed on a graphical user interface. Every user with a network connection to the device has read access to that device via a browser. Depending on the physical structure of the switch, various information about the device, the set parameters, and the operating state can be viewed.

ℹ Modifications can only be made by entering the valid login details. By default upon delivery, the user name is "**admin**" and the password is "**private**" or "**private_**" for SNMPv3.

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

3.5 SNMP management

ℹ The device-specific MIB files for the GHS can be downloaded from the device via the web interface (Device Information/Technical Data/Device Description).

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

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

ℹ By default upon delivery, the user interfaces of the device accept "private" as the password. Since the SNMP specification for SNMPv3 specifies a minimum password length of 8 characters, please use "private_" for this user interface.

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

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

3.5.1 SNMP interface

All managed Factoryline components have an SNMP agent. This agent of an FL SWITCH GHS 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-M MIB).

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

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

By default upon delivery, the user interfaces of the device accept "private" as the password. Since the SNMP specification for SNMPv3 specifies a minimum password length of 8 characters, please use "private_" for this user interface.

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

Management Information Base (MIB)

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

Agent

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

Table 3-2 Traps for the GHS

Trap	Meaning
trapAdminPasswdAccess	Sent to the defined trap receivers on each modification or attempted modification of the device password and contains information about the status of the last modification or attempted modification.
trapFWHealth	Sent on each firmware-related modification and contains additional information about the firmware status.
trapFWConf	Sent each time the configuration is saved and informs the management station that the configuration has been saved successfully. This trap is sent in the event of configuration modifications (port name, port mode, device name, IP address, trap receiver address, port mirroring, etc.), which are not yet saved permanently. The trap also provides a warning that, if not saved permanently, the changes will be lost on a reset.
trapPowerSupply	Sent each time the redundant power supply fails.
tarpSecurityPort	Sent each time an impermissible MAC address is received at a port where MAC-based security is activated.
trapRstpRingFailure	Sent in the event of a link interrupt in the redundant RSTP ring.
trapPofScrjPort	Sent each time one of the PoE ports reaches or exits a critical state.
trapPoePort	Sent each time one of the POF-SCRJ ports reaches or exits a critical state.
trapMrpStatusChange	Sent each time the MRP manager changes status.
trapTemperatureManagement	Sent when the permissible temperature range is exited.
trapDigitalInput	Sent each time one of the digital inputs changes status.
trapManagerConnection	Trap to test the connection between the SNMP agent and the network management station.

Private MIBs

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

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

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

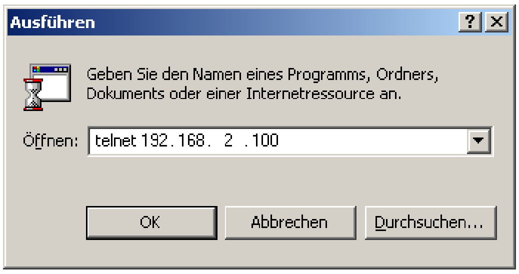
The aging time (default: 40 seconds) is not set using the private MIBs, instead it is set using the "dot1dTpAgingTime" MIB object (OID 1.3.6.1.2.1.17.4.2). The available setting range is 10 - 825 seconds.

3.6 Configuring the Telnet terminal

In order to use the Telnet connection, the switch must already have an IP address. This IP address may, for example, have been set via the CLI or the serial connection or may have been assigned via the automatic BootP or DHCP mechanisms (see also 4.3.1 "Assigning IP parameters with IPAssign").

Establishing the Telnet connection

Connect the PC and the switch to an Ethernet network. From the Start menu, select the "Run..." option. Enter the following command and the IP address of the device. Click "OK" to establish the connection to the switch.



Geben Sie den Namen eines Programms, Ordners, Dokuments oder einer Internetressource an.

Öffnen: telnet 192.168. 2 .100

Figure 3-12 Establishing the Telnet connection

When the Telnet interface is called, you must log in. The default settings are:

User: **admin**

Password: **private**

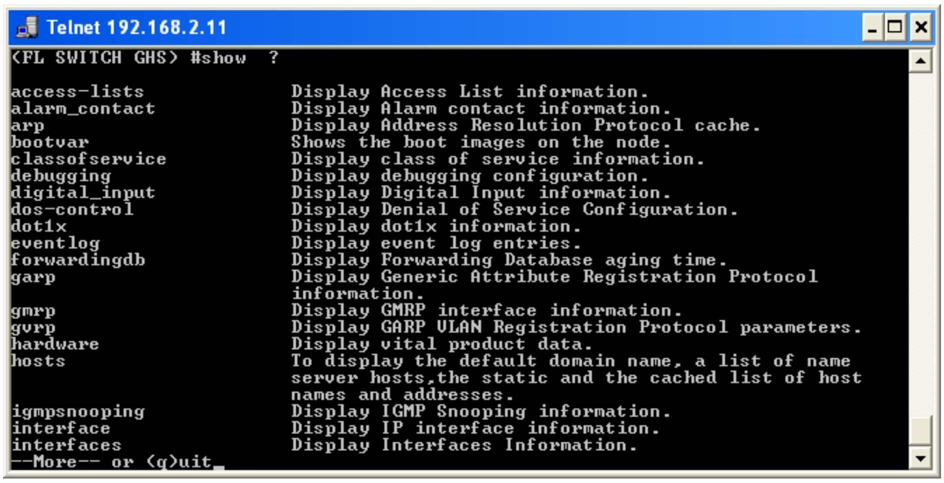
After logging in, you are at the top level in the Telnet interface. Display:

```
(FL SWITCH GHS) >
```

If you now enter "?", a list of all other possible commands will be displayed. In this case:

```
access-lists
alarm_contact
```

```
arp ...
```



```
(FL SWITCH GHS) #show  ?

access-lists            Display Access List information.
alarm_contact           Display Alarm contact information.
arp                     Display Address Resolution Protocol cache.
bootvar                 Shows the boot images on the node.
classofservice          Display class of service information.
debugging               Display debugging configuration.
digital_input           Display Digital Input information.
dos-control             Display Denial of Service Configuration.
dot1x                   Display dot1x information.
eventlog                Display event log entries.
forwardingdb            Display Forwarding Database aging time.
garp                    Display Generic Attribute Registration Protocol
                        information.
gmrp                    Display GMRP interface information.
gvrp                    Display GARP VLAN Registration Protocol parameters.
hardware                Display vital product data.
hosts                   To display the default domain name, a list of name
                        server hosts,the static and the cached list of host
                        names and addresses.
igmpsnooping            Display IGMP Snooping information.
interface               Display IP interface information.
interfaces              Display Interfaces Information.
--More-- or (q)uit
```

Figure 3-13 Telnet command list

Enter the desired word with the corresponding arguments and confirm with ENTER. If you do not know the corresponding arguments for the desired command, add "?" to the command. Example:

```
(FL SWITCH GHS) >show ?
```

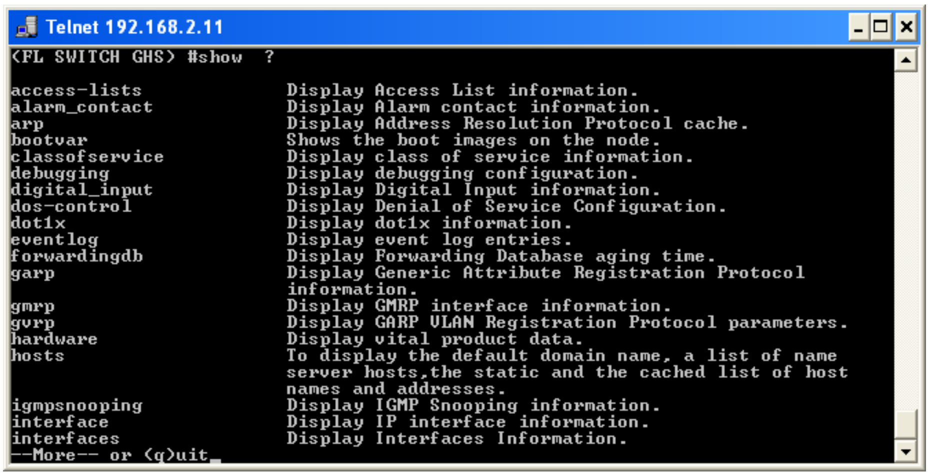
3.6.0.1 Calling privilege mode

In privilege mode, you have access to all the Telnet options. You can tell that you are in privilege mode, as the cursor in Telnet changes from ">" to "#".

Procedure:

- Call Telnet as described above.
- Log in.

- Enter "enable". Confirm the password prompt that then appears by pressing ENTER.



```
<FL SWITCH GHS> #show  ?

access-lists             Display Access List information.
alarm_contact            Display Alarm contact information.
arp                      Display Address Resolution Protocol cache.
bootvar                  Shows the boot images on the node.
classofservice           Display class of service information.
debugging                Display debugging configuration.
digital_input            Display Digital Input information.
dos-control              Display Denial of Service Configuration.
dot1x                    Display dot1x information.
eventlog                 Display event log entries.
forwardingdb             Display Forwarding Database aging time.
garp                     Display Generic Attribute Registration Protocol
                         information.
gmrp                     Display GMRP interface information.
gvrp                     Display GARP VLAN Registration Protocol parameters.
hardware                 Display vital product data.
hosts                    To display the default domain name, a list of name
                         server hosts,the static and the cached list of host
                         names and addresses.
igmpsnooping             Display IGMP Snooping information.
interface                Display IP interface information.
interfaces               Display Interfaces Information.
--More-- or (q)uit_
```

Figure 3-14 Switching to privilege mode and calling the list of arguments

4 Startup

A "Product Information" CD is supplied with the Gigabit Modular Switches. This contains the IPAssign tool (see 4.3.1 "Assigning IP parameters with IPAssign") for assigning IP addresses, background literature on Ethernet, and other documentation specific to the Gigabit Modular Switches.

The switches can also be started up without the CD.

4.1 Basic settings

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

4.1.1 Default upon delivery/default settings

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

- The password is "private".
- All IP parameters are deleted. The switch has **no** valid IP parameters:

IP address:	0.0.0.0
Subnet mask:	0.0.0.0
Gateway:	0.0.0.0

- BootP is activated as the addressing mechanism.
- All available ports are activated with the following parameters:
  - Auto negotiation
  - 100 Mbps - full duplex for FX fiberglass modules (FL IF ...) and HCS ports
  - 1000 Mbps - full duplex for SFP slot modules
- All counters of the SNMP agent are deleted.
- The web and Telnet server, SNMP agent, CLI, and RS-232 interface are active.
- Port mirroring, Rapid Spanning Tree, MRP, port security, multicast filtering, VLAN, DHCP relay agent option 82, and LLDP are deactivated.
- Port security is deactivated for all ports.
- Access control for WBM is deactivated.
- The alarm contact only opens in the event of non-redundant power supply and a detected PoE error.
- The transmission of SNMP traps is deactivated and the switch has no valid trap destination IP address.
- The aging time is set to 40 seconds.
- The switch is in "Ethernet" mode (default settings).
- The WBM refresh interval is set to 30 seconds.
- Management is in VLAN 1.
- The SNTP function (automatic setting of the system time) is deactivated.

– PROFINET and Ethernet/IP are deactivated.

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

During switch restart, the active configuration including IP parameters is written to a plugged-in configuration memory.

The GHS offers several user interfaces for accessing configuration and diagnostic data. The preferred interfaces are the web interface, CLI, and SNMP interface. These interfaces can be used to make all the necessary settings and request all information.

Access to the serial interface via Telnet/RS-232 interface or SSH only enables access to basic information.

The following generally applies: Settings are not automatically saved permanently. To permanently save the active configuration, select "Save ..." in the relevant user interface.

4.2 Activating the default IP address

After the boot phase, proceed as follows with the buttons/display:

- Press "Menu".
- Select "IP Menu" and press "Select".
- Select "IP Settings" and press "Select".
- Select "Default IP" and press "Set".

The switch can now be accessed via IP address **192.168.0.100**. Make any necessary adjustments on your PC.

Please note:

– The selection of the default IP is not stored retentively. Save the desired configuration via the management interface.

– Make sure that there is only one device with the IP address 192.168.0.100 in your network.

4.3 Assigning IP parameters

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

The two buttons on the display must be held down together for a few seconds to trigger a reset.

By default upon delivery, the "BootP" function is activated. 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.

> If the switch has not been assigned valid IP parameters, "No IP assigned 01" will appear in the display.

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)
- DCP (Discovery and Configuration Protocol)

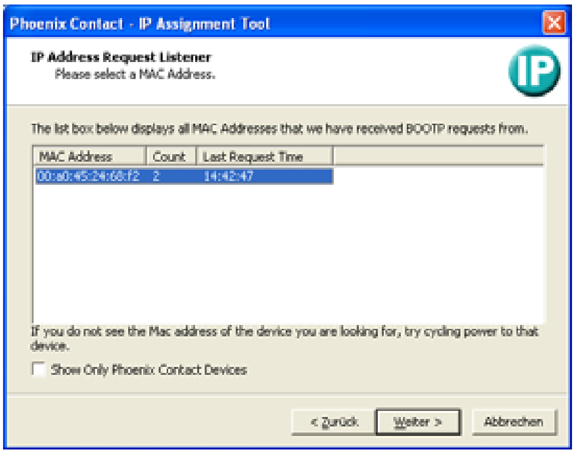
> If DHCP is selected as the assignment mechanism, the DHCP server must offer a DHCP lease time of **at least five** minutes, so that the switch accepts the assigned IP parameters.

4.3.1 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.

Sequence

- Connect the switch to your PC and start IPAssign. The tool then displays the devices that are sending BootP requests to assign an IP.



Phoenix Contact - IP Assignment Tool

IP Address Request Listener
Please select a MAC Address.

The list box below displays all MAC Addresses that we have received BOOTP requests from.

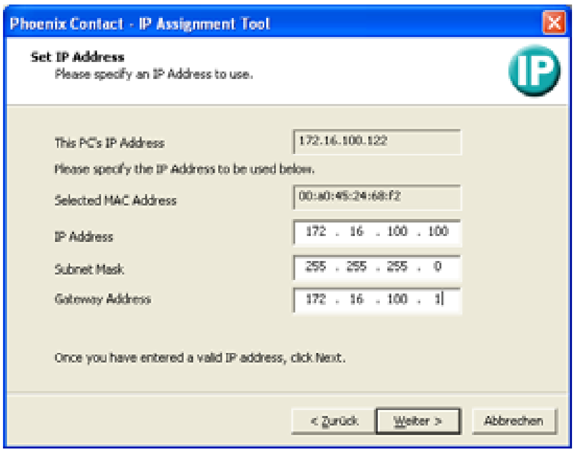
MAC Address	Count	Last Request Time
00:a0:45:24:68:f2	2	14:42:47

If you do not see the Mac address of the device you are looking for, try cycling power to that device.

□ Show Only Phoenix Contact Devices

Figure 4-1 Devices sending BootP requests in IPAssign

- Click "Next" and enter the desired IP parameters.



Phoenix Contact - IP Assignment Tool

Set IP Address
Please specify an IP Address to use.

This PC's IP Address: 172.16.100.122

Please specify the IP Address to be used below.

Selected MAC Address: 00:a0:45:24:68:f2

IP Address: 172 . 16 . 100 . 100

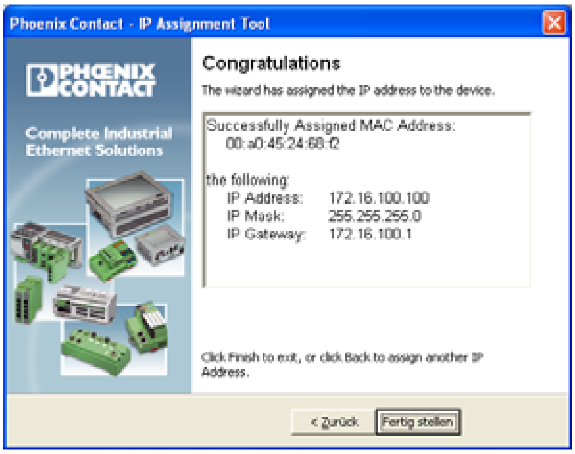
Subnet Mask: 255 . 255 . 255 . 0

Gateway Address: 172 . 16 . 100 . 1

Once you have entered a valid IP address, click Next.

Figure 4-2 Mask for IP parameters

- Click "Next". If successful, this window is displayed.



Phoenix Contact - IP Assignment Tool

Congratulations
The wizard has assigned the IP address to the device.

Successfully Assigned MAC Address:
00:a0:45:24:68:f2

the following:
IP Address: 172.16.100.100
IP Mask: 255.255.255.0
IP Gateway: 172.16.100.1

Click Finish to exit, or click Back to assign another IP Address.

Figure 4-3 Message in IPAssign

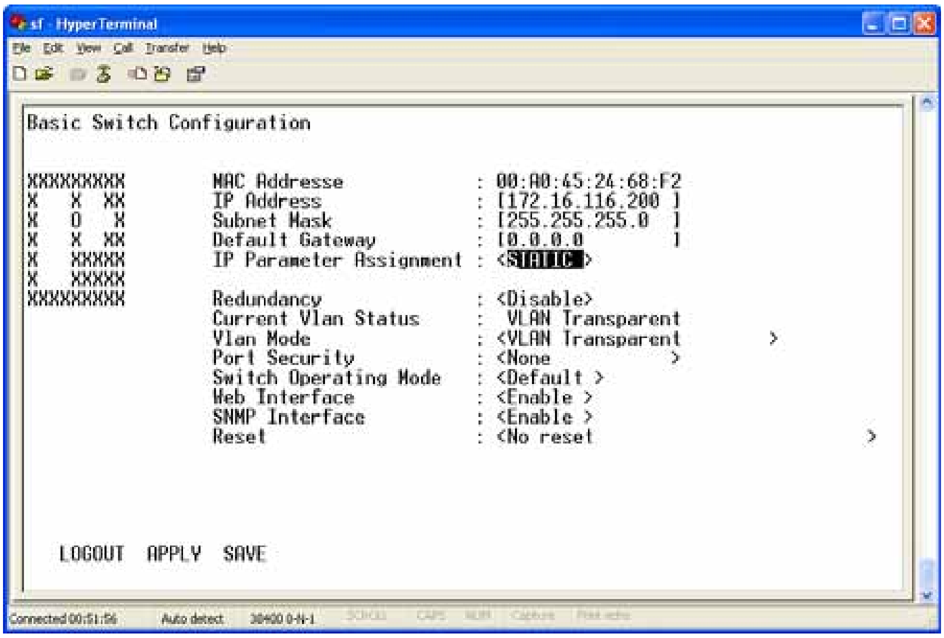
4.3.2 Example for V.24 (RS-232) as a serial connection

Establish a communication connection as described in Section 3.2 "RS-232 interface for external management".

Changing the IP address

- Open the serial interface and log in.
- The default settings are:
  User: **admin**
  Password: **private**

- Now select "IP Parameter Assignment" and, using the spacebar, change the selection to "Static".



```
Basic Switch Configuration


XXXXXXXXX        MAC Addresse             : 00:A0:45:24:68:F2
X    X  XX       IP Address               : [172.16.116.200 ]
X    O   X       Subnet Mask              : [255.255.255.0  ]
X    X  XX       Default Gateway          : [0.0.0.0        ]
X    XXXXX       IP Parameter Assignment  : <STATIC >
X    XXXXX
XXXXXXXXX        Redundancy               : <Disable>
                 Current Vlan Status      :  VLAN Transparent
                 Vlan Mode                : <VLAN Transparent         >
                 Port Security            : <None             >
                 Switch Operating Mode    : <Default >
                 Web Interface            : <Enable >
                 SNMP Interface           : <Enable >
                 Reset                    : <No reset                          >




   LOGOUT   APPLY   SAVE
```

Figure 4-4 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".

4.3.3 Assigning IP parameters via the CLI and SSH

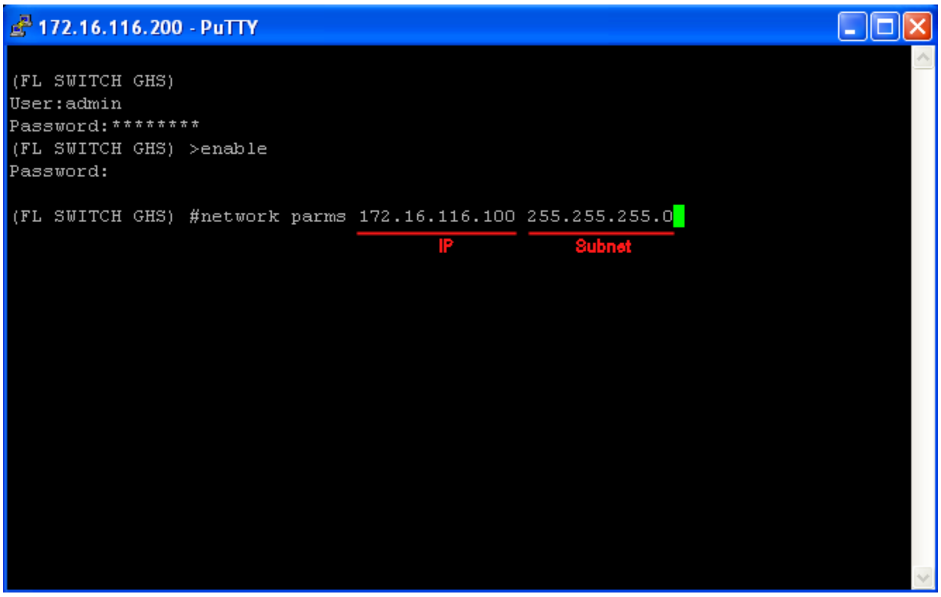
In order to use CLI management via SSH, the switch must already have an IP address. This IP address may, for example, have been set via the CLI or the serial connection or may have been assigned via the automatic BootP or DHCP mechanisms (see also 4.3.1 "Assigning IP parameters with IPAssign").

Setting and changing the IP address for the first time

- Open the CLI with a SSH client and the current IP address.
  Example: http://172.16.116.200
- The default settings are:
  User: **admin**
  Password: **private**
- Switch to privilege mode using "enable" and confirm the password prompt with ENTER (see Section "Calling privilege mode" on page 3-11).
- Enter the following: "network parms <IP address> <Subnet mask> <Default gateway>".
  Example: The new IP is: 172.16.116.100, the subnetwork is 255.255.255.0, there is no default gateway. SSH entry in privilege mode:

```
network parms 172.16.116.100 255.255.255.0
```

A subnet mask **must** be assigned, a default gateway **can** be assigned.



```
(FL SWITCH GHS)
User:admin
Password:********
(FL SWITCH GHS) >enable
Password:

(FL SWITCH GHS) #network parms 172.16.116.100 255.255.255.0
```

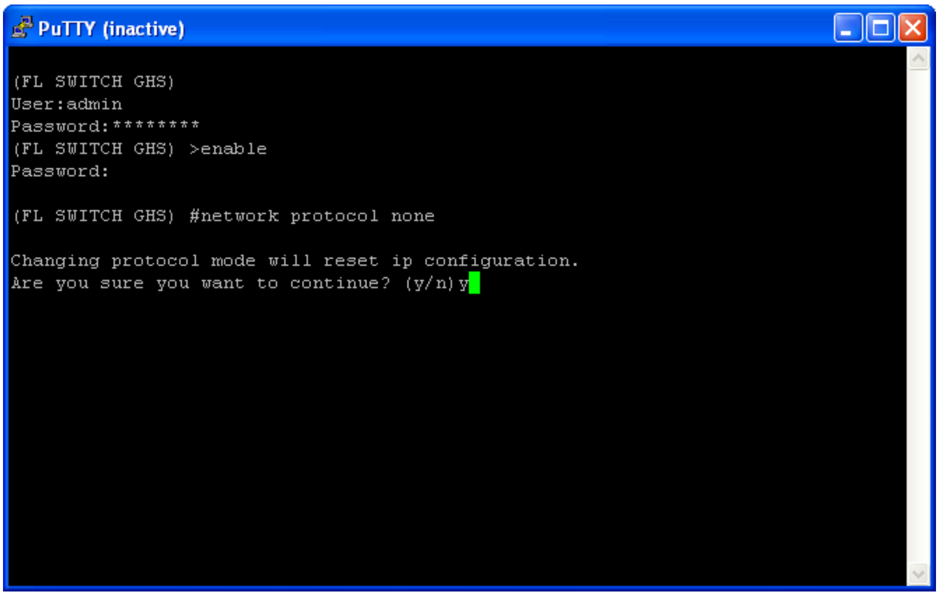
Figure 4-5 SSH client

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

Possible error:

If your entry has been rejected with the message "Network protocol must be none to set IP address", you must first disable the active IP address assignment mechanism and then assign the IP statically to the device. To disable IP assignment mechanisms, please enter the following (in privilege mode):

```
network protocol none
```



```
(FL SWITCH GHS)
User:admin
Password:********
(FL SWITCH GHS) >enable
Password:

(FL SWITCH GHS) #network protocol none

Changing protocol mode will reset ip configuration.
Are you sure you want to continue? (y/n)y
```

Figure 4-6 SSH prompt

4.3.4 Assignment of IP parameters via DHCP/DCP

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

4.4 Modifying IP parameters

Requirements for the use of WBM

As the web server operates using the Hyper Text Transfer Protocol, a standard browser can be used. Access is via the URL "http://IP address of the device".
Example: "http://172.16.116.100".
For full operation of the web pages, the browser must support JavaScript 1.2 and Cascading Style Sheets Level 1. We recommend the use of Microsoft Internet Explorer 6.0.

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

Once you have established all the necessary connections and the BootP server (e.g., IPAssign.exe) has been started, start the GHS or execute a reset.

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

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

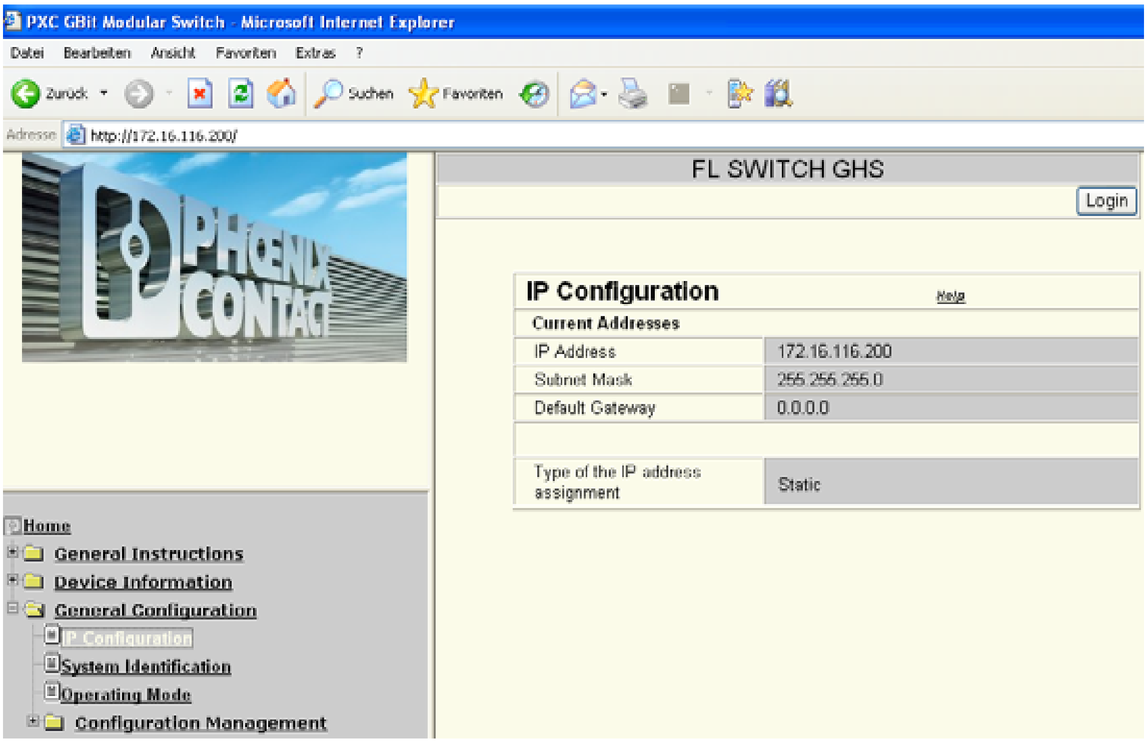
4.4.1 Example for web-based management

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 CLI or the serial connection or may have been assigned via the automatic BootP or DHCP mechanisms (see also 4.3.1 "Assigning IP parameters with IPAssign").

Changing the IP address

- Open the web interface with a browser and the current IP address.
  Example: http://172.16.116.200
- Select the "General Configuration" page and then "IP Configuration".

- In order to make changes, you must log into the device. Click on "Login" at the top of the web page.



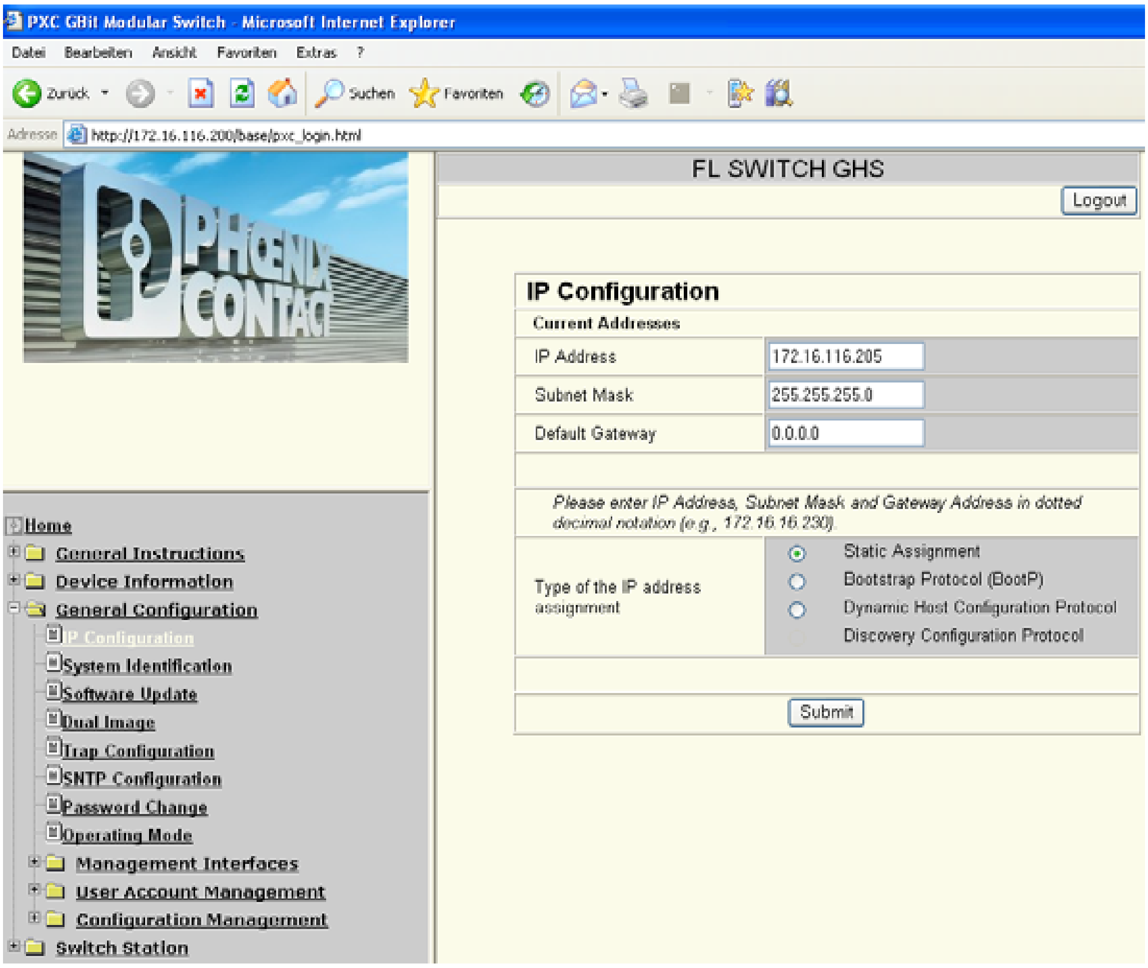
IP Configuration

Current Addresses	
IP Address	172.16.116.200
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Type of the IP address assignment	Static

Figure 4-7 "IP Configuration" web page

- The default settings are:
  User: **admin**
  Password: **private**
- Return to the "General Configuration/IP Configuration" page.

- Under "Type of the IP address assignment", select "Static assignment" and enter the new IP address in the corresponding field. Click on "Submit" to apply the change.



Adresse: http://172.16.116.200/base/pxc_login.html

FL SWITCH GHS

IP Configuration

Current Addresses

IP Address	172.16.116.205
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0

Please enter IP Address, Subnet Mask and Gateway Address in dotted decimal notation (e.g., 172.16.16.230).

Type of the IP address assignment:
● Static Assignment
○ Bootstrap Protocol (BootP)
○ Dynamic Host Configuration Protocol
Discovery Configuration Protocol

Figure 4-8 "IP Configuration" web page following successful login

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

4.4.2 Changing IP parameters via the CLI

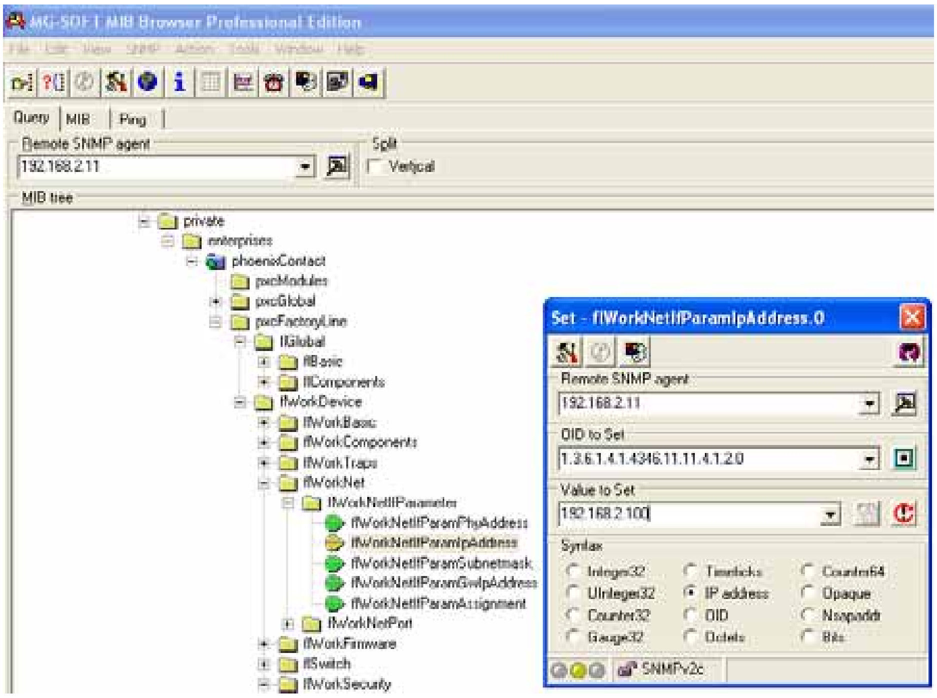
See 4.3.3 "Assigning IP parameters via the CLI and SSH".

4.4.3 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 CLI or the serial connection or may have been assigned via the automatic BootP or DHCP mechanisms (see also 4.3.1 "Assigning IP parameters with IPAssign").

Changing the IP address

- Open the OID (flWorkNetIfParamIpAddress) 1.3.6.1.4.1.4346.11.11.4.1.2 using an MIB browser, which is connected to the device via the current IP address.
- Enter the desired IP and apply this using "Set".



Remote SNMP agent: 192.168.2.11

OID to Set: 1.3.6.1.4.1.4346.11.11.4.1.2.0

Value to Set: 192.168.2.100

Syntax: ● IP address

Figure 4-9 IP address assignment via SNMP

4.5 Password concept

When making initial contact with the device and checking the current state for the first time, it is not necessary to log in. As soon as functions that require authorization are called, a login window appears where you must enter your user name and password.

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

After having entered the valid password, no further entry of the password is necessary for a period of 5 minutes (default). After this period of time has elapsed or after clicking on "Logout", the password must be re-entered.

The period of time can be set from 0 minutes to 60 minutes.

WBM: Switch Station/Services

SNMP object: "flWorkFWCtrlLoginExpire"

CLI user manual: Unknown source of cross-reference

The concept is valid for the first ten users logged in at the same time. All other users must confirm each configuration modification by entering the password, until less than ten users are logged in. A user can assign various rights to other users.

4.6 Using Smart mode

Smart mode enables the user to change the operating mode of the switch without having to access the management interface.

The switch offers the following setting options via Smart mode:

– Reset to the default settings
– Set PROFINET mode
– Set Ethernet/IP mode
– Exit Smart mode without changes

4.6.1 Activating Smart mode/easy setup

The display/operator interface is used to select the desired setting. The setting, which will apply when exiting Smart mode, can be viewed in the display.

4.6.1.1 Calling Smart mode

- After restarting the device, press and hold down "Activate" for around five seconds until the display contains "Smart Mode/Easy Setup". If Smart mode is active, "Smart Mode" will appear in the display.

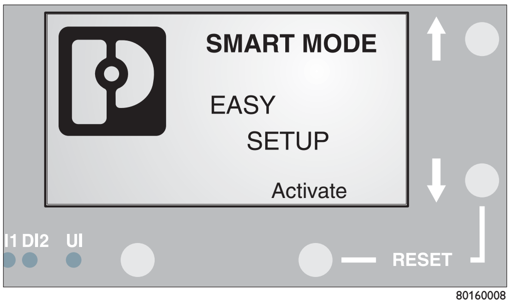


Figure 4-10 Display contents after booting in order to call Smart mode

4.6.1.2 Selecting the desired setting

- To select the various settings, use the arrow keys next to the display and press "Set" to activate the desired setting.

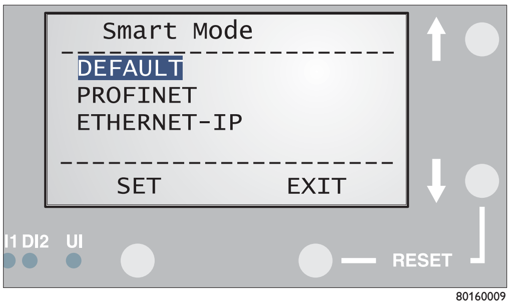


Figure 4-11 Display contents in Smart mode

4.6.1.3 Exit Smart mode without changes

- Press "Exit".

4.6.1.4 Possible operating modes in Smart mode

The switch supports the selection of the following operating modes in Smart mode (see also example below):

Table 4-1 Operating modes in Smart mode

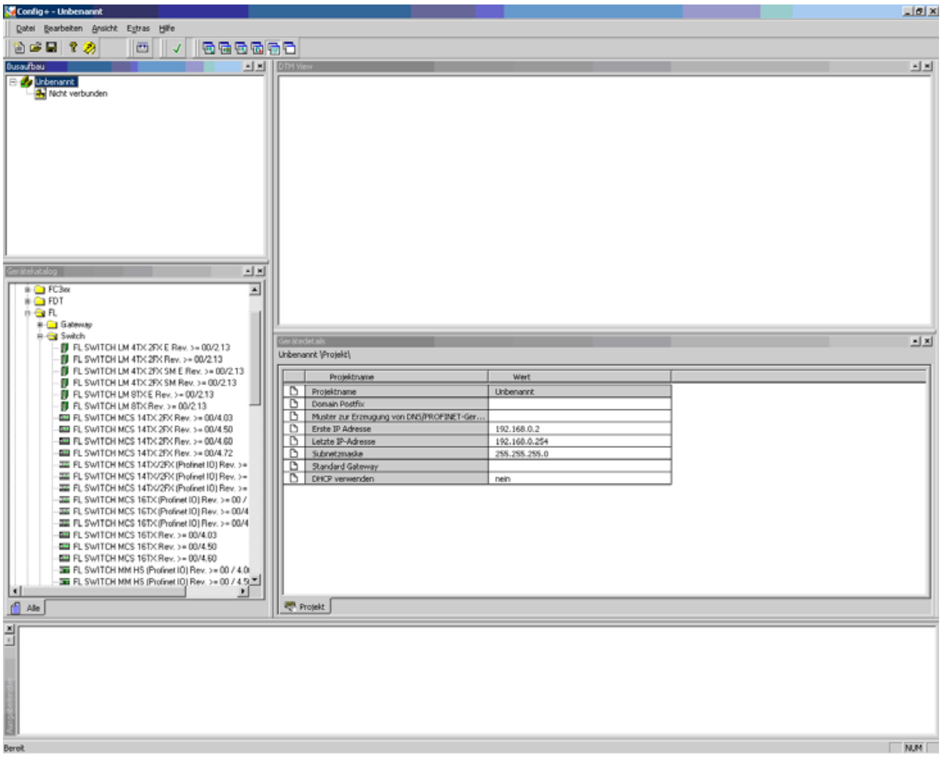
Mode	Display
Exit Smart mode without changes	EXIT
Reset to the default settings	DEFAULT
Set PROFINET mode	PROFINET
Set Ethernet/IP mode	ETHERNET-IP

4.7 Startup with the MDC wizard

Industrial automation solutions are increasingly based on Ethernet communication, which has resulted in more widespread use of infrastructure components and has meant that networks have become larger and more complex. The easy parameterization, configuration, and diagnostics of the components used is therefore particularly important. Config+, a powerful software tool, provides corresponding functions for Ethernet networks. The tool can be found in the download area under "CONFIG+ DEMO". A particular advantage of this tool is the built-in open FDT interface to integrate third-party software directly in Config+ and use special device user interfaces (DTM) for proprietary and third-party components. If several components of a system are to have the same parameters, considerable time savings can be made during configuration by using a special wizard for multi-device parameterization. The wizard enables one or more parameters of a component to be easily applied to other devices of the same or a similar type. For switches, the Rapid Spanning Tree Protocol (RSTP), Media Redundancy Protocol (MRP), trap receiver, Link Layer Discovery Protocol (LLDP) or Virtual Local Area Networks (VLANs) can be parameterized simultaneously for various selected devices.

Time-consuming individual adjustment and modification of device functions via web-based management is thus eliminated.

4.7.1 Calling a new project under Config+


Config+ - Unbenannt
Datei Bearbeiten Ansicht Extras Hilfe
Busaufbau
Unbenannt
Nicht verbunden
DTM View
Gerätekatalog
FC3xx
FDT
FL
Gateway
Switch
FL SWITCH LM 4TX 2FX E Rev. >= 00/2.13
FL SWITCH LM 4TX 2FX Rev. >= 00/2.13
FL SWITCH LM 4TX 2FX SM E Rev. >= 00/2.13
FL SWITCH LM 4TX 2FX SM Rev. >= 00/2.13
FL SWITCH LM 8TX E Rev. >= 00/2.13
FL SWITCH LM 8TX Rev. >= 00/2.13
FL SWITCH MCS 14TX 2FX Rev. >= 00/4.03
FL SWITCH MCS 14TX 2FX Rev. >= 00/4.50
FL SWITCH MCS 14TX 2FX Rev. >= 00/4.60
FL SWITCH MCS 14TX 2FX Rev. >= 00/4.72
FL SWITCH MCS 14TX/2FX (Profinet IO) Rev. >=
FL SWITCH MCS 14TX/2FX (Profinet IO) Rev. >=
FL SWITCH MCS 14TX/2FX (Profinet IO) Rev. >=
FL SWITCH MCS 16TX (Profinet IO) Rev. >= 00 /
FL SWITCH MCS 16TX (Profinet IO) Rev. >= 00/4
FL SWITCH MCS 16TX (Profinet IO) Rev. >= 00/4
FL SWITCH MCS 16TX Rev. >= 00/4.03
FL SWITCH MCS 16TX Rev. >= 00/4.50
FL SWITCH MCS 16TX Rev. >= 00/4.60
FL SWITCH MM HS (Profinet IO) Rev. >= 00 / 4.0
FL SWITCH MM HS (Profinet IO) Rev. >= 00 / 4.5
Alle
Gerätedetails
Projekt
Bereit
NUM

Unbenannt \Projekt\

Projektname	Wert
Projektname	Unbenannt
Domain Postfix	
Muster zur Erzeugung von DNS/PROFINET-Ger…	
Erste IP Adresse	192.168.0.2
Letzte IP-Adresse	192.160.0.254
Subnetzmaske	255.255.255.0
Standard Gateway	
DHCP verwenden	nein

Figure 4-12 New project under Config+

The layout and contents of the window can be changed. Here the "Bus Structure", "Device Catalog", "DTM View", "Device Details", and "Output Details" windows are open and recommended for use (see Figure 4-12).

1. A virtual PC must be integrated into the project => locate AXSNMP 1.0 in the device catalog under "Phoenix Contact\FDT\PC" and integrate in the bus configuration under the project (see Figure 4-13)

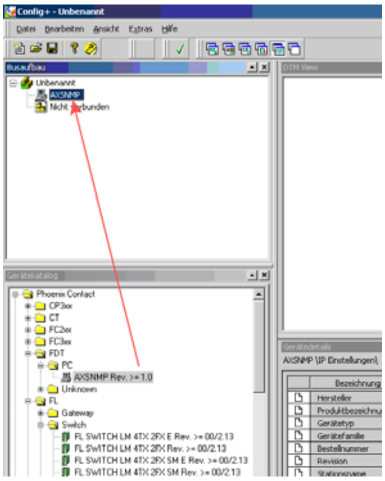
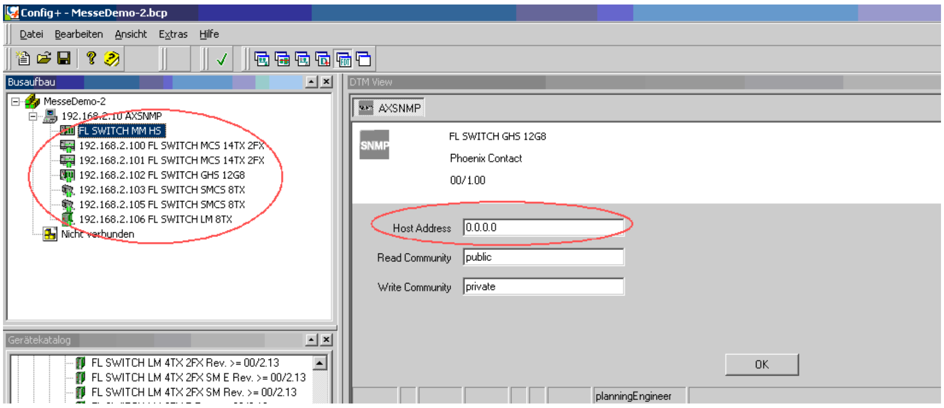


Figure 4-13 Selecting the desired components

2. Select the desired Ethernet components from the device catalog and append under the AXSNMP virtual PC; note the firmware version of the devices.


Config+ - MesseDemo-2.bcp
Datei Bearbeiten Ansicht Extras Hilfe
Busaufbau
MesseDemo-2
192.168.2.10 AXSNMP
FL SWITCH MM HS
192.168.2.100 FL SWITCH MCS 14TX 2FX
192.168.2.101 FL SWITCH MCS 14TX 2FX
192.168.2.102 FL SWITCH GHS 12G8
192.168.2.103 FL SWITCH SMCS 8TX
192.168.2.105 FL SWITCH SMCS 8TX
192.168.2.106 FL SWITCH LM 8TX
Nicht verbunden
Gerätekatalog
FL SWITCH LM 4TX 2FX Rev. >= 00/2.13
FL SWITCH LM 4TX 2FX SM E Rev. >= 00/2.13
FL SWITCH LM 4TX 2FX SM Rev. >= 00/2.13
DTM View
AXSNMP
SNMP
OK
planningEngineer

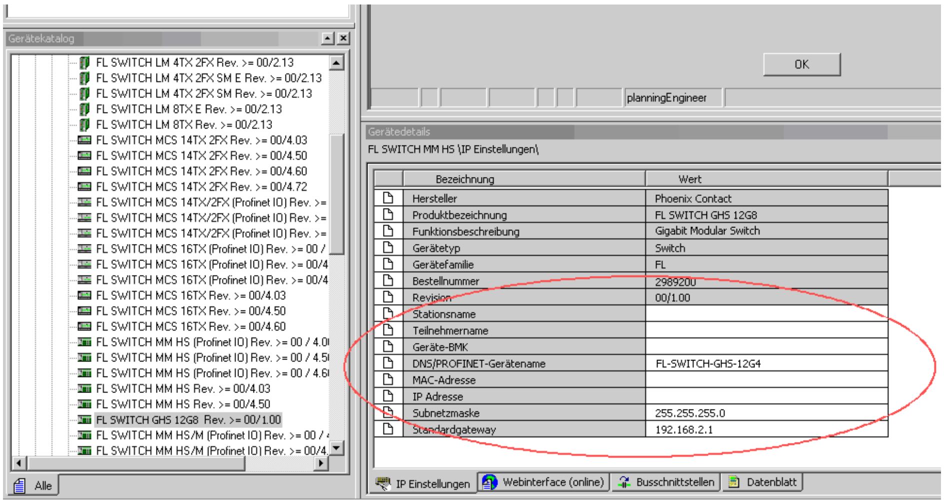
FL SWITCH GHS 12G8
Phoenix Contact
00/1.00

Host Address: 0.0.0.0
Read Community: public
Write Community: private

Figure 4-14 Entering the IP parameters

In the case of a new device (an FL SWITCH MM HS in this example) that has been implemented correctly, a tab automatically appears in "DTM View" where the IP address (host address) must be entered (see Figure 4-14).

In addition, the IP address, subnet mask, PROFINET device name (if applicable), MAC address, etc. must be entered in the "Device Details" window (see Figure 4-15).


Gerätekatalog
FL SWITCH LM 4TX 2FX Rev. >= 00/2.13
FL SWITCH LM 4TX 2FX SM E Rev. >= 00/2.13
FL SWITCH LM 4TX 2FX SM Rev. >= 00/2.13
FL SWITCH LM 8TX E Rev. >= 00/2.13
FL SWITCH LM 8TX Rev. >= 00/2.13
FL SWITCH MCS 14TX 2FX Rev. >= 00/4.03
FL SWITCH MCS 14TX 2FX Rev. >= 00/4.50
FL SWITCH MCS 14TX 2FX Rev. >= 00/4.60
FL SWITCH MCS 14TX 2FX Rev. >= 00/4.72
FL SWITCH MCS 14TX/2FX (Profinet IO) Rev. >=
FL SWITCH MCS 14TX/2FX (Profinet IO) Rev. >=
FL SWITCH MCS 14TX/2FX (Profinet IO) Rev. >=
FL SWITCH MCS 16TX (Profinet IO) Rev. >= 00 /
FL SWITCH MCS 16TX (Profinet IO) Rev. >= 00/4
FL SWITCH MCS 16TX (Profinet IO) Rev. >= 00/4
FL SWITCH MCS 16TX Rev. >= 00/4.03
FL SWITCH MCS 16TX Rev. >= 00/4.50
FL SWITCH MCS 16TX Rev. >= 00/4.60
FL SWITCH MM HS (Profinet IO) Rev. >= 00 / 4.0
FL SWITCH MM HS (Profinet IO) Rev. >= 00 / 4.5
FL SWITCH MM HS (Profinet IO) Rev. >= 00 / 4.6
FL SWITCH MM HS Rev. >= 00/4.03
FL SWITCH MM HS Rev. >= 00/4.50
FL SWITCH GHS 12G8 Rev. >= 00/1.00
FL SWITCH MM HS/M (Profinet IO) Rev. >= 00 / 4
FL SWITCH MM HS/M (Profinet IO) Rev. >= 00/4
Alle
OK
planningEngineer
Gerätedetails
IP Einstellungen
Webinterface (online)
Busschnittstellen
Datenblatt

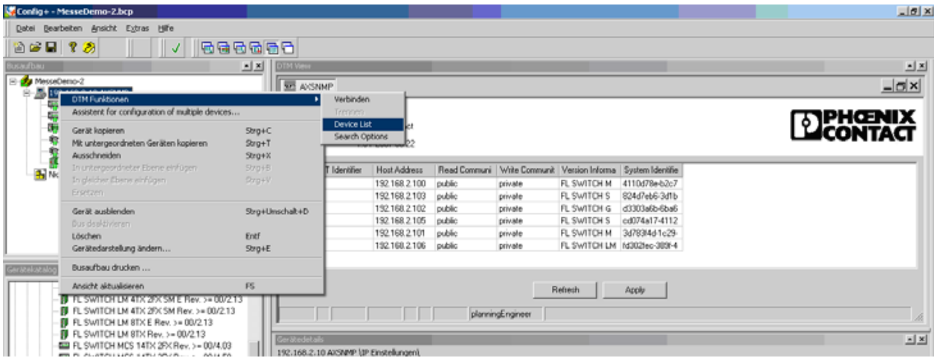
FL SWITCH MM HS \IP Einstellungen\

Bezeichnung	Wert
Hersteller	Phoenix Contact
Produktbezeichnung	FL SWITCH GHS 12G8
Funktionsbeschreibung	Gigabit Modular Switch
Gerätetyp	Switch
Gerätefamilie	FL
Bestellnummer	2989200
Revision	00/1.00
Stationsname	
Teilnehmername	
Geräte-BMK	
DNS/PROFINET-Gerätename	FL-SWITCH-GHS-12G4
MAC-Adresse	
IP Adresse	
Subnetzmaske	255.255.255.0
Standardgateway	192.168.2.1

Figure 4-15 Device data in the wizard

Following correct entry, this data will appear as circled in Figure 4-15.

All accessible and THEREFORE configurable devices can be displayed via the context menu by right-clicking on "AXSNMP\DTM Functions\Device List" in "DTM View" (see Figure 4-16).

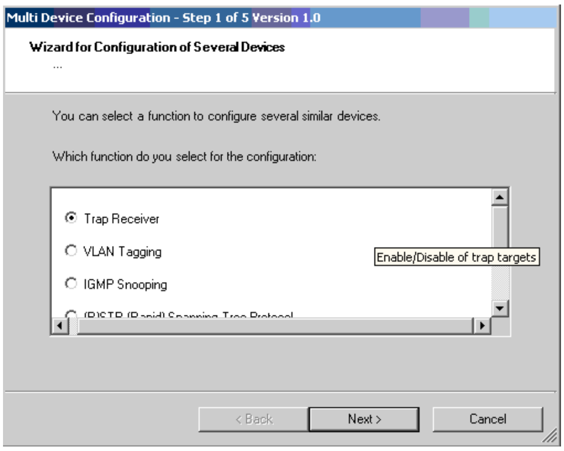

Config+ - MesseDemo-2.bcp
Datei Bearbeiten Ansicht Extras Hilfe
Busaufbau
MesseDemo-2
DTM View
AXSNMP
DTM Funktionen
Assistent for configuration of multiple devices...
Gerät kopieren Strg+C
Mit untergeordneten Geräten kopieren Strg+T
Ausschneiden Strg+X
In untergeordneter Ebene einfügen Strg+B
In gleicher Ebene einfügen Strg+V
Ersetzen
Gerät ausblenden Strg+Umschalt+D
Bus deaktivieren
Löschen Entf
Gerätedarstellung ändern... Strg+E
Busaufbau drucken ...
Ansicht aktualisieren F5
Verbinden
Trennen
Device List
Search Options
PHOENIX CONTACT
Refresh
Apply
planningEngineer
Gerätekatalog
FL SWITCH LM 4TX 2FX SM E Rev. >= 00/2.13
FL SWITCH LM 4TX 2FX SM Rev. >= 00/2.13
FL SWITCH LM 8TX E Rev. >= 00/2.13
FL SWITCH LM 8TX Rev. >= 00/2.13
FL SWITCH MCS 14TX 2FX Rev. >= 00/4.03
Gerätedetails
192.168.2.10 AXSNMP \IP Einstellungen\

T Identifier	Host Address	Read Communi	Write Communit	Version Informa	System Identifie
	192.168.2.100	public	private	FL SWITCH M	4110d78e-b2c7
	192.168.2.103	public	private	FL SWITCH S	824d7eb6-3d1b
	192.168.2.102	public	private	FL SWITCH G	d3303a6b-6ba6
	192.168.2.105	public	private	FL SWITCH S	cd074a17-4112
	192.168.2.101	public	private	FL SWITCH M	3d783f4d-1c29-
	192.168.2.106	public	private	FL SWITCH LM	fd302fec-389f-4

Figure 4-16 Context menu - "DTM View"

4.7.2 Configuration with the MDC wizard

All configurable devices can be selected via the context menu that appears when right-clicking on one of the devices and the "Wizard for Configuration of Several Devices" appears where further functions can be selected:



Multi Device Configuration - Step 1 of 5 Version 1.0

Wizard for Configuration of Several Devices

...

You can select a function to configure several similar devices.

Which function do you select for the configuration:

- ● Trap Receiver
- ○ VLAN Tagging
- ○ IGMP Snooping
- ○ (R)STP (Rapid) Spanning Tree Protocol

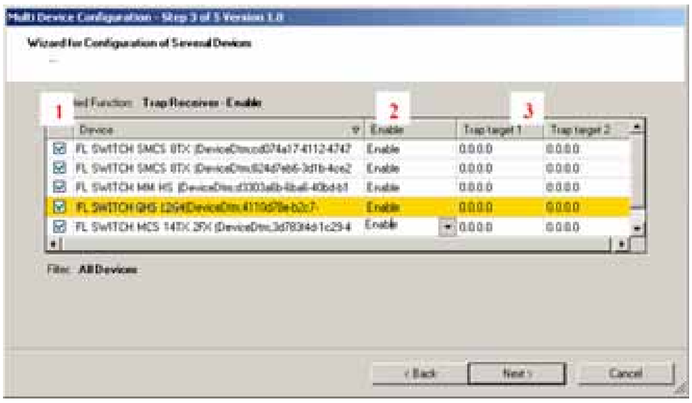
Figure 4-17 MDC wizard

The following functions can be configured using MDC:

- Enable/disable trap receiver
- Enable transparent VLAN tagging or tagging mode
- Enable/disable IGMP snooping
- Enable/disable RSTP
- Enable/disable MRP
- Enable/disable large tree support
- Enable/disable fast ring detection
- Enable/disable LLDP

4.7.2.1 Trap receiver

- Call MDC
- Step 1: Select the trap receiver function
- Step 2: Set parameters to "Enable" or "Disable"
- Step 3: A list is displayed of all the devices that support the trap receiver function (see Figure 4-18)
- In the table, devices that are not to be modified can be deactivated (uncheck device) (see Figure 4-18/item 1)
- In the table, devices can be simultaneously enabled or disabled (see Figure 4-18/item 2)
- Trap targets are specified for the first and/or second address (see Figure 4-18/item 3)
- Step 4: Start downloading the settings
- Step 5: Close MDC



Multi Device Configuration - Step 3 of 5 Version 1.0

Wizard for Configuration of Several Devices

...

ted Function: Trap Receiver - Enable

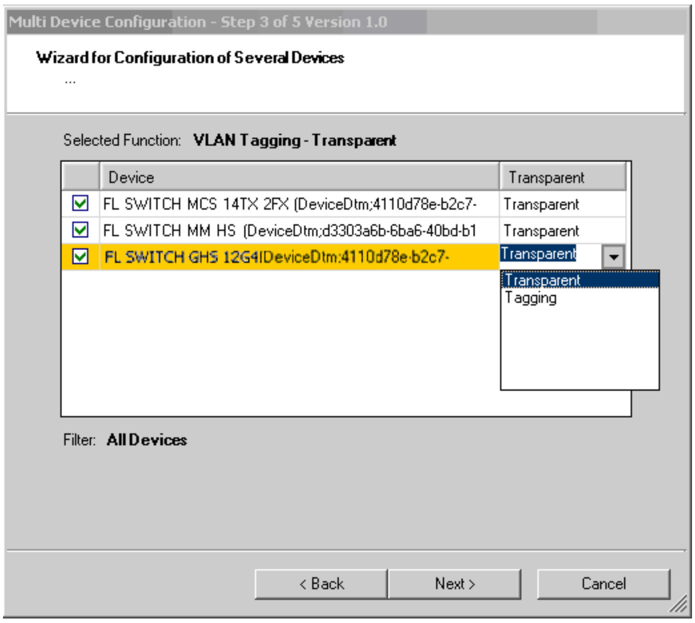
	Device	Enable	Trap target 1	Trap target 2
☑	FL SWITCH SMCS 8TX (DeviceDtm;cd074a17-4112-4747	Enable	0.0.0.0	0.0.0.0
☑	FL SWITCH SMCS 8TX (DeviceDtm;624d7eb6-3d1b-4ce2	Enable	0.0.0.0	0.0.0.0
☑	FL SWITCH MM HS (DeviceDtm;d3303a6b-6ba6-40bd-b1	Enable	0.0.0.0	0.0.0.0
☑	FL SWITCH GHS 12G4(DeviceDtm;4110d78e-b2c7-	Enable	0.0.0.0	0.0.0.0
☑	FL SWITCH MCS 14TX 2FX (DeviceDtm;3d78344d-1c29-4	Enable	0.0.0.0	0.0.0.0

Filter: All Devices

Figure 4-18 Trap receiver selection in the MDC wizard

4.7.2.2 VLAN tagging

- Call MDC
- Step 1: Select the VLAN tagging function
- Step 2: Set parameters to "Transparent" or "Tagging"
- Step 3: A list is displayed of all the devices that support VLAN tagging (see Figure 4-19)
- In the table, devices that are not to be modified can be deactivated (uncheck device)
- In the table, devices can be simultaneously selected as "Transparent" or "Tagging" (see Figure 4-19)
- Step 4: Start downloading the settings
- Step 5: Close MDC



Multi Device Configuration - Step 3 of 5 Version 1.0

Wizard for Configuration of Several Devices

...

Selected Function: **VLAN Tagging - Transparent**

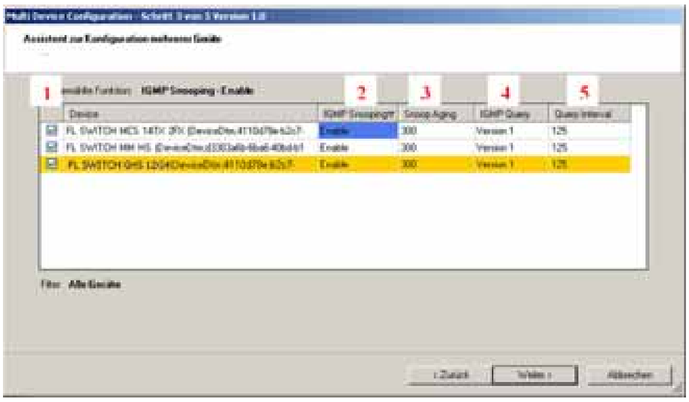
	Device	Transparent
☑	FL SWITCH MCS 14TX 2FX (DeviceDtm;4110d78e-b2c7-	Transparent
☑	FL SWITCH MM HS (DeviceDtm;d3303a6b-6ba6-40bd-b1	Transparent
☑	FL SWITCH GHS 12G4IDeviceDtm:4110d78e-b2c7-	Transparent

Filter: **All Devices**

Figure 4-19 Selecting the tagging mode

4.7.2.3 IGMP snooping

- Call MDC
- Step 1: Select the IGMP snooping function
- Step 2: Set parameters to "Enable" or "Disable"
- Step 3: A list is displayed of all the devices that support IGMP snooping
- In the table, devices that are not to be modified can be deactivated (uncheck device) (see Figure 4-20/item 1)
- In the table, devices can be simultaneously activated or deactivated (see Figure 4-20/item 2)
- In the table, different aging times can be selected for the individual devices (see Figure 4-20/item 3). A response is received from the devices within the set time and multicast groups are created dynamically. This time must always be longer than the querier interval (see item 5).
- For each device, the querier can be set to Version 1, Version 2 or disabled (see Figure 4-20/item 5)
- The interval during which a querier request is sent can be set individually for each device (see Figure 4-20/item 5). All multicast devices then send back a response.
- Step 4: Start downloading the settings
- Step 5: Close MDC


Multi Device Configuration - Schritt 3 von 3 Version 1.0

Assistent zur Konfiguration mehrerer Geräte

...wählte Funktion: IGMP Snooping - Enable

	Device	IGMP Snooping	Snoop Aging	IGMP Query	Query Interval
☑	FL SWITCH MCS 14TX 2FX (DeviceDtm.4110d79e-b2c7	Enable	300	Version 1	125
☑	FL SWITCH MM HS (DeviceDtm.d3303a6b-6ba6-40bd-b1	Enable	300	Version 1	125
☑	FL SWITCH GHS 12G4(DeviceDtm.4110d79e-b2c7	Enable	300	Version 1	125

Filter: Alle Geräte

Figure 4-20 IGMP settings in the MDC wizard

4.7.2.4 RSTP activation/deactivation

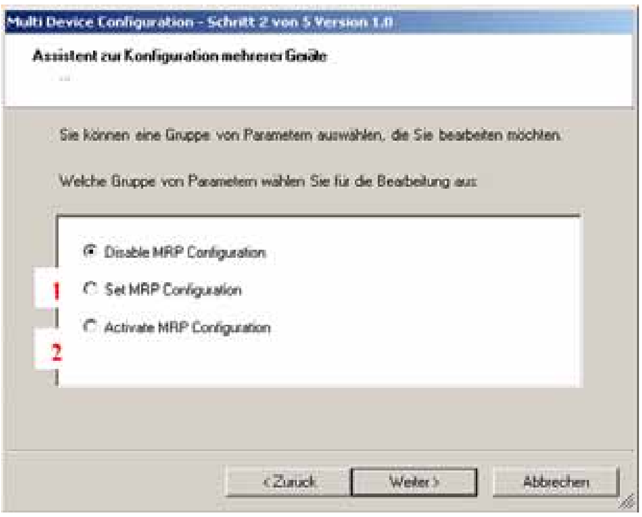
- Call MDC
- Step 1: Select the Rapid Spanning Tree function
- Step 2: Set parameters to "Enable" or "Disable"
- Step 3: A list is displayed of all the devices that support RSTP
- In the table, devices can be simultaneously enabled or disabled
- Step 4: Start downloading the settings
- Step 5: Close MDC

The MDC automatically activates the web pages in the devices and RSTP.

When disabled, only the function is deactivated, not the web page display.

4.7.2.5 MRP activation/deactivation

- Call MDC
- Step 1: Select the MRP function
- Step 2: Select the *Set MRP Configuration* option (see Figure 4-21/item 1)



Multi Device Configuration - Schritt 2 von 5 Version 1.0

Assistent zur Konfiguration mehrerer Geräte

Sie können eine Gruppe von Parametern auswählen, die Sie bearbeiten möchten.

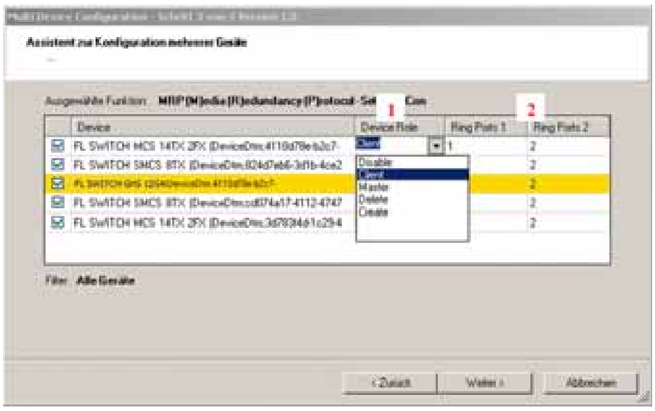
Welche Gruppe von Parametern wählen Sie für die Bearbeitung aus:

● Disable MRP Configuration

○ Set MRP Configuration

○ Activate MRP Configuration

Figure 4-21 Activating redundancy



Multi Device Configuration - Schritt 3 von 5 Version 1.0

Assistent zur Konfiguration mehrerer Geräte

Ausgewählte Funktion: **MRP (M)edia (R)edundancy (P)rotocol - Set ... Con**

	Device	Device Role	Ring Ports 1	Ring Ports 2
☑	FL SWITCH MCS 14TX 2FX (DeviceDtm;4110d78e-b2c7-	Client	1	2
☑	FL SWITCH SMCS 8TX (DeviceDtm;824d7eb6-3d1b-4ce2			2
☑	FL SWITCH GHS 12G(DeviceDtm;4110d78e-b2c7-			2
☑	FL SWITCH SMCS 8TX (DeviceDtm;cd874a17-4112-4747			2
☑	FL SWITCH MCS 14TX 2FX (DeviceDtm;3d7834d1c294			2

Filter: **Alle Geräte**

Figure 4-22 Specifying the MRP role

- Step 3: A list is displayed of all the devices that support MRP
- In the table, devices can be simultaneously set
- In the table, you can specify whether the specific device is a "Master" or "Client" (see Figure 4-22/item 1)
- In the table, you can specify the ring ports for each device (see Figure 4-22/item 2)
- Step 4: Start downloading the settings
- Step 5: Close MDC

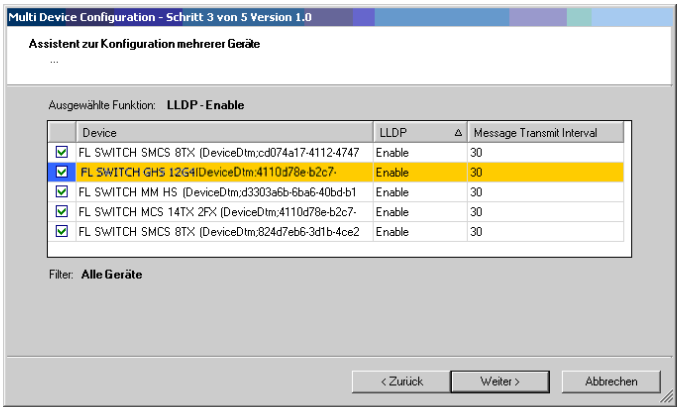
This procedure must then be repeated:

- Call MDC
- Step 1: Select the MRP function
- Step 2: Select the *Activate MRP Configuration* option (see Figure 4-22/item 2)
- Step 3: A list is displayed of all the devices that support MRP
- Step 4: Start downloading the settings
- Step 5: Close MDC

4.7.2.6 Large tree support or fast ring detection

- Call MDC
- Step 1: Select the desired function (large tree support or fast ring detection)
- Step 2: Set parameters to "Enable" or "Disable"
- Step 3: A list is displayed of all the devices that support the desired function
- Step 4: Start downloading the settings
- Step 5: Close MDC

4.7.2.7 LLDP activation



Multi Device Configuration - Schritt 3 von 5 Version 1.0

Assistent zur Konfiguration mehrerer Geräte

...

Ausgewählte Funktion: **LLDP - Enable**

	Device	LLDP △	Message Transmit Interval
☑	FL SWITCH SMCS 8TX (DeviceDtm;cd074a17-4112-4747	Enable	30
☑	FL SWITCH GHS 12G4(DeviceDtm:4110d78e-b2c7-	Enable	30
☑	FL SWITCH MM HS (DeviceDtm;d3303a6b-6ba6-40bd-b1	Enable	30
☑	FL SWITCH MCS 14TX 2FX (DeviceDtm;4110d78e-b2c7-	Enable	30
☑	FL SWITCH SMCS 8TX (DeviceDtm;824d7eb6-3d1b-4ce2	Enable	30

Filter: **Alle Geräte**

Figure 4-23 Setting LLDP in the MDC wizard

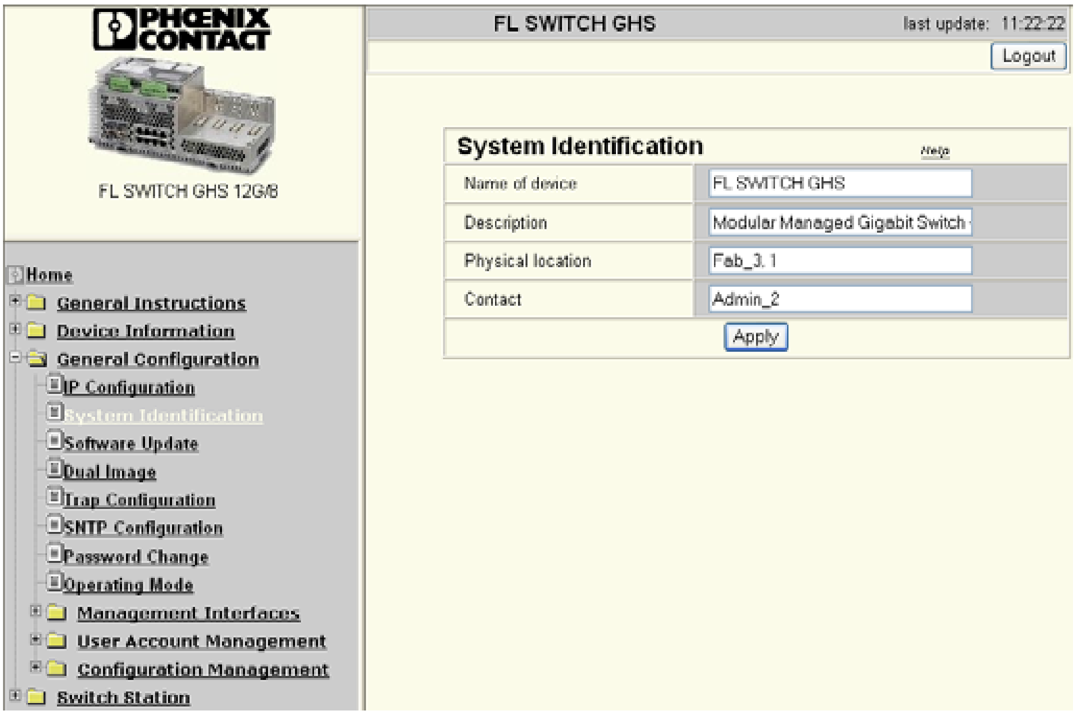
- Call MDC
- Step 1: Select the LLDP function
- Step 2: Set parameters to "Enable" or "Disable"
- Step 3: A list is displayed of all the devices that support LLDP
- In the last column of the table, the time within which the switch sends the LLDP information to the network via BPDU is set for each device
- Step 4: Start downloading the settings
- Step 5: Close MDC

5 Administrative settings

5.1 Assigning names for device identification

5.1.1 WBM

The "System Identification" menu is used to display or modify user-specific device data, e.g., location, device name or function.



FL SWITCH GHS   last update: 11:22:22

System Identification

Name of device	FL SWITCH GHS
Description	Modular Managed Gigabit Switch
Physical location	Fab_3.1
Contact	Admin_2

Figure 5-1 "System Identification" menu

5.1.2 SNMP

The settings can be found under OID 1.3.6.1.2.1.1 under the following path:

Full path: iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).system(1)

5.1.3 CLI

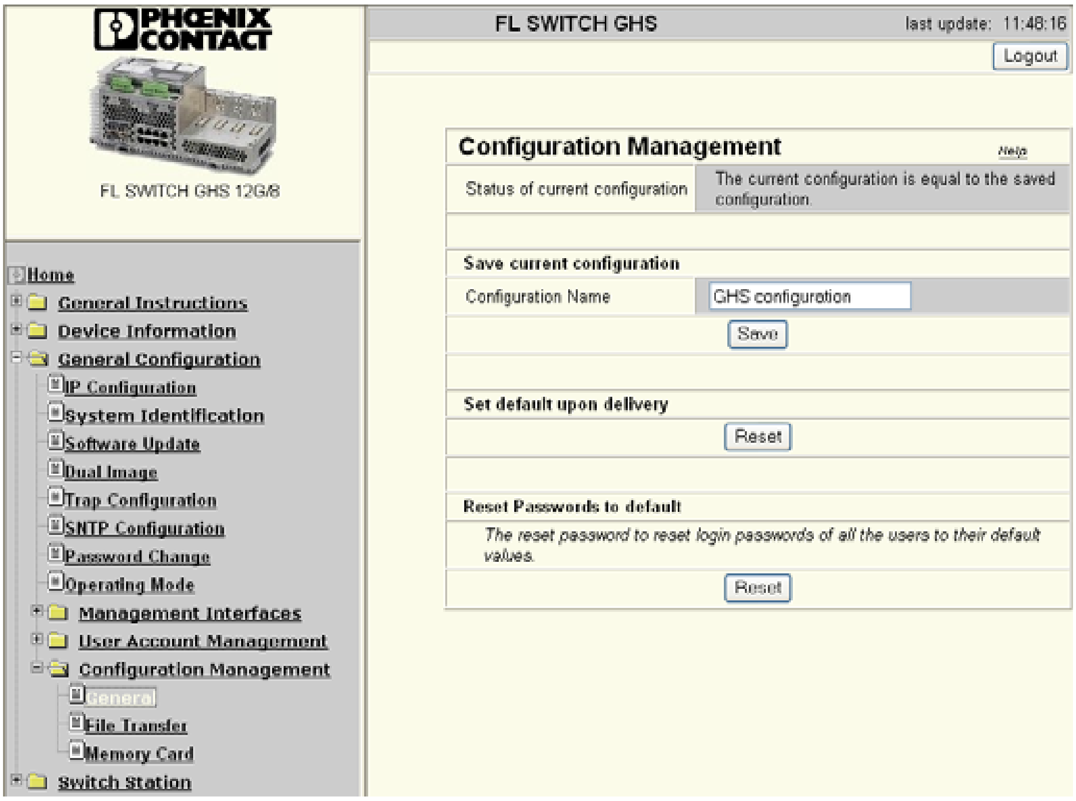
The settings can be found in the CLI under "show sysinfo".

CLI user manual: Unknown source of cross-reference

5.2 Saving the configuration

5.2.1 WBM

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



Configuration Management

Status of current configuration	The current configuration is equal to the saved configuration.
Save current configuration	
Configuration Name	GHS configuration
Set default upon delivery	
Reset Passwords to default	

The reset password to reset login passwords of all the users to their default values.

Figure 5-2 "Configuration Management" menu

Set default upon delivery

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

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

5.2.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.11.2.5 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlConf(5)

5.2.3 CLI

The settings can be found in the CLI under "write memory".

CLI user manual: Unknown source of cross-reference

6 Software update

6.1 Software/firmware update

The "Software Update" menu is used to view or modify the parameters for a software update and to perform the update. The switch suggests a location for saving the new software. (image1 or image2).

> Before performing a software update, save the existing firmware under "save here before" in the "Note: ..." row.

Next, enter the IP address of the TFTP server from which the software upload is started.

> For the TFTP server, start a TFTP server that you have installed on your PC. You can also start the "Factory Manager" tool from Phoenix Contact; this has an integrated TFTP server, but it must be activated.
>
> If you use Factory Manager, you must save the file that is to be installed in the following directory: C:\Program Files\Phoenix Contact\Factory Manager\Version 2.3\download.

The update process can take up to 3 minutes. To use the software, you must restart the switch. This can be done manually or automatically by selecting the "Update with automatic Reboot" option.

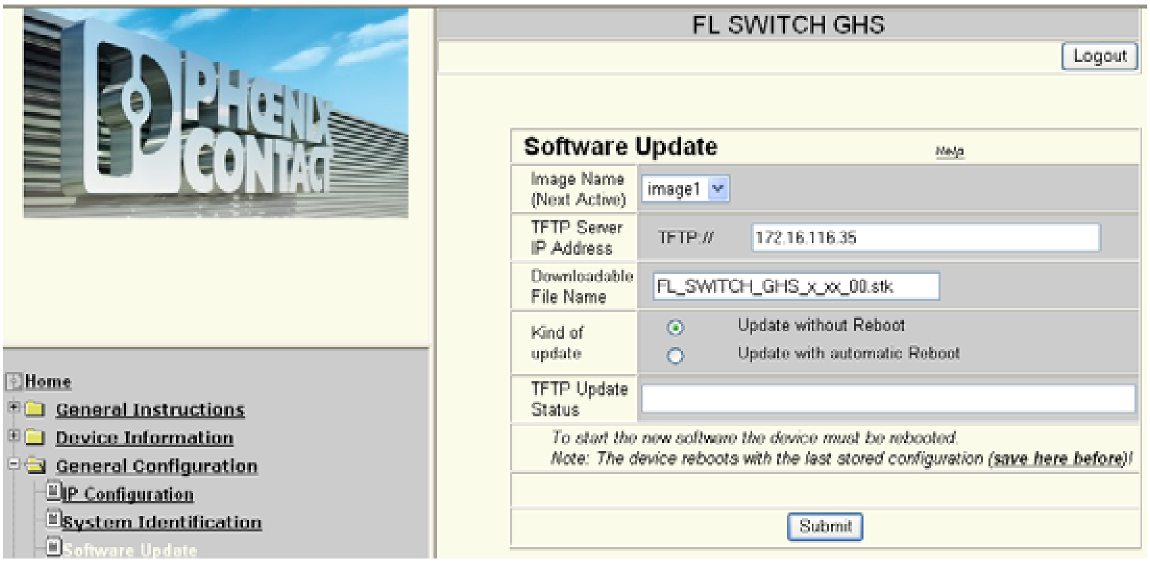
Following reboot, the switch operates with the new firmware.

The old firmware is not deleted, instead it is saved under the other image (example: if the new firmware has been saved under "image2", the previously used firmware will be located in "image1").

To select the old firmware, please refer to Section 6.2 "Dual Image".

6.1.1 WBM

The "Software Update" menu is used to view or modify the parameters for a software update and to trigger the update.



Software Update

Image Name (Next Active): image1

TFTP Server IP Address: TFTP:// 172.16.116.35

Downloadable File Name: FL_SWITCH_GHS_x_xx_00.stk

Kind of update: ● Update without Reboot ○ Update with automatic Reboot

TFTP Update Status:

To start the new software the device must be rebooted.
Note: The device reboots with the last stored configuration (save here before)!

Figure 6-1 "Software Update" web page

A reset is not carried out **automatically** following a firmware update. The desired option can be selected in WBM.

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 settings default upon delivery.

6.1.2 Firmware backup

The device has a backup solution for firmware. Despite a firmware update, the old software is saved in an image and can be selected again later. The switch can then be easily switched to the old software without this having to be installed again. If an error occurs during firmware installation, e.g., for firmware installed under "image1", or you no longer wish to use the new software for other reasons, select the "image2" item under "Image Name (Next Active)" and, following a restart, the switch will start operating with the software version used prior to the software update.

This ensures the continued operability of your switch.

6.1.3 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.11.2.4 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlUpdate(4)

6.1.4 CLI

If you use a serial connection for software update, please note that transfer can take over 30 minutes.

The settings can be found in the CLI under "copy".

CLI user manual: Unknown source of cross-reference

7 PROFINET

The device-specific FDCML/GSDML files for the GHS can be downloaded from the device via the web interface (Device Information/Technical Data/Device Description).

7.1 Selecting PROFINET mode

This selection can be made via the serial interface, Smart mode, the CLI, SNMP or WBM.

When activating PROFINET mode, the following default settings are made for operation:

- The Link Layer Discovery Protocol (LLDP) is activated with the following configuration specifications for PROFINET components:
  - Message transmit interval: 5 s
  - Message transmit hold multiplier: 2
  - TLV port ID with subtype locally assigned in the following format: port-xyz
  - TLV chassis ID with subtype locally assigned transmits the station name
- The Discovery and Configuration Protocol (DCP) is activated as the mechanism for assigning IP parameters.
- The station name (system name) is deleted if the value for the "System Name" object contains the device type (default upon delivery).
- The MRP protocol is not activated.
- The PDEV function is activated.

In addition, when switching to PROFINET mode, the configuration is saved automatically.

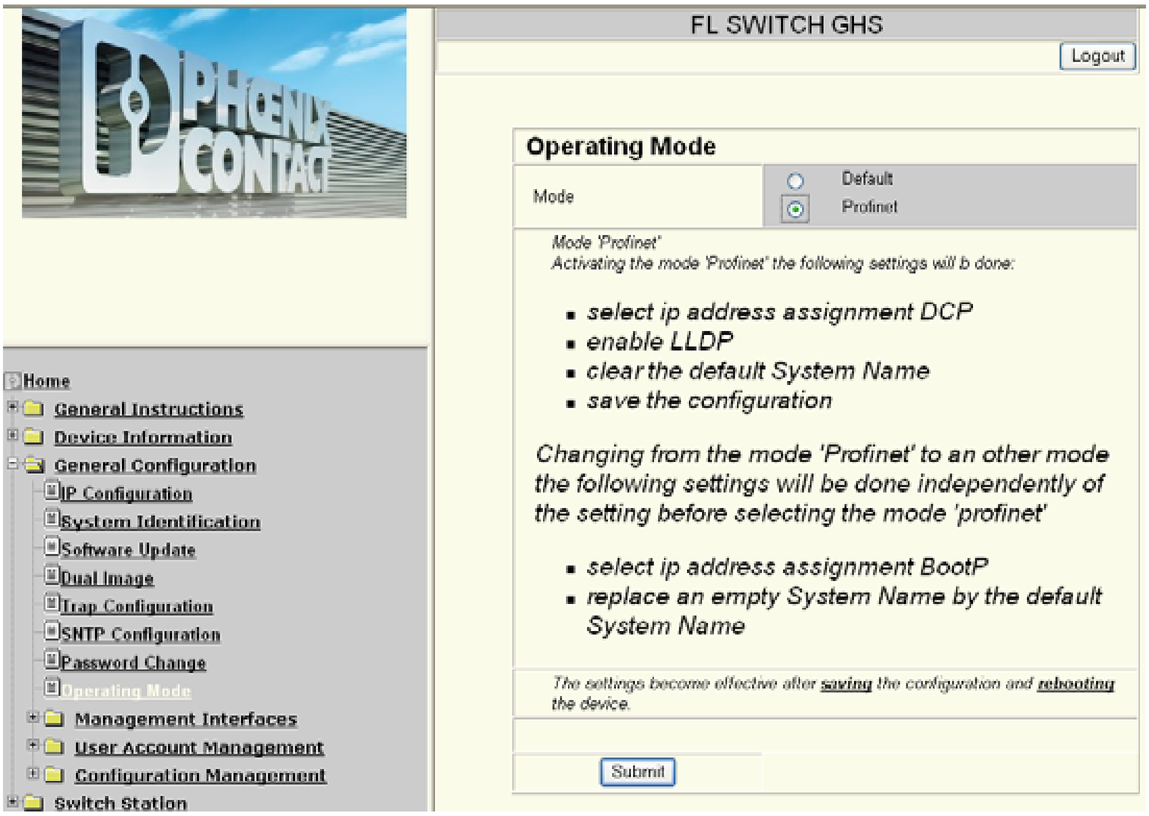
The switch then starts in PROFINET mode for the first time and waits for a name and a PROFINET IP address to be assigned. At this point, the switch is already visible in the network via LLDP with the default name "FL SWITCH ..." and the IP address "0.0.0.0".

The switch indicates in the display that it is waiting for a valid IP configuration via DCP.

The switch cannot be accessed via other network services such as ping at this time.

7.1.1 WBM

The operating mode can be selected in the "Operating Mode" menu.



Operating Mode

Mode: ○ Default ● Profinet

Mode 'Profinet'
Activating the mode 'Profinet' the following settings will b done:

- select ip address assignment DCP
- enable LLDP
- clear the default System Name
- save the configuration

Changing from the mode 'Profinet' to an other mode the following settings will be done independently of the setting before selecting the mode 'profinet'

- select ip address assignment BootP
- replace an empty System Name by the default System Name

The settings become effective after saving the configuration and rebooting the device.

Figure 7-1 "Operating Mode" web page

7.1.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.11.2.1.10 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlBasic(1).flWorkFWCtrlOperatingMode(10)

7.1.3 CLI

The settings for activation can be found in the CLI under "OperatingMode_Profinet".

The other settings can be found under "configure/Profinet".

CLI user manual: Unknown source of cross-reference

7.2 Process data communication

The following process data is used:

Management input byte

Bytes 01/02 - Status word

Byte 03 - Ethernet port 1 - 8

Byte 04 - Ethernet port 9 - 16

Byte 05 - Ethernet port 17 - 24

Byte 06 - Ethernet port 25 - 28

Management output byte

Bytes 01/02 - Control word

Link information for the individual ports

Byte 01 - Port 1
Byte 02 - Port 2
Byte 03 - Port 3

7.2.1 Control word

The control word is a special process data item used to make settings, which are not to be executed via a conventional process data item. The control word of the management agent can be described with a command consisting of two bytes. The device responds to this with the same command in the status word. Byte 0 specifies the action and the new status; byte 1 specifies the port number. If a command is to apply to all the ports, the value 0xFF can be sent instead of the port number. A command should only be sent once, but never in a process data communication cycle.

Table 7-1 Assignment of control word 1

Action	Status	Byte 0	Byte 1
Link monitoring	ON	0x01	Port or 0xFF
	OFF	0x02	Port or 0xFF
POF SCRJ diagnostics	ON	0x03	Port or 0xFF
	OFF	0x04	Port or 0xFF
Power supply	ON	0x05	0x00
	OFF	0x06	0x00
Interface removed	ON	0x07	0x00
	OFF	0x08	0x00
MRP ring failure	ON	0x09	0x00
	OFF	0x0a	0x00
Link enable status	ON	0x20	Port
	OFF	0x21	Port

7.2.1.1 Additional process data

The switch can send the following process data:

- Summary of the link states of all ports (three bytes) - each port corresponds to one bit (0 - Link down; 1 - Link up)

Byte	1, 2, 3, 4	1, 2, 3, 4	1, 2, 3, 4	1, 2, 3, 4	1, 2, 3, 4	1, 2, 3, 4	1, 2, 3, 4	1, 2, 3, 4
Bit	7	6	5	4	3	2	1	0
Port	8/16/24	7/15/23	6/14/22	5/13/21	4/12/20/28	3/11/19/27	2/10/18/26	1/9/17/25

- The slots transmit link information for each port. This includes:
  - Link status: (0 - Link down; 1 - Link up)
  - Far End Fault status: (0 - No fault; 1 - Fault)
  - Port enable status: (0 - Enabled; 1 - Disabled)
  - Link mode: (0 - Forwarding; 1 - Blocking)

Bit	7	6	5	4	3	2	1	0
Meaning	Link mode					Port enable	Far End Fault	Link status

7.2.2 Additional process data

The device has another process data byte, which contains information about the following actual states:

- Status of the alarm contacts: (0 - Closed; 1 - Open)
- Status of the digital inputs: (0 - Low; 1 - High)
- MRP manager status: (0 - Ring OK; 1 - Ring error)

Bit	7	6	5	4	3	2	1	0
Port	MRP				DI 2	DI 1	Alarm contact 2	Alarm contact 1

The slots send link information for each port. This includes:

- Link status: 0 - Link down; 1 - Link up
- Far End Fault status: 0 - No fault; 1 - Fault
- Port enable status: 0 - Enabled; 1 - Disabled
- Link mode: 0 - Forwarding; 1 - Blocking

Bit	7	6	5	4	3	2	1	0
Meaning	Link mode					Port enable	Far End Fault	Link status

8 Activating and configuring redundancy mechanisms

You can select Rapid Spanning Tree (RSTP)/Multiple Spanning Tree (MSTP) or Media Redundancy Protocol (MRP) as the redundancy mechanism. Please note the different requirements for the topology or redundancy management.

The Rapid Spanning Tree Protocol (RSTP) is used to implement network topologies with redundant paths and has now become official IEEE standard 802.1w.

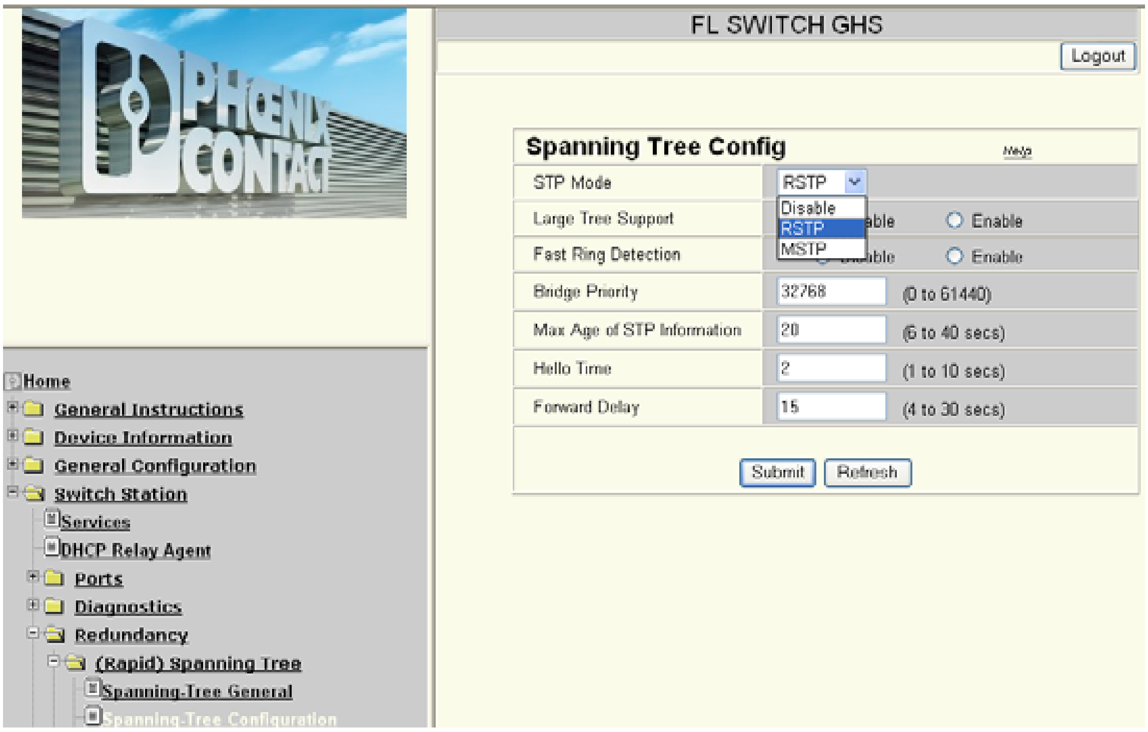
Startup consists of two parts that must be executed in the specified order:

1. Enable (R)STP on all switches that are to be operated as active (R)STP components in the network.
2. Connect the switches to form a meshed topology.

8.1 Activating and configuring RSTP/MSTP

8.1.1 WBM

The Spanning Tree variants can be selected and activated in the "Switch Station/Redundancy/(Rapid) Spanning Tree/Spanning Tree Configuration" menu. When using more than one virtual LAN (VLAN) in a network, the Multiple Spanning Tree Protocol (MSTP) redundancy mechanism defined in IEEE 802.1q is also supported.



FL SWITCH GHS

Spanning Tree Config

STP Mode	RSTP (Disable / RSTP / MSTP)	
Large Tree Support	○ Disable	○ Enable
Fast Ring Detection	○ Disable	○ Enable
Bridge Priority	32768	(0 to 61440)
Max Age of STP Information	20	(6 to 40 secs)
Hello Time	2	(1 to 10 secs)
Forward Delay	15	(4 to 30 secs)

Figure 8-1 "Spanning Tree Configuration" web page

It is sufficient to set the Rapid Spanning Tree status to "Enable" in order to start RSTP using default settings. Priority values can be specified for the switch. The 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 "Priority" field. The value will be rounded automatically to the next multiple of 4096.

Large Tree Support

If RSTP is operated using the default values, it is suitable for up to seven switches along the relevant path. The RSTP protocol would therefore be possible in a ring topology for up to 15 switches.

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

– In the large tree support RSTP topology, do not use devices that do not support large tree support.

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

Maximum Age of STP Information

The parameter is set by the root switch and used by all switches in the ring. The parameter is sent to make sure that each switch in the network has a constant value, against which the age of the saved configuration is tested.

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

Hello Time

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

Forward Delay

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

> The "Maximum Age of STP", "Hello Time", and "Forward Delay" parameters are optimized by default upon delivery. They should not be modified.

8.1.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.15.4 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flSwitch(15).flSwitchRedundancy(4)

8.1.3 CLI

The settings can be found in the CLI under "show spanning-tree".

CLI user manual: Unknown source of cross-reference.

8.2 Activating MRP

A ring can be created in the network using MRP and a redundant connection provided. Each ring must contain an MRP manager, all other devices (in the ring) must support the MRP client function. The ring is created using dedicated ports. The MRP ports must be configured in the switch management. When configured correctly, MRP offers a guaranteed maximum switch-over time of 200 ms.

Please note that MRP is disabled by default upon delivery.

On the Gigabit Modular Switch, MRP licensing is implemented using the FL SD Flash/MRM SD card (Order No. 2700270). If no license is present, "MRP Manager" mode will not be available.

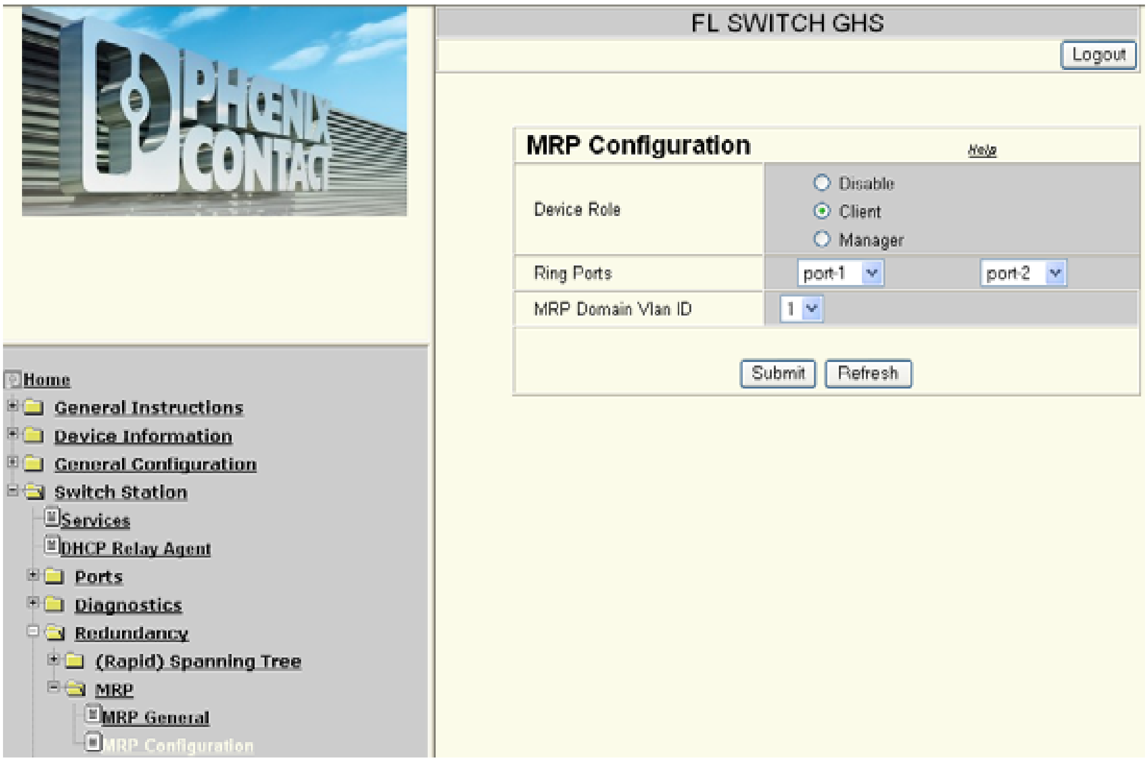
The license can be inserted and activated later during runtime.

Removal of the license during runtime is not recommended.

Only FL SD Flash/MRM cards (Order No. 2700270) from Phoenix Contact can be used for licensing. Formatting the card will result in irrevocable loss of the MRP license.

8.2.1 WBM

The MRP role of this device can be selected and activated in the "Switch Station/Redundancy/MRP/MRP Configuration" menu.



FL SWITCH GHS

MRP Configuration

Device Role: ○ Disable ● Client ○ Manager

Ring Ports: port-1 port-2

MRP Domain Vlan ID: 1

Figure 8-2 "MRP Configuration" web page

Once the role of the switch in the network has been defined, the two ring ports have to be defined.

When using virtual LANs (VLANs), the VLAN where the ring ports are located must also be defined.

8.2.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.11.2.10.1 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlMRP(10).flWorkFWCtrlMRPConfig(1)

8.2.3 CLI

The settings can be found in the CLI under "show mrp".

CLI user manual: Unknown source of cross-reference

9 Activating security mechanisms

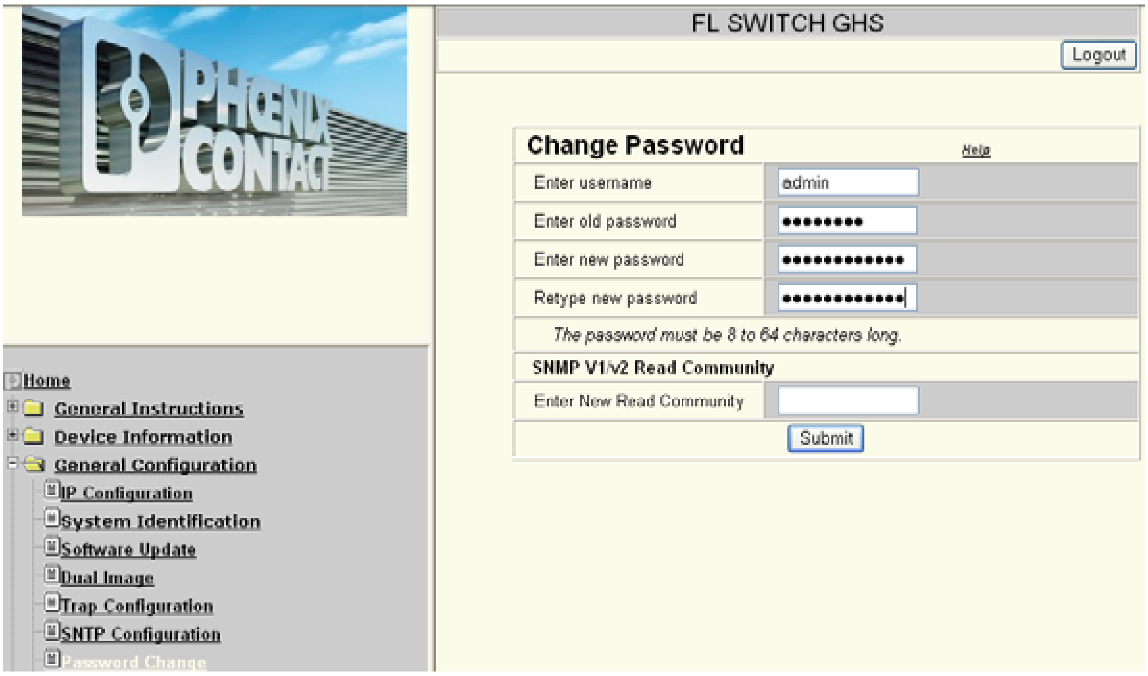
The Gigabit Modular Switch offers comprehensive security features, such as password protection, a security environment, HTTPS, SSH/Telnet, various user access options, and port security features.

In order to modify parameters, you must be logged into the GHS via login access. After successfully logging in for the first time, it is recommended that you change your password.

9.1 Changing the user password

9.1.1 WBM

The current passwords can be changed and activated in the "General Configuration/Change Password" menu.



Change Password

Enter username	admin
Enter old password	•••••••••
Enter new password	•••••••••••••
Retype new password	•••••••••••••

The password must be 8 to 64 characters long.

SNMP V1/v2 Read Community

Enter New Read Community	

Figure 9-1 "Change Password" web page

9.1.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.11.2.3 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxc FactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlPasswd(3)

9.1.3 CLI

The settings can be found in the CLI under "config passwords".

CLI user manual: Unknown source of cross-reference

9.2 Security context

Here, the security context of the device can be:

- – Uploaded from the browser to the device
- – Downloaded and saved from the device
- – Regenerated

The security context contains information that is required for secure access to the device. The security context is generated on initial startup and differs for each individual device. It contains the following information:

– Certificates for secure access to web management

– SSH host key

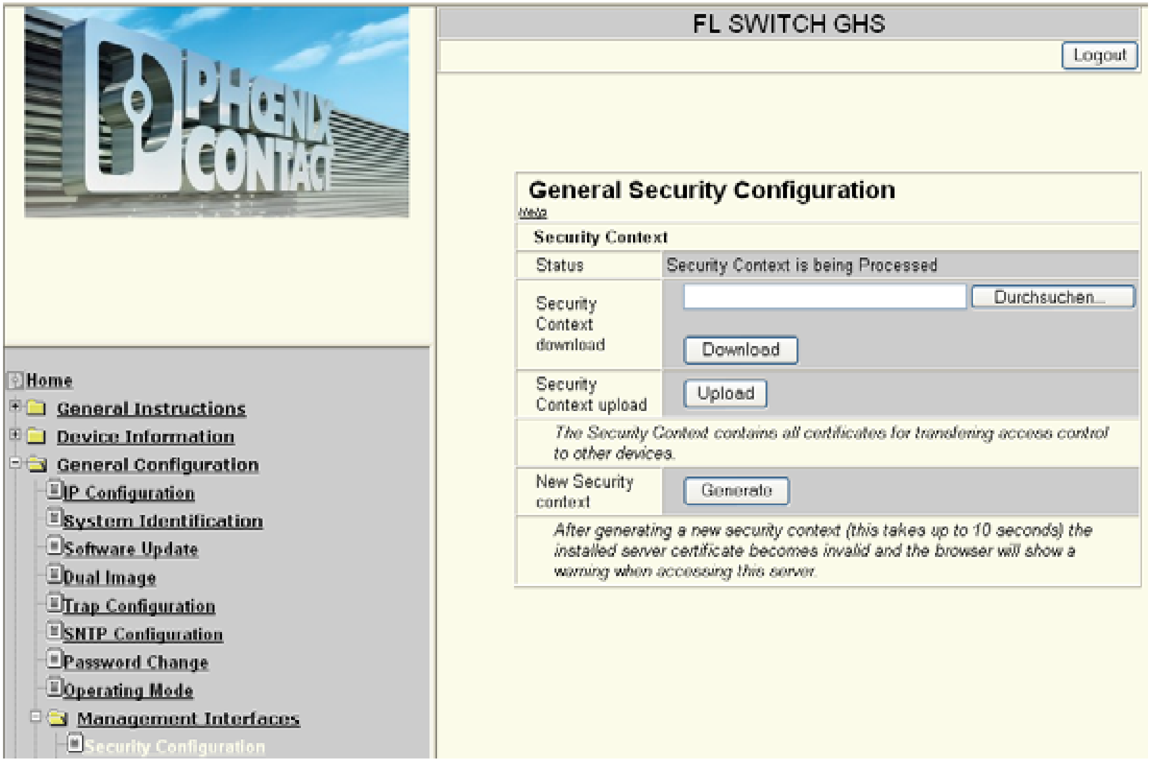
For example, if the server certificate ("HTTPS" menu) is installed in the web browser, the device can be accessed without a browser security warning. Following distribution of the security context to other devices, equally no warning message is generated by the browser when attempting to access web management.

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

ℹ The security context is encrypted with the current valid device password. This means that the security context can only be successfully loaded on the device if the passwords are the same when downloading and uploading the security context. After uploading a security context to the device, web management cannot be accessed for a few seconds.

9.2.1 WBM

The security context can be generated and uploaded/downloaded in the "General Configuration/Management Interfaces/Security Configuration" menu.



General Security Configuration

Help

Security Context

Status	Security Context is being Processed
Security Context download	Durchsuchen... Download
Security Context upload	Upload

The Security Context contains all certificates for transfering access control to other devices.

New Security context	Generate

After generating a new security context (this takes up to 10 seconds) the installed server certificate becomes invalid and the browser will show a warning when accessing this server.

Figure 9-2 "General Security Configuration" web page

9.2.2 SNMP

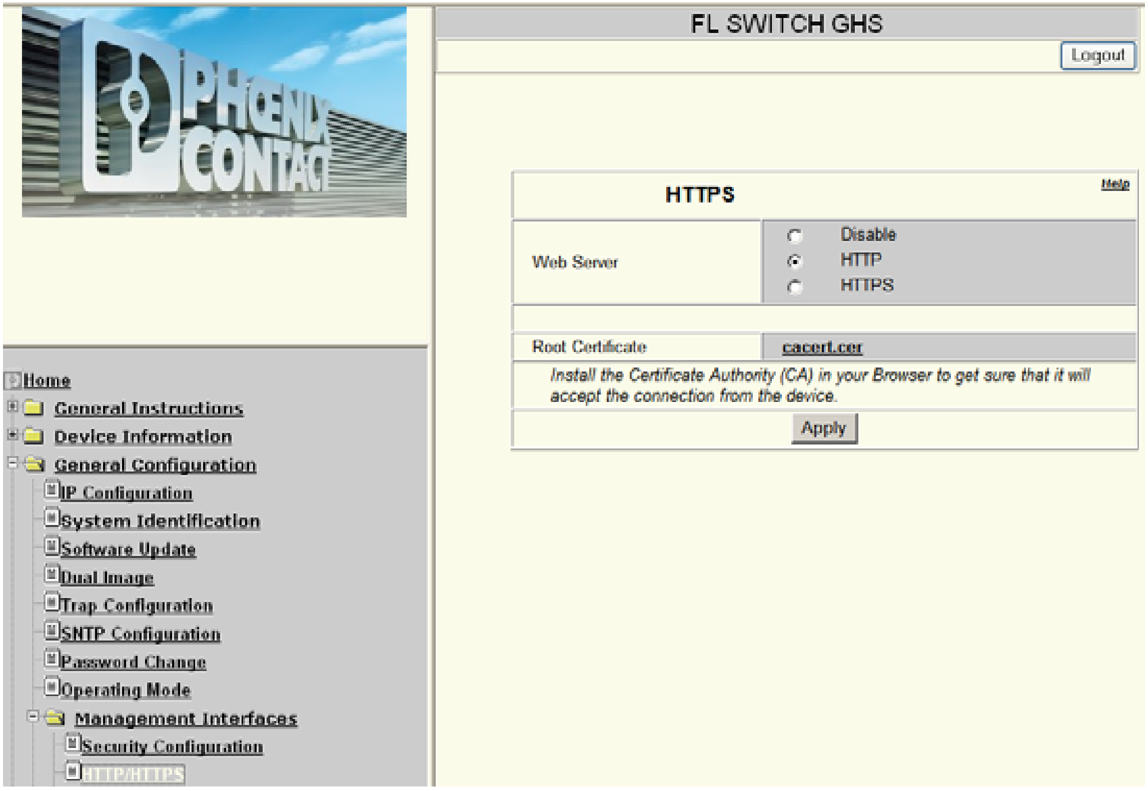
The settings can be found under OID 1.3.6.1.4.1.4346.11.11.20.1.5.3 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkSecurity(20).flWorkSecurityCtrl(1).flWorkSecurityCtrlClientAuth(5).flWorkSecurityCtrlGenSecurityContext(3)

9.3 Web server protocol

9.3.1 WBM

The web server can be disabled or you can choose between HTTP or HTTPS in the "General Configuration/Management Interfaces/HTTP/HTTPS" menu. When the HTTPS protocol is selected, communication between the WBM pages for the switch and the browser on your computer is encrypted and can only be established following prior authentication. The HTTP protocol transmits data in plain text.



FL SWITCH GHS

HTTPS

Web Server	○ Disable ● HTTP ○ HTTPS
Root Certificate	cacert.cer

Install the Certificate Authority (CA) in your Browser to get sure that it will accept the connection from the device.

Figure 9-3 "HTTPS" web page

9.3.2 SNMP

For **HTTP**: The settings can be found under OID 1.3.6.1.4.1.4346.11.11.11.2.1.6 under the following path:

Full path:
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(6)

For **HTTPS**: The settings can be found under OID 1.3.6.1.4.1.4346.11.11.11.2.1.12 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlBasic(1).flWorkFWCtrlHTTPSecure(12)

9.3.3 CLI

The settings can be found in the CLI under "ip".

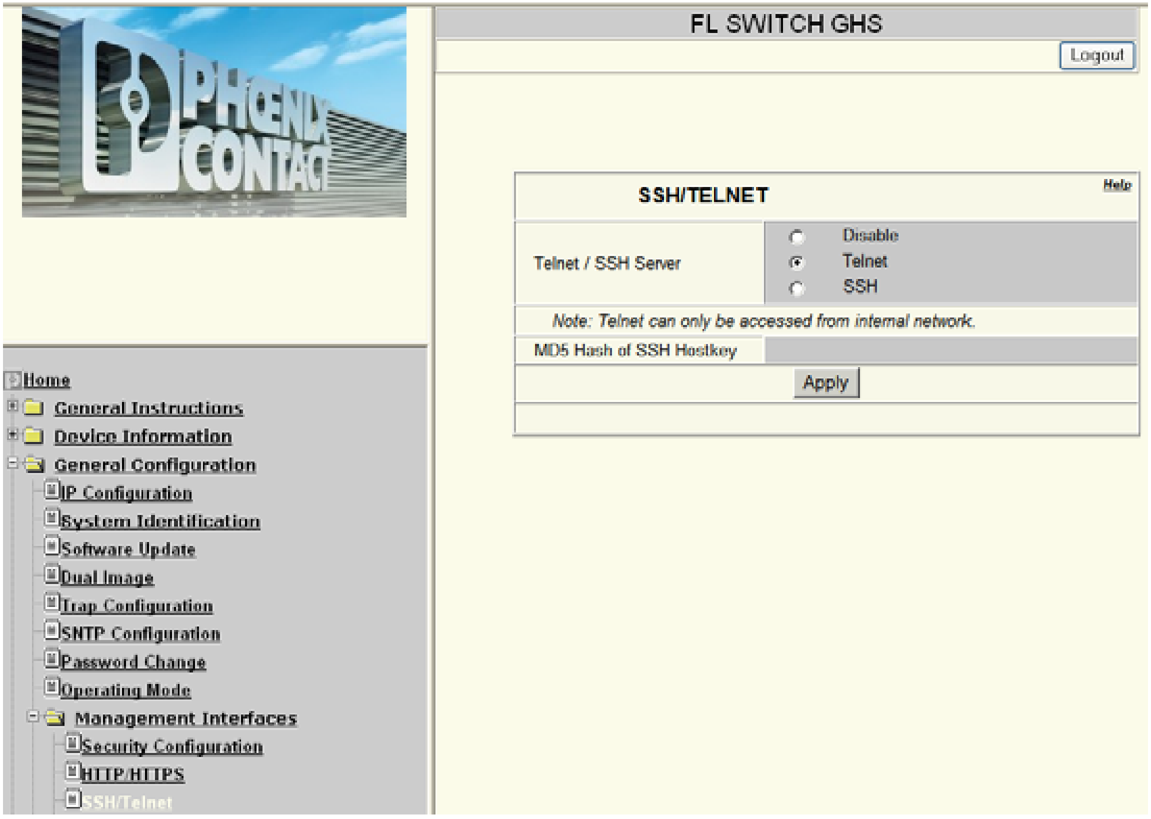
CLI user manual for HTTP: Unknown source of cross-reference

CLI user manual for HTTPS: Unknown source of cross-reference

9.4 Activating Secure Shell/Telnet

9.4.1 WBM

The use of Secure Shell/Telnet can be activated/deactivated in the "General Configuration/Management Interfaces/SSH/Telnet" menu. Secure Shell or SSH refers to a network protocol that can be used to securely establish an encrypted network 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 you were sat at the remote console.



SSH/TELNET

Telnet / SSH Server	○ Disable ● Telnet ○ SSH

Note: Telnet can only be accessed from internal network.

MD5 Hash of SSH Hostkey	

Figure 9-4 "SSH/Telnet" web page

9.4.2 SNMP

For **SSH**: The settings can be found under OID 1.3.6.1.4.1.4346.11.11.11.2.1.13 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlBasic(1).flWorkFWCtrlSSH(13)

For **Telnet**: The settings can be found under OID 1.3.6.1.4.1.4346.11.11.11.2.12.3 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlTelnetGroup(12).flWorkFWCtrlTelnetAllowNewMode(3)

9.4.3 CLI

For SSH: The settings can be found in the CLI under "ip ssh".

For Telnet: The settings can be found in the CLI under "ip telnet".

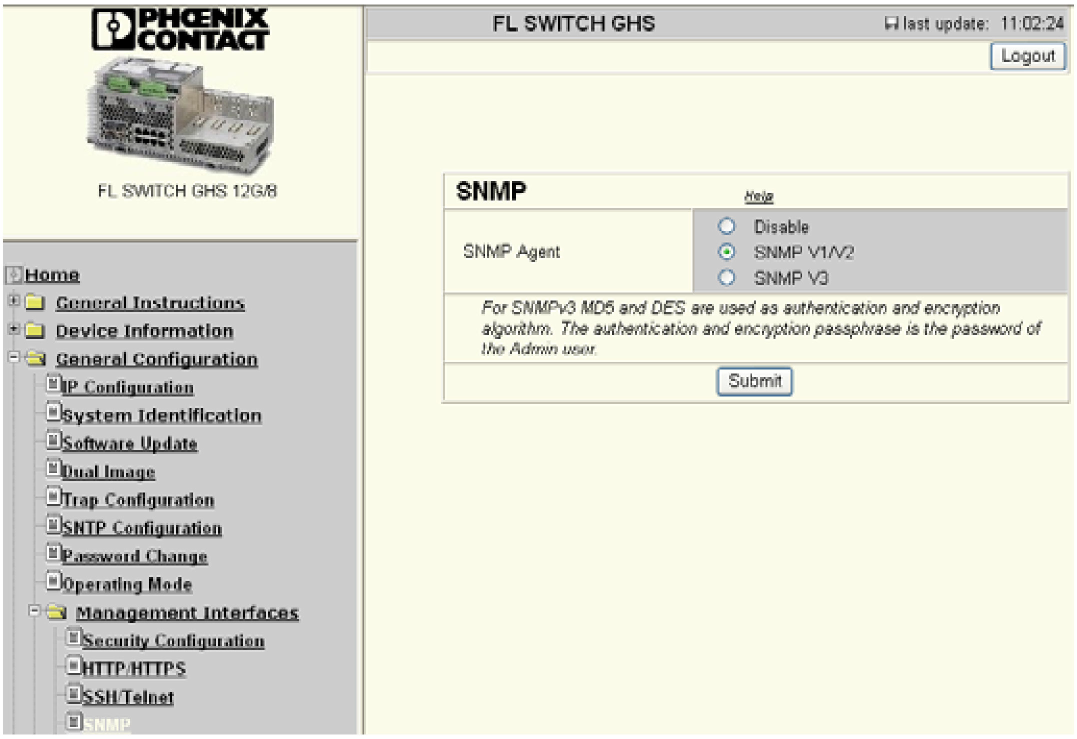
For SSH: CLI user manual: Unknown source of cross-reference

For SSH: CLI user manual: Unknown source of cross-reference

9.5 Activating SNMP

9.5.1 WBM

The use of SNMP can be activated/deactivated or the protocol version can be selected in the "General Configuration/Management Interfaces/SNMP" menu.



SNMP

SNMP Agent: ○ Disable ● SNMP V1/V2 ○ SNMP V3

For SNMPv3 MD5 and DES are used as authentication and encryption algorithm. The authentication and encryption passphrase is the password of the Admin user.

Figure 9-5 "SNMP" web page

9.5.2 SNMP

For **SNMP on/off**: The settings can be found under OID 1.3.6.1.4.1.4346.11.11.11.2.1.9 under the following path:

Full path:
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(9)

For **SNMPv3**: The settings can be found under OID 1.3.6.1.4.1.4346.11.11.11.2.1.14 under the following path:

Full path:
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(14)

9.5.3 CLI

The settings can be found in the CLI under "snmp-server version".

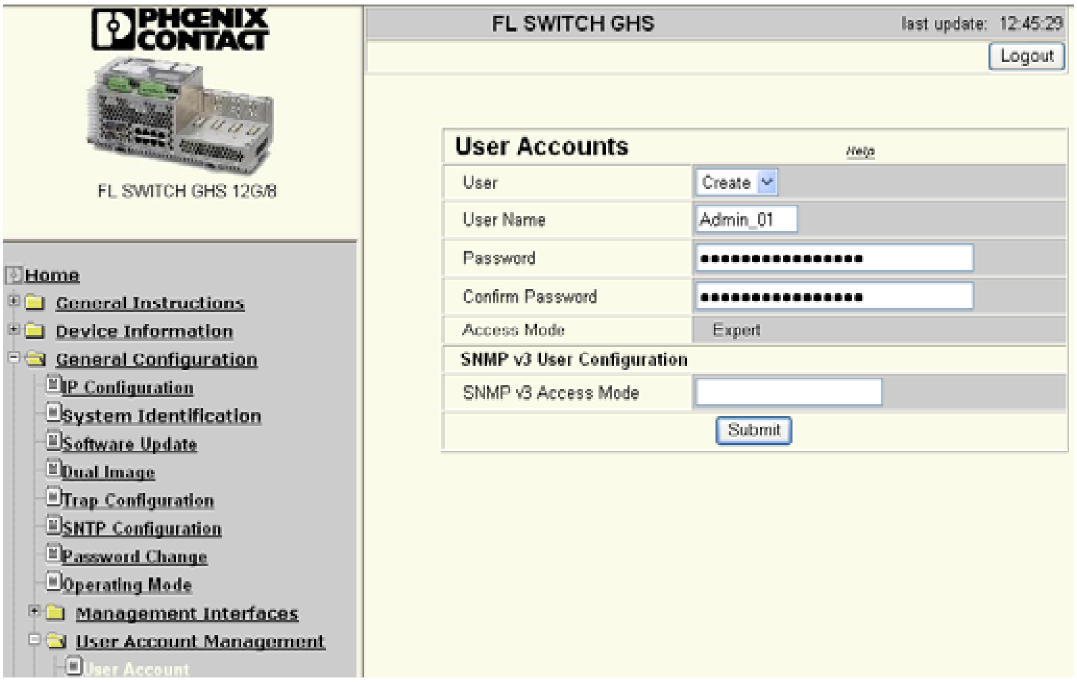
CLI user manual: Unknown source of cross-reference

9.6 Managing user accounts

Various user roles can be created on the GHS. While an administrator has read and write access and can therefore configure and parameterize the switch, a guest user only has read access.

9.6.1 WBM

User accounts can be managed in the "General Configuration/User Account Management/User Account" menu.



User Accounts

User	Create
User Name	Admin_01
Password	●●●●●●●●●●●●●●●●
Confirm Password	●●●●●●●●●●●●●●●●
Access Mode	Expert
SNMP v3 User Configuration	
SNMP v3 Access Mode	

Figure 9-6 "User Accounts" web page

9.6.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.11.2.14 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlUserConfigGroup(14)

9.6.3 CLI

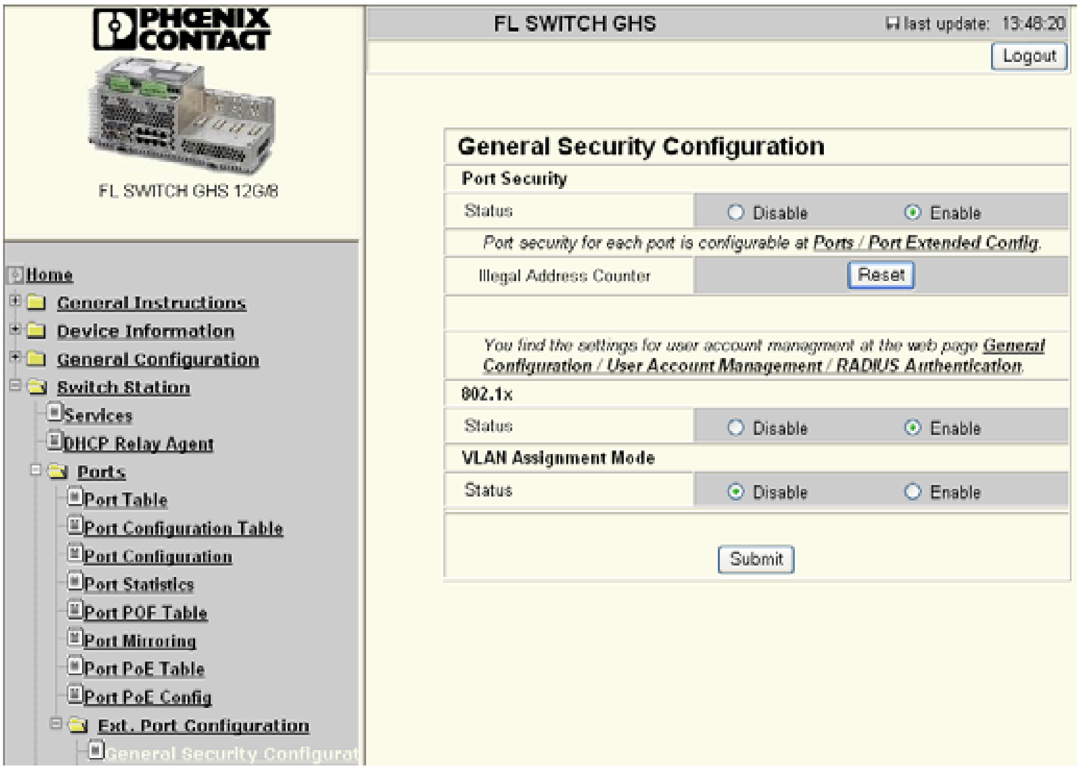
The settings can be found in the CLI under "users".

CLI user manual: Unknown source of cross-reference

9.7 Activating/deactivating port security or IEEE 802.1x

9.7.1 WBM

The use of port security or the IEEE 802.1x function can be enabled/disabled in the "Switch Station/Ports/Ext. Port Configuration/General Security Configuration" menu.



General Security Configuration

Port Security

Status ○ Disable ● Enable

Port security for each port is configurable at Ports / Port Extended Config.

Illegal Address Counter

You find the settings for user account managment at the web page General Configuration / User Account Management / RADIUS Authentication.

802.1x

Status ○ Disable ● Enable

VLAN Assignment Mode

Status ● Disable ○ Enable

Figure 9-7 "General Security Configuration" web page

9.7.2 SNMP

The settings for **Port Security** can be found under OID 1.3.6.1.4.1.4346.11.11.11.2.8.2.5 under the following path:

Full path:
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)

The settings for **IEEE 802.1x** can be found under OID 1.3.6.1.4.1.4346.11.11.11.2.8.3.1 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxc FactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlSecurity(8).flWorkFWCtrlSecurityDot1x(3).flWorkFWCtrlSecurityDot1xPortTable(1)

9.7.3 CLI

The settings for **Port Security** can be found in the CLI under "configure/port-security".

CLI user manual: Unknown source of cross-reference

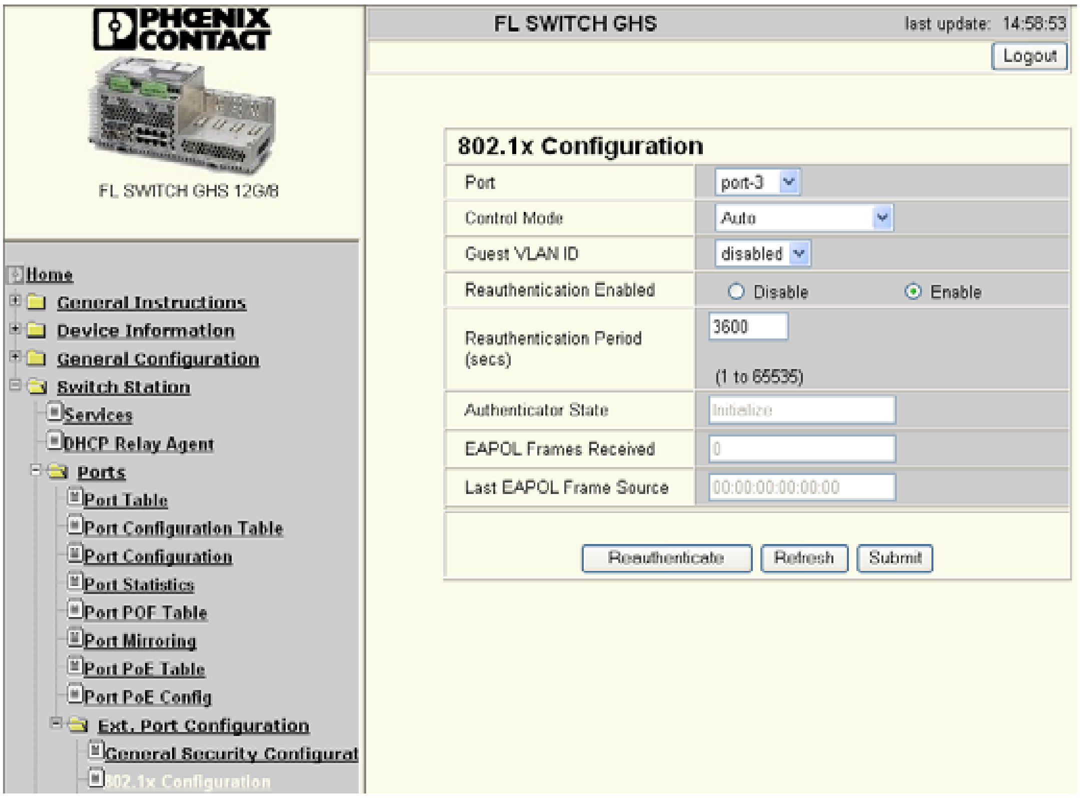
The settings for **IEEE 802.1x** can be found in the CLI under "configure/dot1x".

CLI user manual: Unknown source of cross-reference

9.8 Configuring 802.1x

9.8.1 WBM

The parameters required for IEEE 802.1x can be set in the "Switch Station/Ports/Ext. Port Configuration/802.1x Configuration" menu. The recommended parameters are preset.



802.1x Configuration

Port	port-3
Control Mode	Auto
Guest VLAN ID	disabled
Reauthentication Enabled	○ Disable ● Enable
Reauthentication Period (secs)	3600 (1 to 65535)
Authenticator State	Initialize
EAPOL Frames Received	0
Last EAPOL Frame Source	00:00:00:00:00:00

Figure 9-8 "802.1x Configuration" web page

9.8.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.11.2.8.3.1.1 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlSecurity(8).flWorkFWCtrlSecurityDot1x(3).flWorkFWCtrlSecurityDot1xPortTable(1).flWorkFWCtrlSecurityDot1xPortEntry(1)

9.8.3 CLI

The settings can be found in the CLI under "configure/ot1x port-control".

CLI user manual: Unknown source of cross-reference

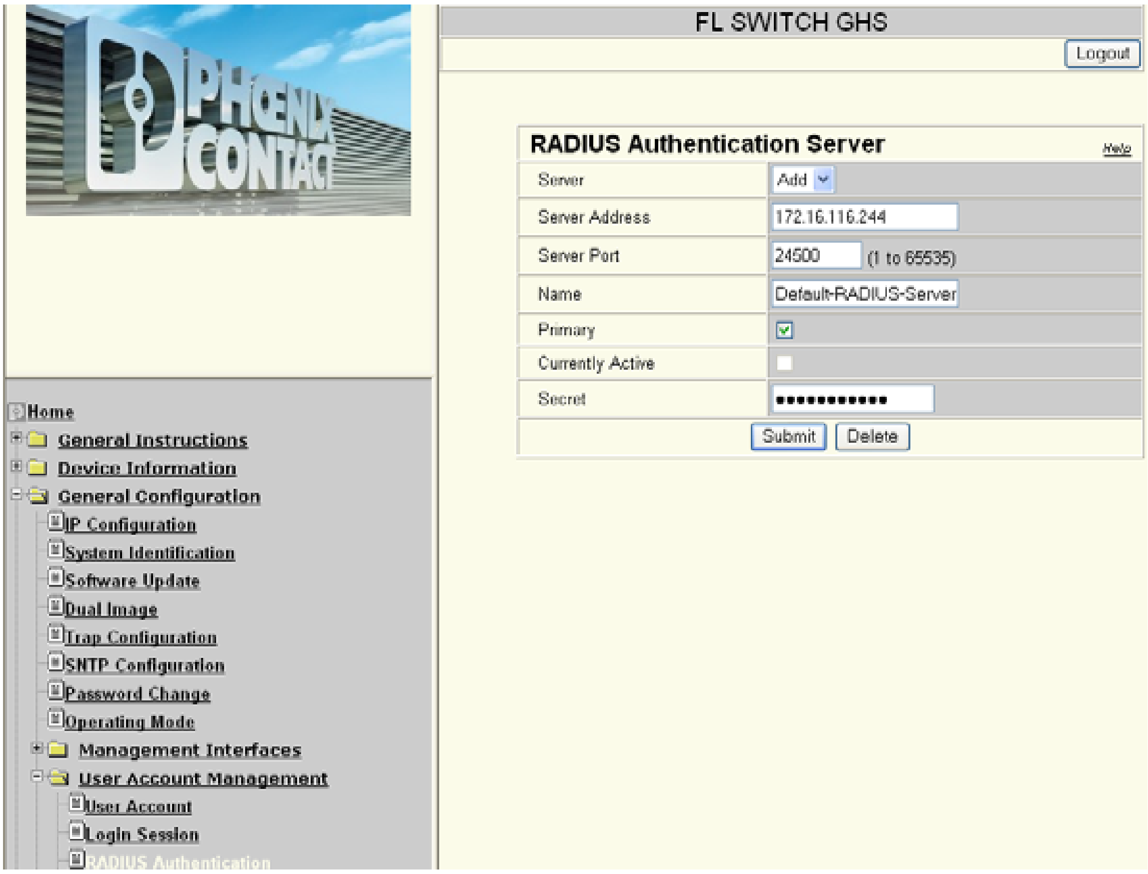
9.9 Configuring the RADIUS server

The RADIUS server is used to implement 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.

9.9.1 WBM

The RADIUS server can be configured in the "General Configuration/User Account Management/RADIUS Authentication" menu.



RADIUS Authentication Server

Server	Add
Server Address	172.16.116.244
Server Port	24500 (1 to 65535)
Name	Default-RADIUS-Server
Primary	☑
Currently Active	□
Secret	●●●●●●●●●●●●

Figure 9-9 "RADIUS Authentication Server" web page

9.9.2 SNMP

The settings can be found in the radiusAuthClientMIB under the following path:

Full path: 1.3.6.1.2.1.67.1.2

This MIB is located in the MIB archive, which can be downloaded from the device web page.

9.9.3 CLI

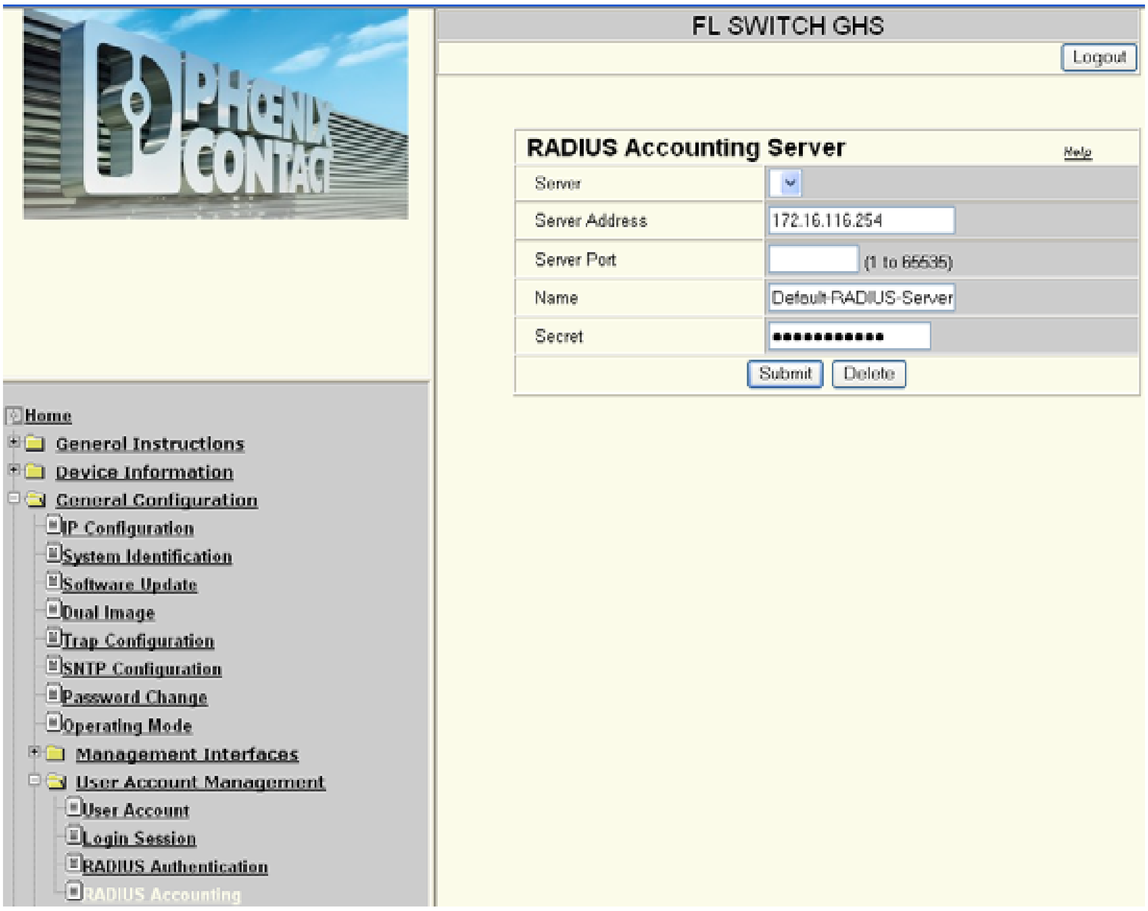
The settings can be found in the CLI under "configure/radius".

CLI user manual: Unknown source of cross-reference

9.10 Configuring the RADIUS accounting server

9.10.1 WBM

The RADIUS accounting server can be configured in the "General Configuration/User Account Management/RADIUS Accounting" menu.



FL SWITCH GHS

RADIUS Accounting Server

Server:
Server Address: 172.16.116.254
Server Port: (1 to 65535)
Name: Default-RADIUS-Server
Secret: ●●●●●●●●●●●●

Figure 9-10 "RADIUS Accounting Server" web page

9.10.2 SNMP

The settings can be found under OID radiusAccClientMIB under the following path:

Full path: 1.3.6.1.2.1.67.2.2

This MIB is located in the MIB archive, which can be downloaded from the device web page.

9.10.3 CLI

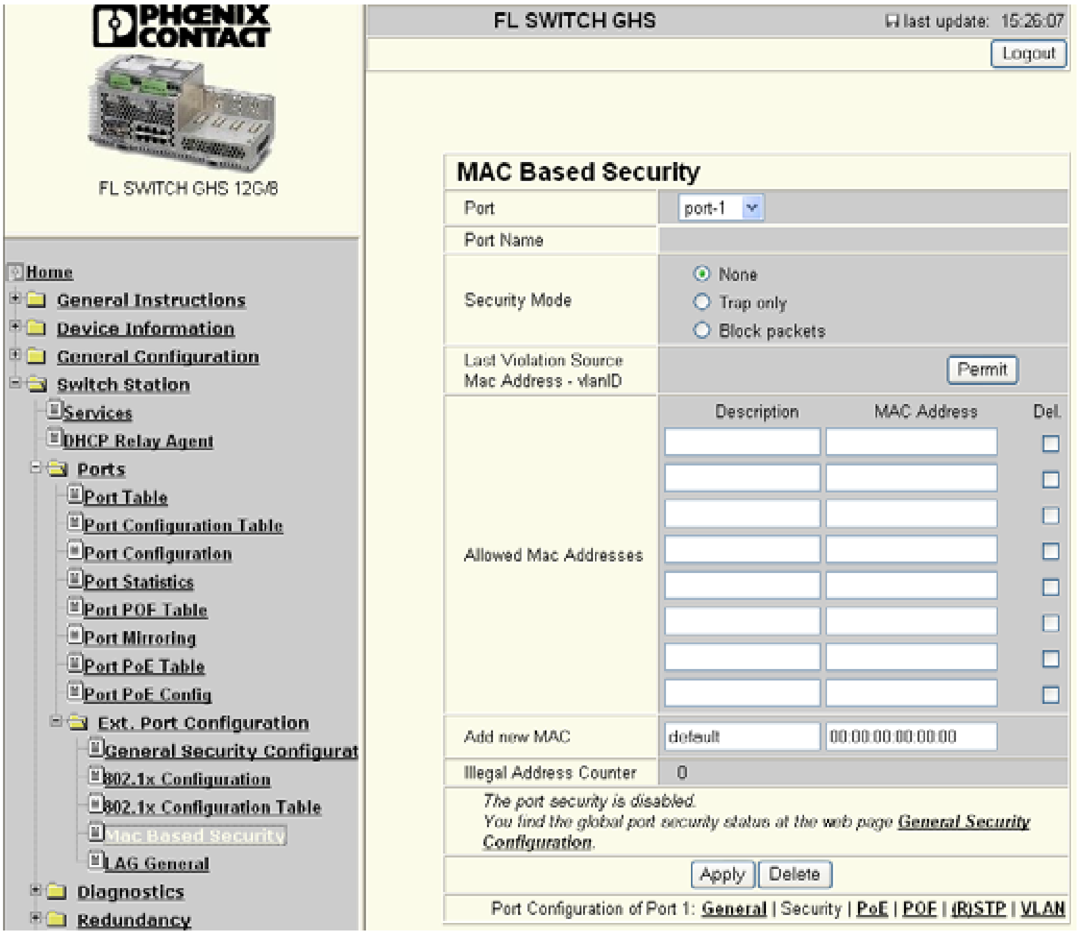
The settings can be found in the CLI under "configure/radius".

CLI user manual: Unknown source of cross-reference

9.11 MAC-based security

9.11.1 WBM

The necessary parameters can be set in the "Switch Station/Ports/Ext. Port Configuration/MAC Based Security" menu.



MAC Based Security

Port	port-1
Port Name	
Security Mode	● None ○ Trap only ○ Block packets
Last Violation Source Mac Address - vlanID	Permit

Allowed Mac Addresses

Description	MAC Address	Del.
		□
		□
		□
		□
		□
		□
		□
		□

Add new MAC	default	00:00:00:00:00:00
Illegal Address Counter	0	

The port security is disabled.
You find the global port security status at the web page ***General Security Configuration****.*

Apply
Delete
Port Configuration of Port 1: General | Security | PoE | POF | (R)STP | VLAN

Figure 9-11 "MAC Based Security" web page

9.11.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.11.2.8.2.2.1 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxc FactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlSecurity(8).flWorkFWCtrlSecurityPort(2).flWorkFWCtrlSecurityPortMacTable(2).flWorkFWCtrlSecurityPortMacEntry(1)

9.11.3 CLI

The settings can be found in the CLI under "configure/port-security".

CLI user manual: Unknown source of cross-reference

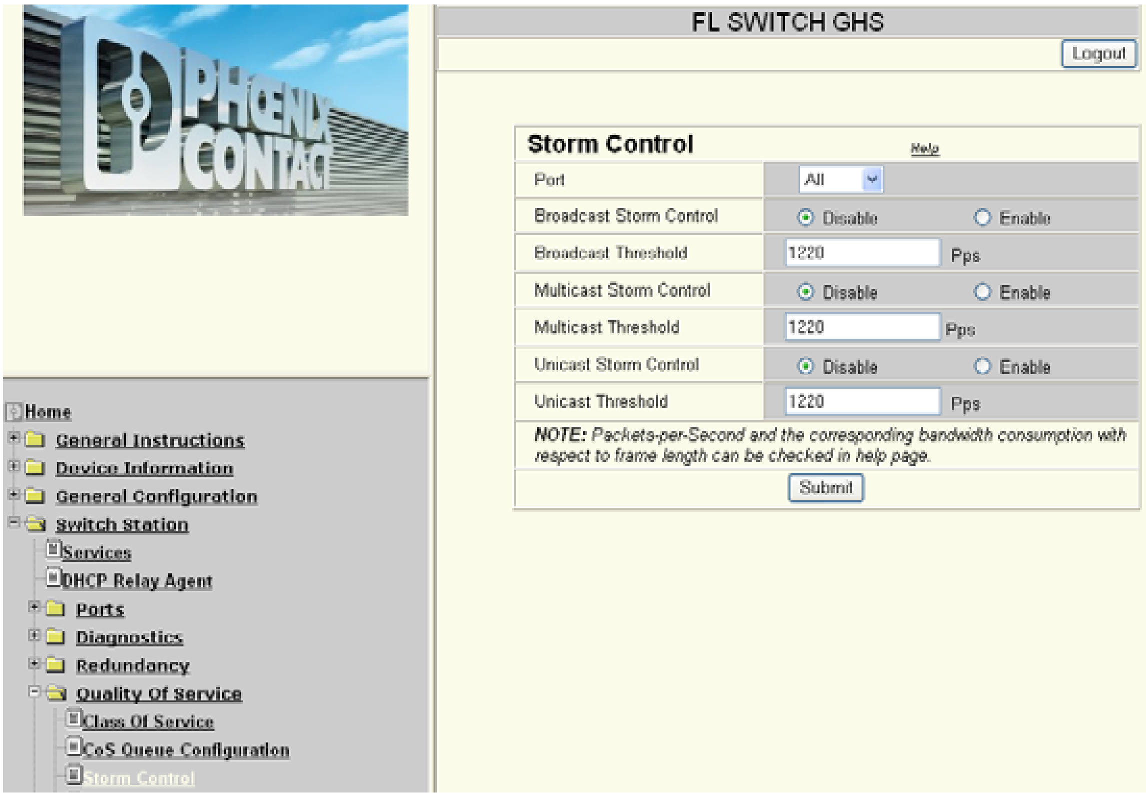
9.12 Storm control

If you have activated the storm control function, you can specify whether the function should be activated for all or only individual ports.

You can then specify the data packet values.

9.12.1 WBM

The necessary parameters can be set in the "Switch Station/Quality of Service/Storm Control" menu.



Storm Control — Help

Port	All	
Broadcast Storm Control	● Disable	○ Enable
Broadcast Threshold	1220 Pps	
Multicast Storm Control	● Disable	○ Enable
Multicast Threshold	1220 Pps	
Unicast Storm Control	● Disable	○ Enable
Unicast Threshold	1220 Pps	

NOTE: Packets-per-Second and the corresponding bandwidth consumption with respect to frame length can be checked in help page.

Submit

Figure 9-12 "Storm Control" web page

9.12.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.15.6 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flSwitch(15).flSwitchRateCtrl(6)

9.12.3 CLI

The settings can be found in the CLI under "configure/storm-control".

CLI user manual: Unknown source of cross-reference

10 Activating a VLAN

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

– Data packets are only forwarded within the relevant VLAN.

– The members of a VLAN can be distributed over a large area.

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

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

10.1 Management VLAN ID

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

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

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

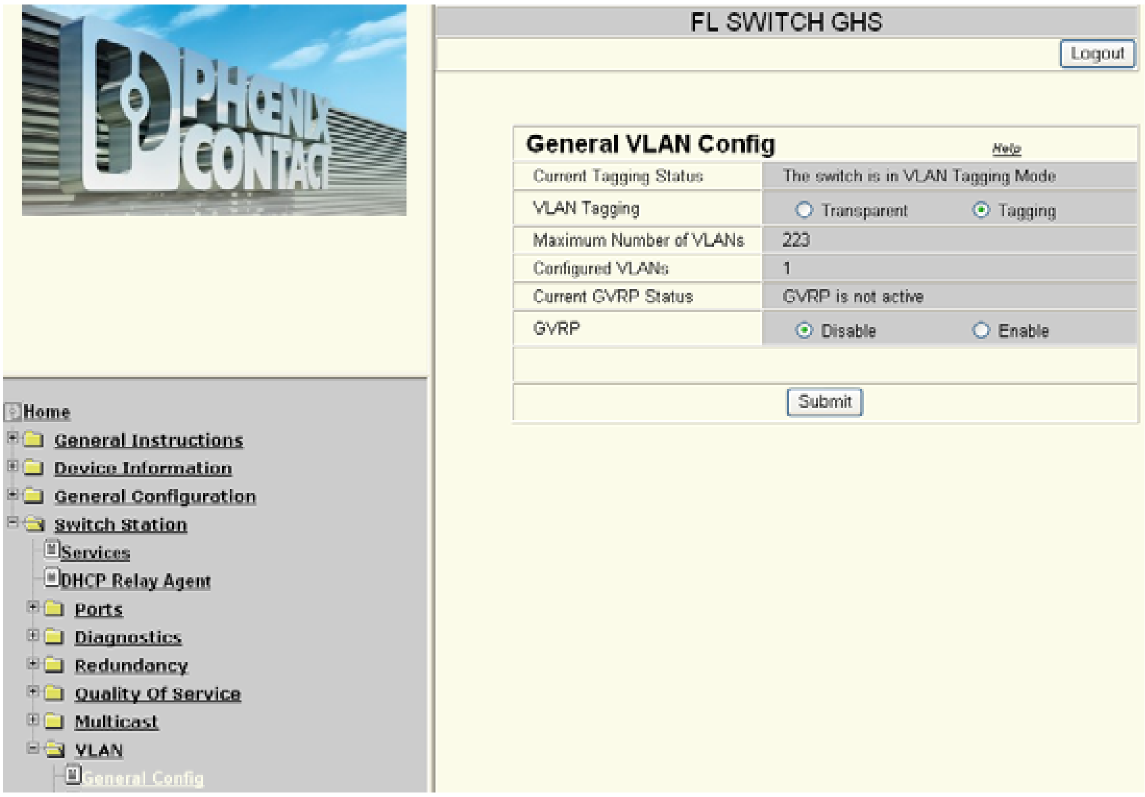
ℹ If you delete the VLAN in which the switch is managed, management is automatically switched to VLAN 1.

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

10.2 General VLAN configuration

10.2.1 WBM

The use of VLANs can be activated/deactivated in the "Switch Station/VLAN/General Config" menu.



General VLAN Config

Current Tagging Status	The switch is in VLAN Tagging Mode
VLAN Tagging	○ Transparent ● Tagging
Maximum Number of VLANs	223
Configured VLANs	1
Current GVRP Status	GVRP is not active
GVRP	● Disable ○ Enable

Figure 10-1 "General VLAN Config" web page

10.2.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.15.1.5 under the following path:

Full path:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flSwitch(15).flSwitchCtrl(1).flSwitchCtrlVlanTagMode(5)

10.2.3 CLI

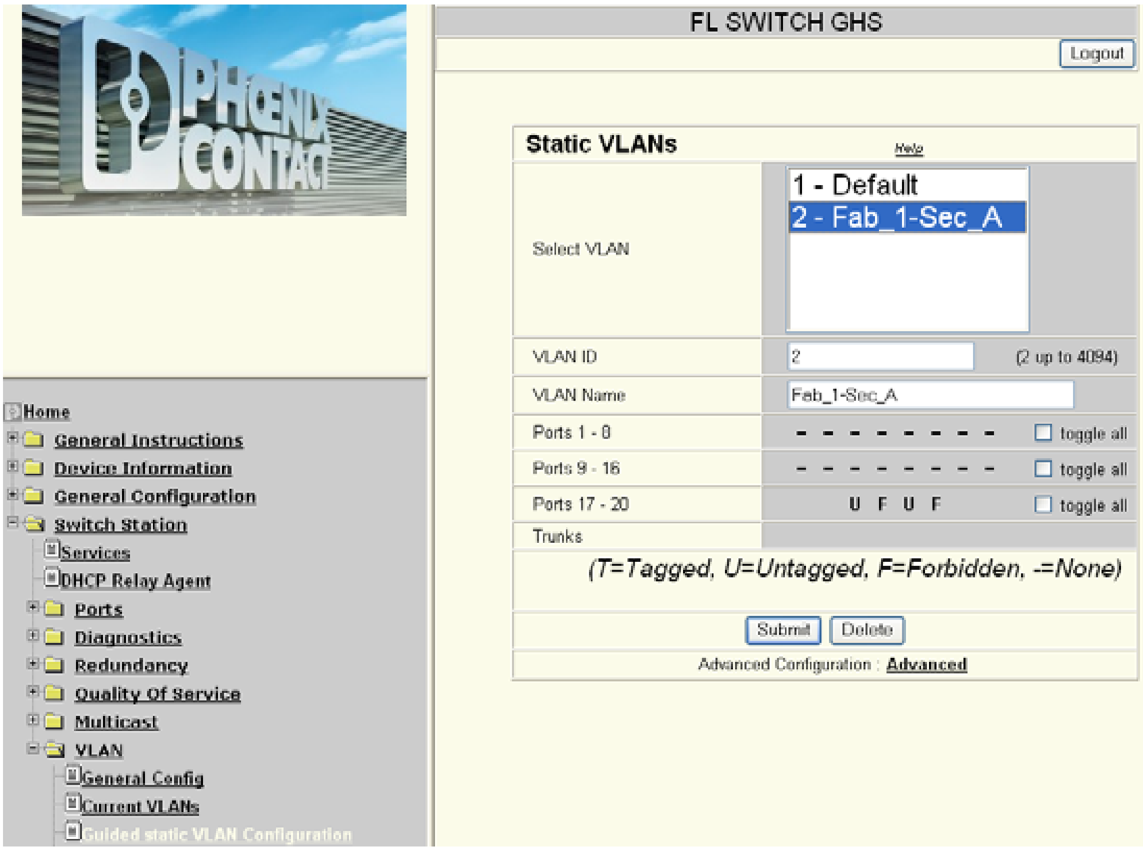
The settings can be found in the CLI under "config vlan".

CLI user manual: Unknown source of cross-reference

10.3 Configuring static VLANs

10.3.1 WBM

Static VLANs can be created and the ports assigned accordingly in the "Switch Station/VLAN/Guided static VLAN Configuration" menu.



FL SWITCH GHS

Static VLANs

Select VLAN	1 - Default 2 - Fab_1-Sec_A	
VLAN ID	2	(2 up to 4094)
VLAN Name	Fab_1-Sec_A	
Ports 1 - 8	- - - - - - - -	□ toggle all
Ports 9 - 16	- - - - - - - -	□ toggle all
Ports 17 - 20	U F U F	□ toggle all
Trunks		

(T=Tagged, U=Untagged, F=Forbidden, -=None)

Advanced Configuration : Advanced

Figure 10-2 "Static VLANs" web page

10.3.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.15.1.5 under the following path:

Full path:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flSwitch(15).flSwitchCtrl(1).flSwitchCtrlVlanTagMode(5)

10.3.3 CLI

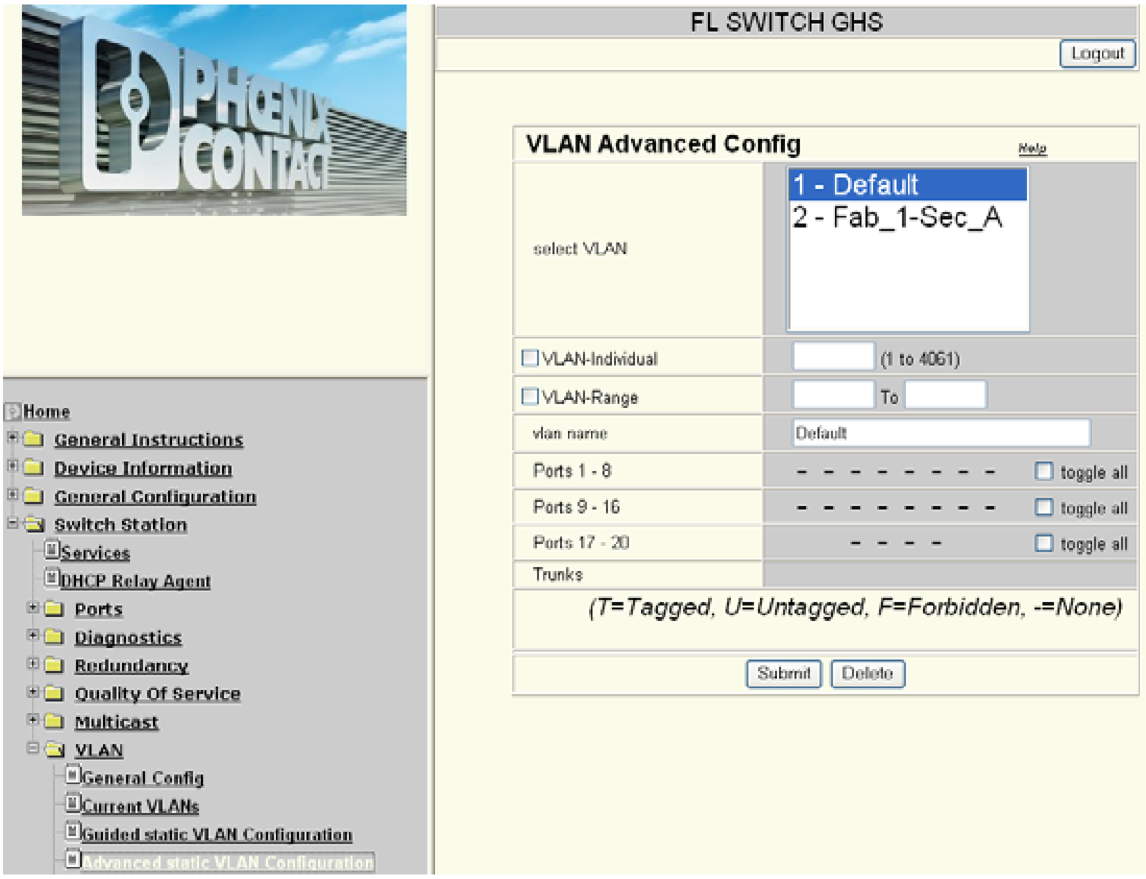
The settings can be found in the CLI under "configure/vlan".

Unknown source of cross-reference

10.4 VLAN Advanced Config

10.4.1 WBM

Static VLANs can be created and the ports assigned accordingly in the "Switch Station/VLAN/Advanced static VLAN Configuration" menu.



VLAN Advanced Config

select VLAN	1 - Default 2 - Fab_1-Sec_A
□ VLAN-Individual	(1 to 4061)
□ VLAN-Range	To
vlan name	Default
Ports 1 - 8	- - - - - - - - □ toggle all
Ports 9 - 16	- - - - - - - - □ toggle all
Ports 17 - 20	- - - - □ toggle all
Trunks	

(T=Tagged, U=Untagged, F=Forbidden, -=None)

Figure 10-3 "VLAN Advanced Config" web page

10.4.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.15.1.5 under the following path:

Full path: iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flSwitch(15).flSwitchCtrl(1).flSwitchCtrlVlanTagMode(5)

10.4.3 CLI

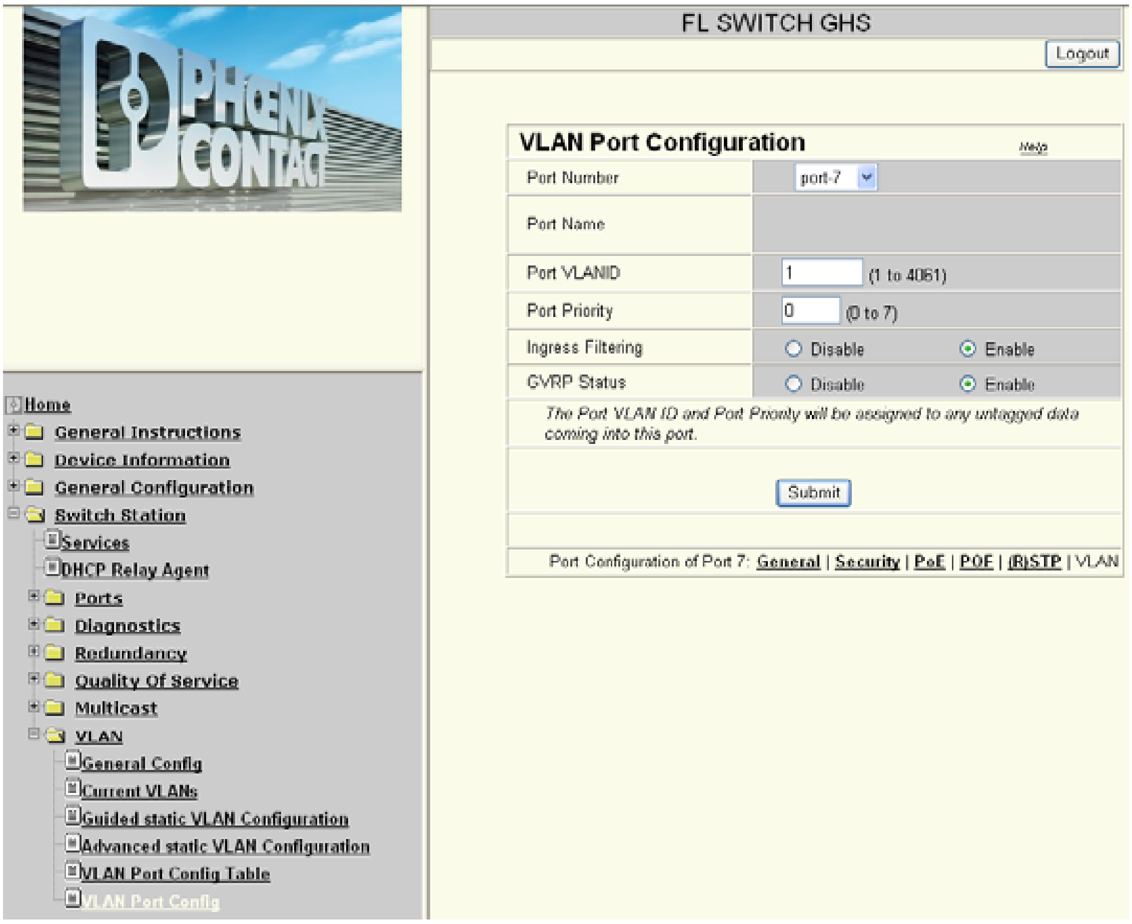
The settings can be found in the CLI under "configure/vlan".

Unknown source of cross-reference

10.5 VLAN Port Configuration

10.5.1 WBM

Port-specific VLAN settings can be made in the "Switch Station/VLAN/VLAN Port Config" menu.



VLAN Port Configuration

Port Number	port-7
Port Name	
Port VLANID	1 (1 to 4061)
Port Priority	0 (0 to 7)
Ingress Filtering	○ Disable ● Enable
GVRP Status	○ Disable ● Enable

The Port VLAN ID and Port Priority will be assigned to any untagged data coming into this port.

Port Configuration of Port 7: General | Security | PoE | POF | (R)STP | VLAN

Figure 10-4 "VLAN Port Configuration" web page

10.5.2 SNMP

The settings can be found under OID 1.3.6.1.2.1.17.7.1.4 under the following path:

Full path: iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).dot1dBridge(17).qBridgeMIB(7).qBridgeMIBObjects(1).dot1qVlan(4)

10.5.3 CLI

The settings can be found in the CLI under "configure/vlan".

Unknown source of cross-reference

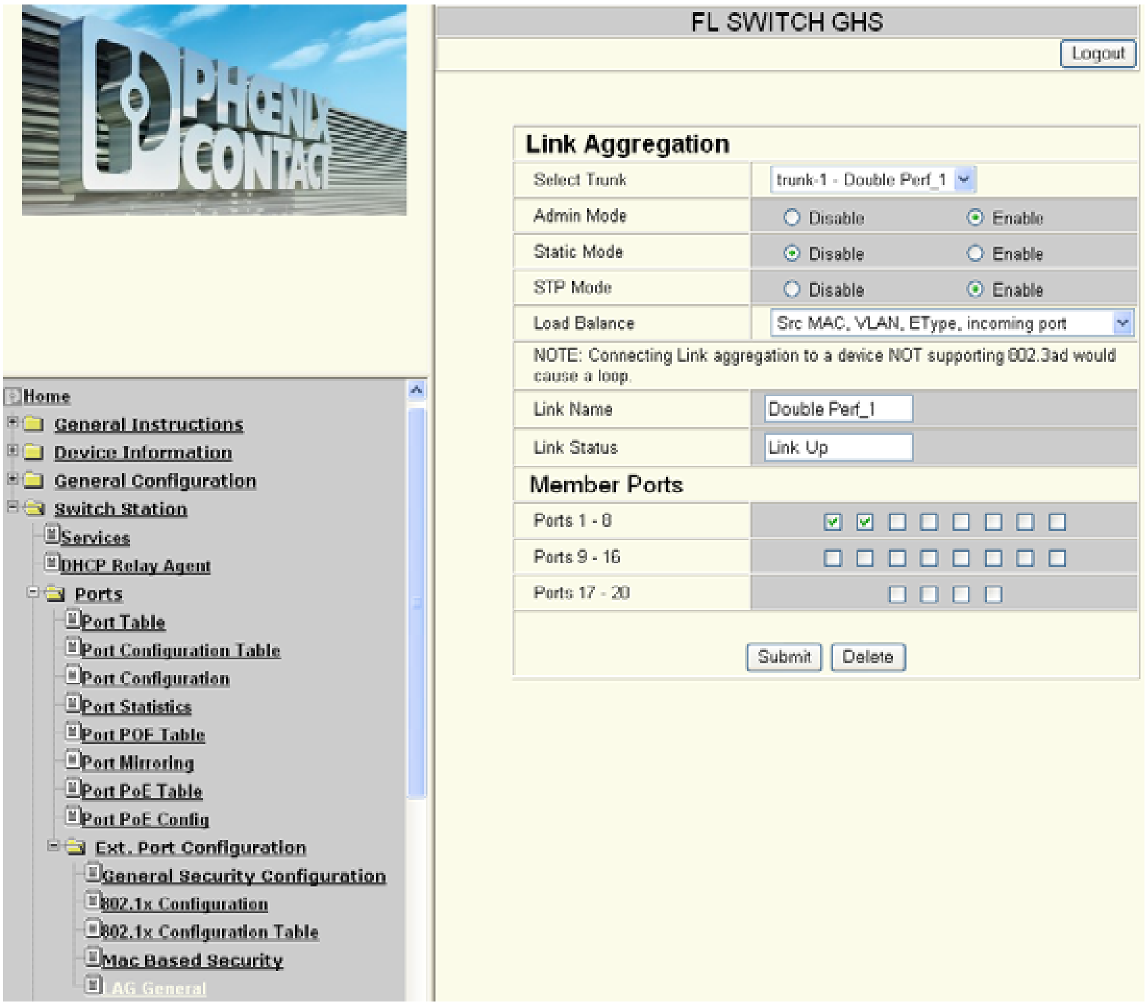
11 Link aggregation

> Make sure that link aggregation is only supported between switches that meet the requirements of standard IEEE 802.3ad.

11.1 Configuring link aggregation

11.1.1 WBM

The use of VLANs can be activated/deactivated in the "Switch Station/Ports/Ext. Port Configuration/LAG General" menu.



Link Aggregation

Select Trunk	trunk-1 - Double Perf_1	
Admin Mode	○ Disable	● Enable
Static Mode	● Disable	○ Enable
STP Mode	○ Disable	● Enable
Load Balance	Src MAC, VLAN, EType, incoming port	

NOTE: Connecting Link aggregation to a device NOT supporting 802.3ad would cause a loop.

Link Name	Double Perf_1
Link Status	Link Up

Member Ports

Ports 1 - 8	☑ ☑ □ □ □ □ □ □
Ports 9 - 16	□ □ □ □ □ □ □ □
Ports 17 - 20	□ □ □ □

Figure 11-1 "Link Aggregation" web page

11.1.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.15.8 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flSwitch(15).flSwitchLagConfig(8)

11.1.3 CLI

The general settings can be found in the CLI under "config/port-channel".

CLI user manual: Unknown source of cross-reference

12 Time settings

12.1 Simple Network Time Protocol (SNTP)

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 to thus 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.

Clients should therefore only be activated on the most remote devices of an NTP network. 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.

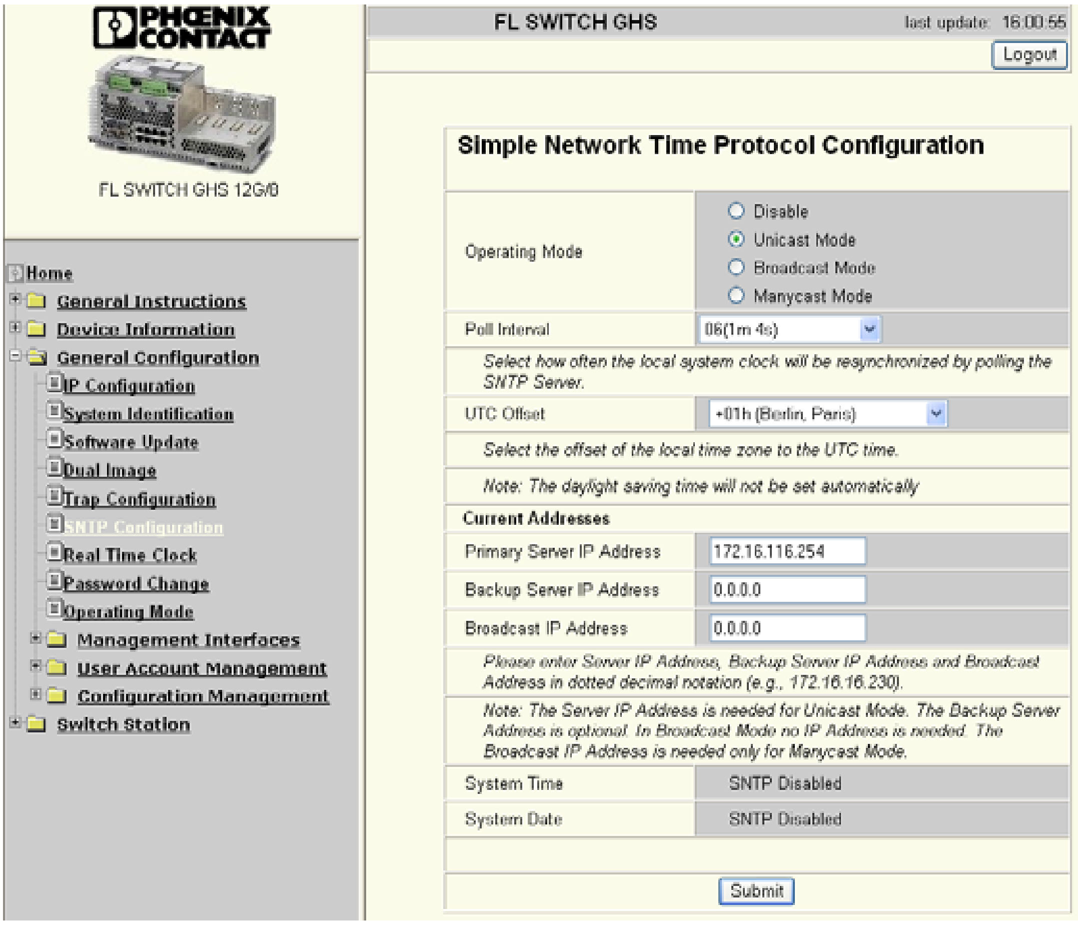
The switch supports the use of the SNTP protocol except in client mode, i.e., switches or other network components only ever receive a time from a time server, but do not transmit their own times.

- Each client synchronizes its system time with that of an SNTP server
- Time synchronization is carried out at fixed synchronization intervals
- The local system time of the client is thus constantly corrected
- Synchronization is carried out in Universal Time Coordinated (UTC) format

12.2 Configuring SNTP

12.2.1 WBM

The use of SNTP can be configured in the "General Configuration/SNTP Configuration" menu.



last update: 16:00:55

Simple Network Time Protocol Configuration

Operating Mode	○ Disable ● Unicast Mode ○ Broadcast Mode ○ Manycast Mode
Poll Interval	06(1m 4s)
Select how often the local system clock will be resynchronized by polling the SNTP Server.	
UTC Offset	+01h (Berlin, Paris)
Select the offset of the local time zone to the UTC time.	
Note: The daylight saving time will not be set automatically	
Current Addresses	
Primary Server IP Address	172.16.116.254
Backup Server IP Address	0.0.0.0
Broadcast IP Address	0.0.0.0
Please enter Server IP Address, Backup Server IP Address and Broadcast Address in dotted decimal notation (e.g., 172.16.16.230).	
Note: The Server IP Address is needed for Unicast Mode. The Backup Server Address is optional. In Broadcast Mode no IP Address is needed. The Broadcast IP Address is needed only for Manycast Mode.	
System Time	SNTP Disabled
System Date	SNTP Disabled

Figure 12-1 "Simple Network Time Protocol Configuration" web page

12.2.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.21.1 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkTimeSynch(21).flWorkTimeSynchSntp(1)

12.2.3 CLI

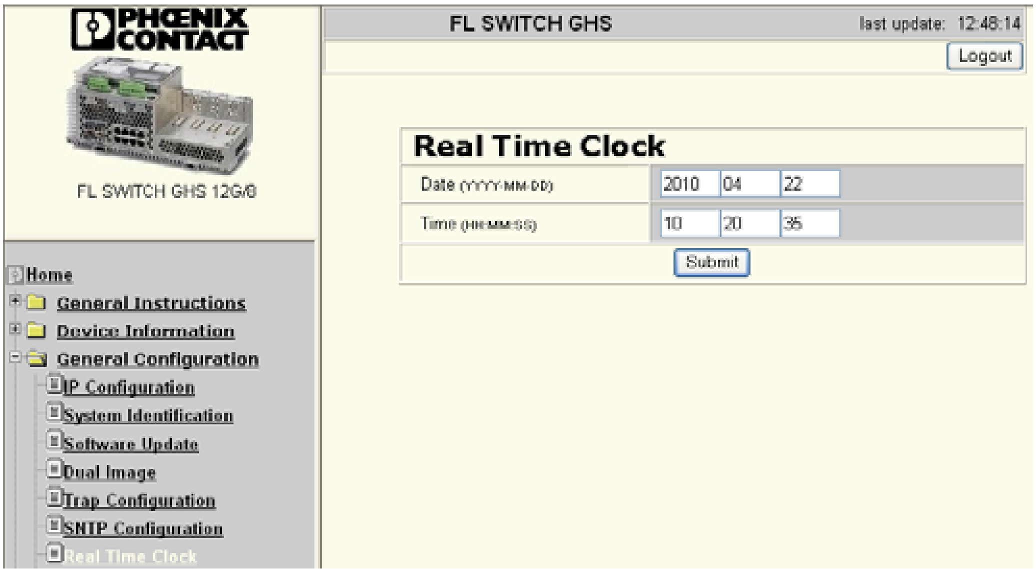
The settings can be found in the CLI under "configure/sntp".

CLI user manual: Unknown source of cross-reference

12.3 Configuring the realtime clock

12.3.1 WBM

The use of an internal clock, which continues running in the event of power failure, can be configured in the "General Configuration/Real Time Clock" menu. The RTC is set automatically if time information has been received via SNTP.



last update: 12:48:14

Real Time Clock

Date (YYYY-MM-DD)	2010	04	22
Time (HH:MM:SS)	10	20	35

Figure 12-2 "Real Time Clock" web page

12.3.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.21.2 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkTimeSynch(21).flWorkTimeSynchRTC(2)

12.3.3 CLI

The settings can be found in the CLI under "time set".

CLI user manual: Unknown source of cross-reference

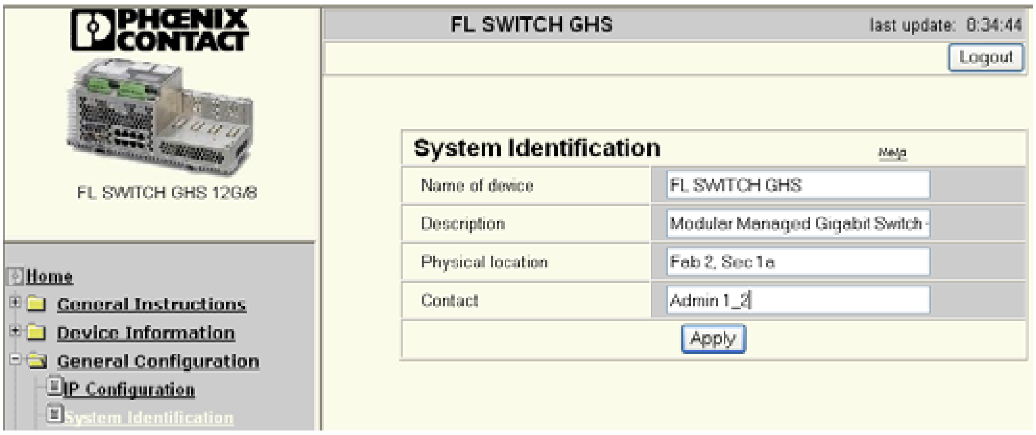
13 Diagnostics

13.1 Configuring system identification

This menu is used to display or modify user-specific device data, e.g., location, device name or function.

13.1.1 WBM

User-specific device data can be configured in the "General Configuration/System Identification" menu.



System Identification

Name of device	FL SWITCH GHS
Description	Modular Managed Gigabit Switch -
Physical location	Fab 2, Sec 1a
Contact	Admin 1_2

Figure 13-1 "System Identification" web page

13.1.2 SNMP

The settings can be found under OID 1.3.6.1.2.1.1 under the following path:

Full path: iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).system(1)

13.1.3 CLI

The settings can be found in the CLI under "hostname".

CLI user manual: Unknown source of cross-reference

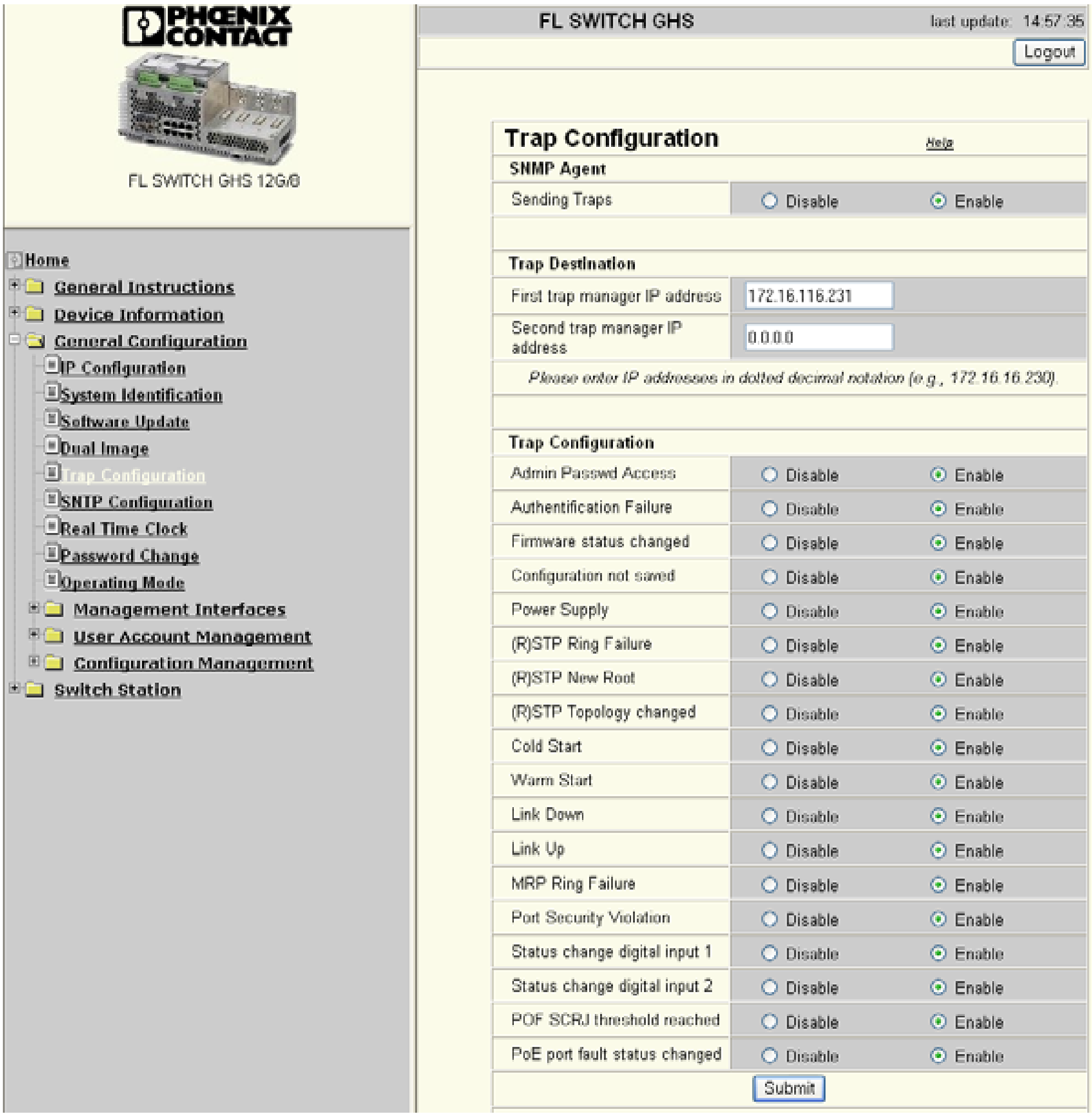
13.2 Configuring traps

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

With the GHS, you can configure the events that are to trigger the sending of a trap as well as the trap receivers.

13.2.1 WBM

The use of traps can be configured in the "General Configuration/Trap Configuration" menu.



Trap Configuration

SNMP Agent

Sending Traps	○ Disable	● Enable

Trap Destination

First trap manager IP address	172.16.116.231
Second trap manager IP address	0.0.0.0

Please enter IP addresses in dotted decimal notation (e.g., 172.16.16.230).

Trap Configuration

Admin Passwd Access	○ Disable	● Enable
Authentification Failure	○ Disable	● Enable
Firmware status changed	○ Disable	● Enable
Configuration not saved	○ Disable	● Enable
Power Supply	○ Disable	● Enable
(R)STP Ring Failure	○ Disable	● Enable
(R)STP New Root	○ Disable	● Enable
(R)STP Topology changed	○ Disable	● Enable
Cold Start	○ Disable	● Enable
Warm Start	○ Disable	● Enable
Link Down	○ Disable	● Enable
Link Up	○ Disable	● Enable
MRP Ring Failure	○ Disable	● Enable
Port Security Violation	○ Disable	● Enable
Status change digital input 1	○ Disable	● Enable
Status change digital input 2	○ Disable	● Enable
POF SCRJ threshold reached	○ Disable	● Enable
PoE port fault status changed	○ Disable	● Enable

Figure 13-2 "Trap Configuration" web page

13.2.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.3 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkTraps(3)

13.2.3 CLI

The settings can be found in the CLI under "configure/sntptrap".

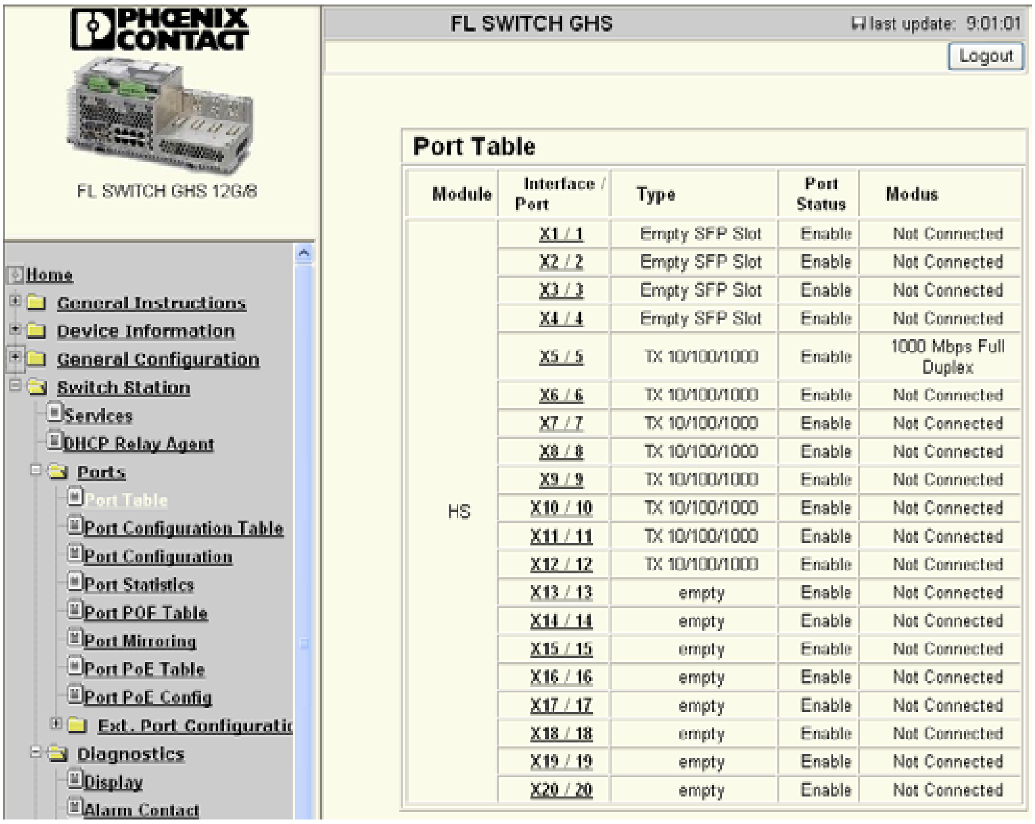
CLI user manual: Unknown source of cross-reference

13.3 Querying port states

This menu is used to call an overview of all available ports.

13.3.1 WBM

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



Port Table

Module	Interface / Port	Type	Port Status	Modus
HS	X1 / 1	Empty SFP Slot	Enable	Not Connected
	X2 / 2	Empty SFP Slot	Enable	Not Connected
	X3 / 3	Empty SFP Slot	Enable	Not Connected
	X4 / 4	Empty SFP Slot	Enable	Not Connected
	X5 / 5	TX 10/100/1000	Enable	1000 Mbps Full Duplex
	X6 / 6	TX 10/100/1000	Enable	Not Connected
	X7 / 7	TX 10/100/1000	Enable	Not Connected
	X8 / 8	TX 10/100/1000	Enable	Not Connected
	X9 / 9	TX 10/100/1000	Enable	Not Connected
	X10 / 10	TX 10/100/1000	Enable	Not Connected
	X11 / 11	TX 10/100/1000	Enable	Not Connected
	X12 / 12	TX 10/100/1000	Enable	Not Connected
	X13 / 13	empty	Enable	Not Connected
	X14 / 14	empty	Enable	Not Connected
	X15 / 15	empty	Enable	Not Connected
	X16 / 16	empty	Enable	Not Connected
	X17 / 17	empty	Enable	Not Connected
	X18 / 18	empty	Enable	Not Connected
	X19 / 19	empty	Enable	Not Connected
	X20 / 20	empty	Enable	Not Connected

Figure 13-3 "Port Table" web page

13.3.2 SNMP

The settings can be found under OID 1.3.6.1.2.1.17.4.4 under the following path:

Full path: iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).dot1dBridge(17).dot1dTp(4).dot1dTpPortTable(4)

13.3.3 CLI

The settings can be found in the CLI under "show/port-channel".

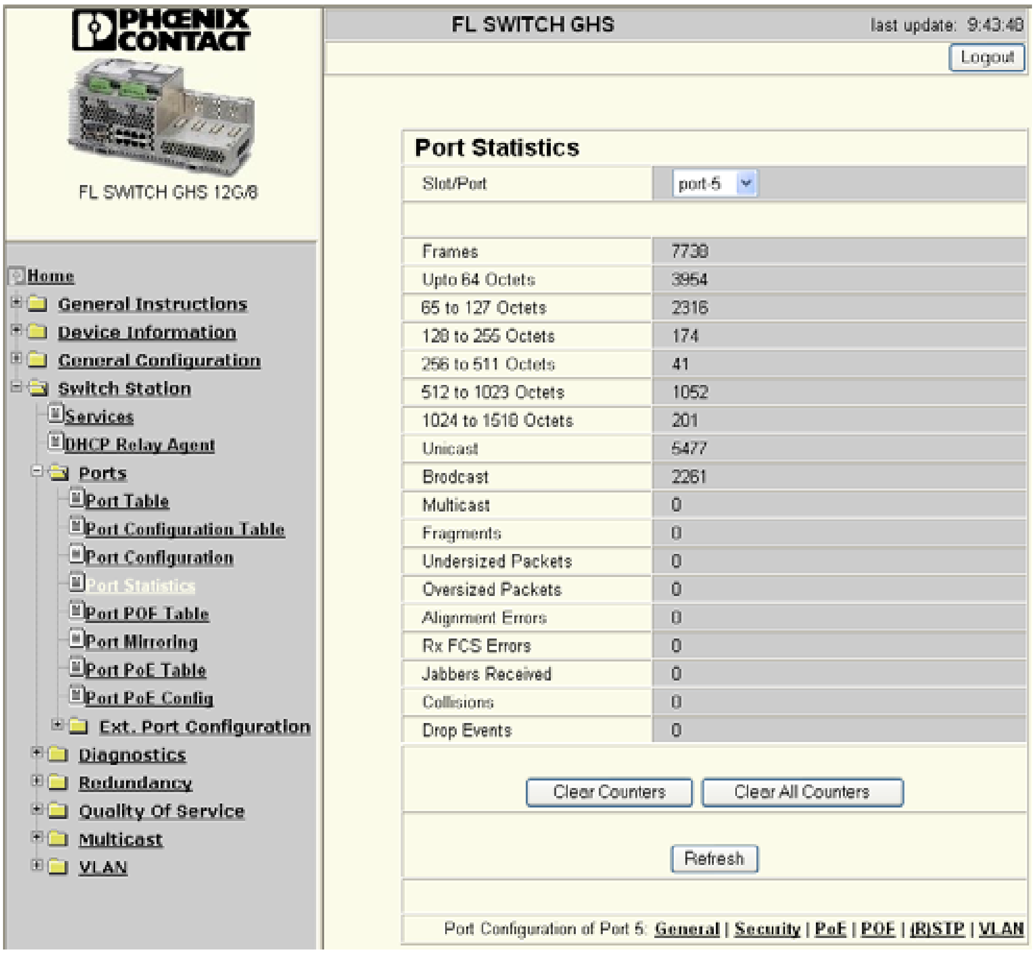
CLI user manual: Unknown source of cross-reference

13.4 Using port statistics

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

13.4.1 WBM

Port-specific data can be viewed or the counters cleared in the "Switch Station/Ports/Port Statistics" menu.



Port Statistics

Slot/Port	port-5
Frames	7738
Upto 64 Octets	3954
65 to 127 Octets	2316
128 to 255 Octets	174
256 to 511 Octets	41
512 to 1023 Octets	1052
1024 to 1518 Octets	201
Unicast	5477
Brodcast	2261
Multicast	0
Fragments	0
Undersized Packets	0
Oversized Packets	0
Alignment Errors	0
Rx FCS Errors	0
Jabbers Received	0
Collisions	0
Drop Events	0

Port Configuration of Port 5: General | Security | PoE | POF | (R)STP | VLAN

Figure 13-4 "Port Statistics" web page

13.4.2 SNMP

The settings can be found under OID 1.3.6.1.2.1.2.2.1 under the following path:

Full path: iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).interfaces(2).ifTable(2).ifEntry(1)

13.4.3 CLI

The settings can be found in the CLI under "show/port-channel".

CLI user manual: Unknown source of cross-reference

13.5 POF-SCRJ diagnostics

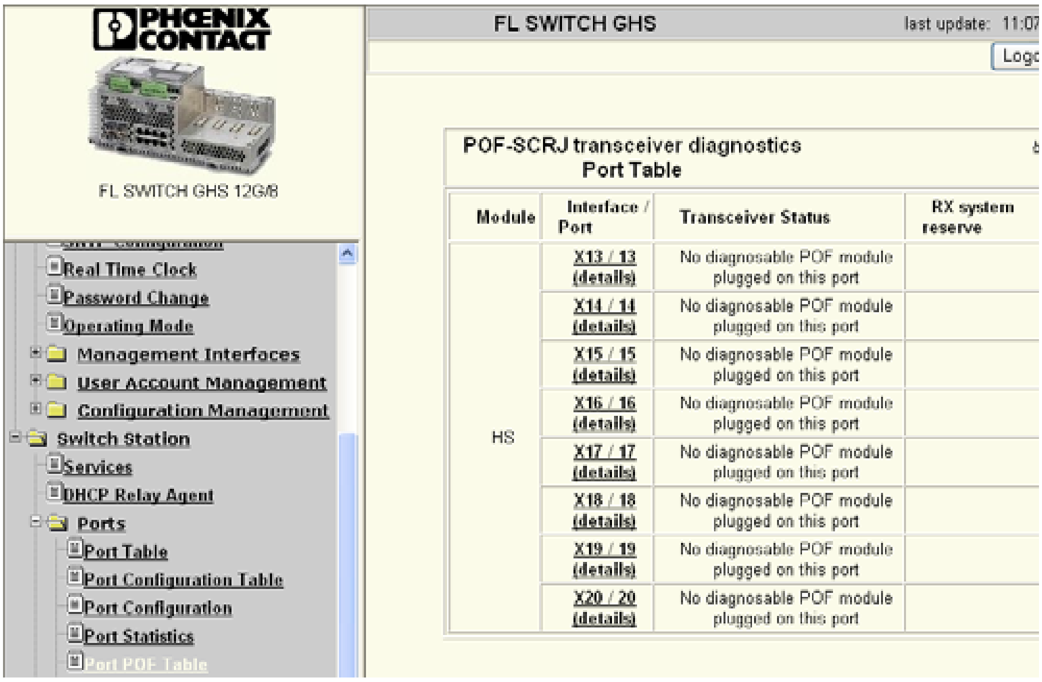
This view provides detailed statistical information about the volume of data for each individual port.

13.5.1 WBM

Available information about the POF-SCRJ interface modules is displayed in the "Switch Station/Ports/Port POF Table" menu.

The following states can be displayed under "Transceiver status":

- "System hardware does not support diagnosable POF modules" (this hardware does not support POF-SCRJ diagnostics)
- "No POF-SCRJ Interface modules present" (no POF-SCRJ module is plugged in)
- "POF-SCRJ Interface module is present and OK" (the system reserve is greater than 2 dB and is displayed under "RX system reserve")
- "POF-SCRJ Interface module is present, but the system reserve is low" (the system reserve is less than 2 dB, but greater than 0 dB)
- "POF-SCRJ Interface module is present, but the system reserve is exhausted" (no system reserve available - the received optical power is below the required minimum value)



POF-SCRJ transceiver diagnostics
Port Table

Module	Interface / Port	Transceiver Status	RX system reserve
HS	X13 / 13 (details)	No diagnosable POF module plugged on this port	
	X14 / 14 (details)	No diagnosable POF module plugged on this port	
	X15 / 15 (details)	No diagnosable POF module plugged on this port	
	X16 / 16 (details)	No diagnosable POF module plugged on this port	
	X17 / 17 (details)	No diagnosable POF module plugged on this port	
	X18 / 18 (details)	No diagnosable POF module plugged on this port	
	X19 / 19 (details)	No diagnosable POF module plugged on this port	
	X20 / 20 (details)	No diagnosable POF module plugged on this port	

Figure 13-5 "POF-SCRJ transceiver diagnostics Port Table" web page

13.5.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.4.2.4 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxc
FactoryLine(11).flWorkDevice(11).flWorkNet(4).flWorkNetPort(2).flWorkNetPortPofScrjIf
Table(4)

13.5.3 CLI

The settings can be found in the CLI under "show/port-channel".

CLI user manual: Unknown source of cross-reference

13.6 Configuring port mirroring

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

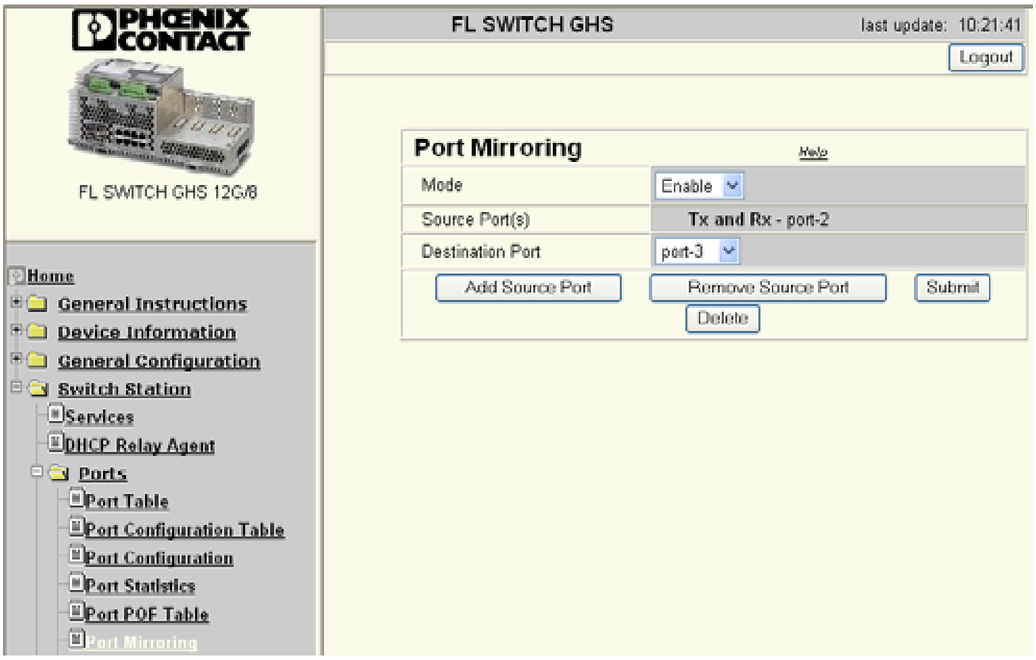
ℹ Trunks grouped to one port via link aggregation cannot be included in the mirroring either individually or as a complete trunk. This applies for use as the mirroring source or destination.

ℹ 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 to be sent directly to this port. In addition, it no longer forwards received packets to other switch ports.

The availability of the network-based user interfaces of the switch (WEB, SNMP, etc.) is no longer ensured via this port.

13.6.1 WBM

Port mirroring is configured in the "Switch Station/Ports/Port Mirroring" menu.



Port Mirroring

Mode	Enable
Source Port(s)	Tx and Rx - port-2
Destination Port	port-3

Figure 13-6 "Port Mirroring" web page

13.6.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.11.15.2 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flSwitch(15)flSwitchPortMirr

13.6.3 CLI

The settings can be found in the CLI under "configure/monitor".

CLI user manual: Unknown source of cross-reference

13.7 Power over Ethernet (PoE)

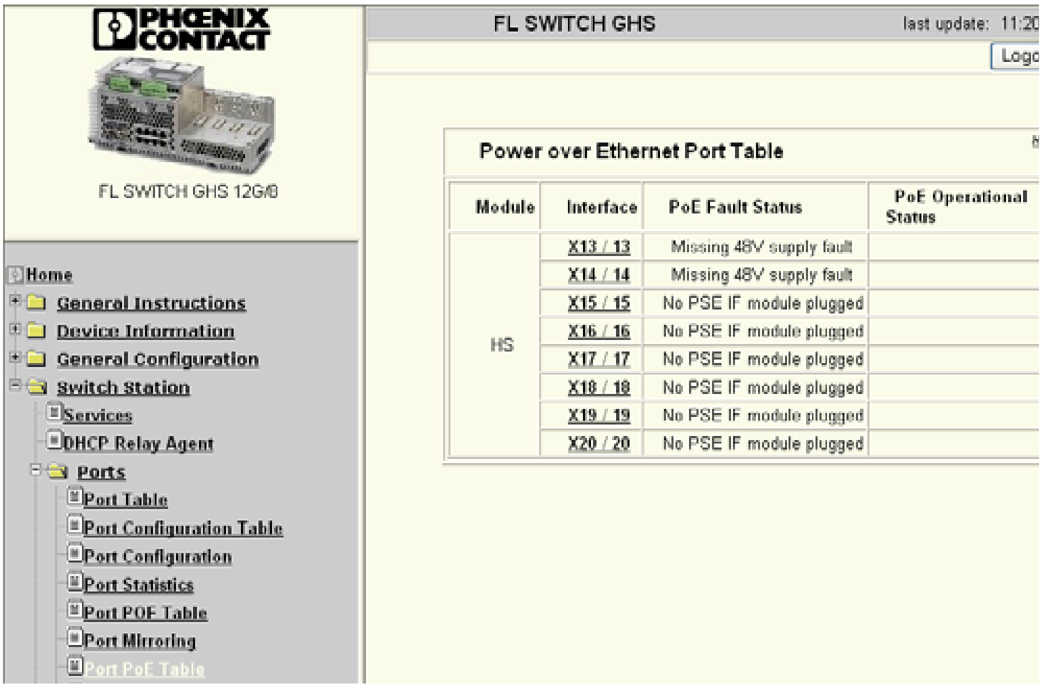
This view shows the PoE status of all ports.

13.7.1 WBM

The following states are supported in the "Switch Station/Ports/Port PoE Table" menu:

- No error
- Error in the external PoE supply voltage

- Temperature too high
- Current limitation activated
- Load disconnected
- The PoE controller does not respond, 48 V supply may be missing
- No PoE interface module inserted in this slot
- The switch does not support PoE interface modules
- No PoE devices connected to this port
- Port Power over Ethernet Configuration



Power over Ethernet Port Table

Module	Interface	PoE Fault Status	PoE Operational Status
HS	X13 / 13	Missing 48V supply fault	
	X14 / 14	Missing 48V supply fault	
	X15 / 15	No PSE IF module plugged	
	X16 / 16	No PSE IF module plugged	
	X17 / 17	No PSE IF module plugged	
	X18 / 18	No PSE IF module plugged	
	X19 / 19	No PSE IF module plugged	
	X20 / 20	No PSE IF module plugged	

Figure 13-7 "Power over Ethernet Port Table" web page

13.7.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.4.2.3 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkNet(4).flWorkNetPort(2).flWorkNetPortPoETable(3)

13.7.3 CLI

The settings can be found in the CLI under "show/poe".

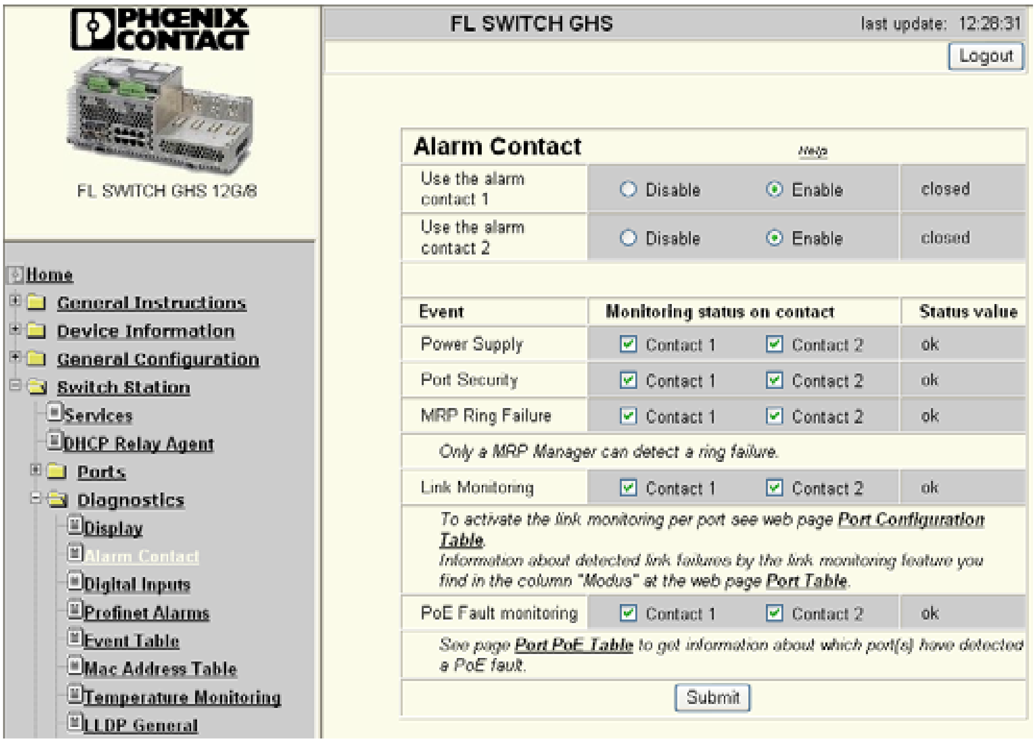
CLI user manual: Unknown source of cross-reference

13.8 Configuring alarm contacts

This menu is used to activate/deactivate events that are indicated via the alarm contacts.

13.8.1 WBM

The use of alarm contacts is configured in the "Switch Station/Diagnostics/Alarm Contact" menu.



FL SWITCH GHS last update: 12:28:31

Alarm Contact

Use the alarm contact 1	○ Disable	● Enable	closed
Use the alarm contact 2	○ Disable	● Enable	closed

Event	Monitoring status on contact		Status value
Power Supply	☑ Contact 1	☑ Contact 2	ok
Port Security	☑ Contact 1	☑ Contact 2	ok
MRP Ring Failure	☑ Contact 1	☑ Contact 2	ok
Only a MRP Manager can detect a ring failure.			
Link Monitoring	☑ Contact 1	☑ Contact 2	ok
To activate the link monitoring per port see web page Port Configuration Table. *Information about detected link failures by the link monitoring feature you find in the column "Modus" at the web page Port Table.*			
PoE Fault monitoring	☑ Contact 1	☑ Contact 2	ok
See page Port PoE Table to get information about which port(s) have detected a PoE fault.			

Figure 13-8 "Alarm Contact" web page

13.8.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.11.2.7 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlAlarmContact(7)

13.8.3 CLI

The settings can be found in the CLI under "configure/monitor".

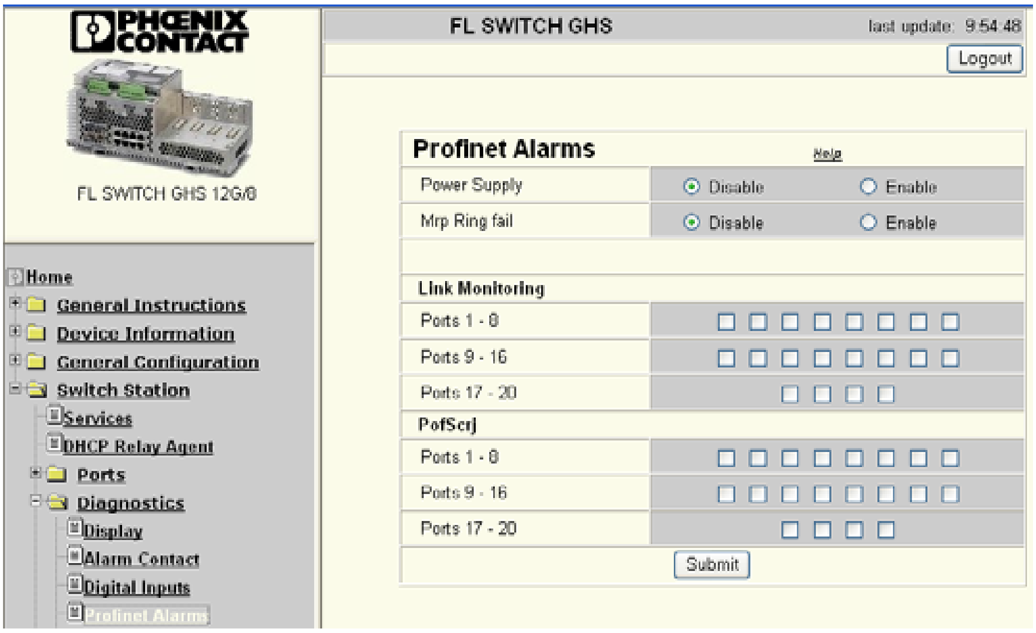
CLI user manual: Unknown source of cross-reference

13.9 Configuring PROFINET alarms

This menu is used to activate/deactivate the events that trigger a PROFINET alarm and to evaluate the ports where these events occur.

13.9.1 WBM

The events and ports are configured in the "Switch Station/Diagnostics/Profinet Alarms" menu.



Profinet Alarms

Power Supply	● Disable	○ Enable
Mrp Ring fail	● Disable	○ Enable

Link Monitoring

Ports 1 - 8	□ □ □ □ □ □ □ □
Ports 9 - 16	□ □ □ □ □ □ □ □
Ports 17 - 20	□ □ □ □

PofScrj

Ports 1 - 8	□ □ □ □ □ □ □ □
Ports 9 - 16	□ □ □ □ □ □ □ □
Ports 17 - 20	□ □ □ □

Figure 13-9 "Profinet Alarms" web page

13.9.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.11.2.9 under the following path:

Full path: iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlProfinet(9)

13.9.3 CLI

The settings can be found in the CLI under "configure/monitor".

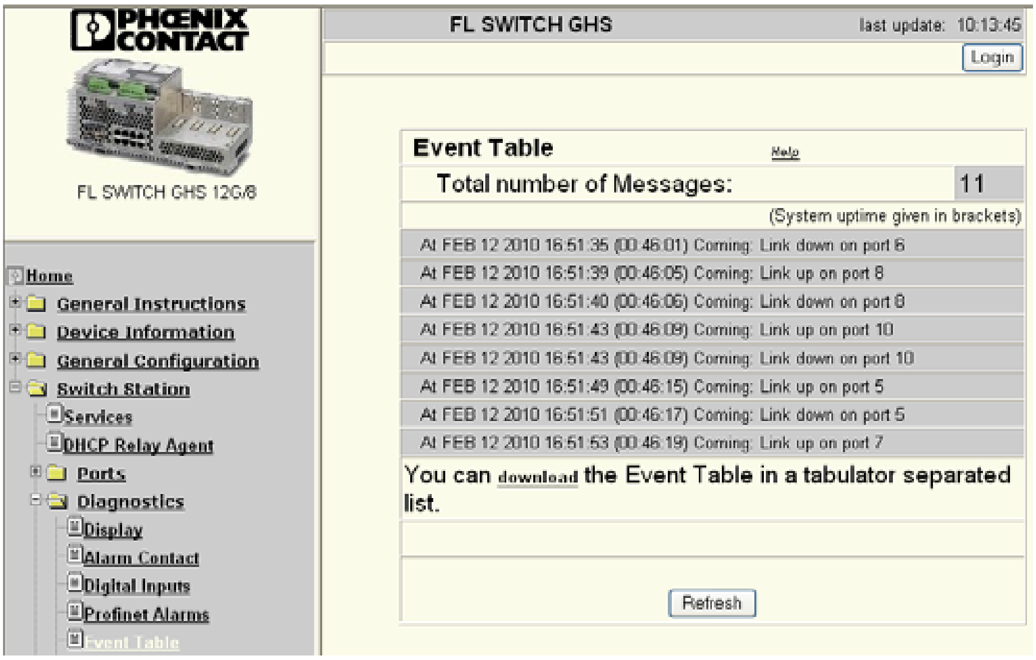
CLI user manual: Unknown source of cross-reference

13.10 Calling the event table

This web page displays events in table format, including the system time.

13.10.1 WBM

The events are displayed in the "Switch Station/Diagnostics/Event Table" menu.



Event Table

Total number of Messages: 11

(System uptime given in brackets)

```
At FEB 12 2010 16:51:35 (00:46:01) Coming: Link down on port 6
At FEB 12 2010 16:51:39 (00:46:05) Coming: Link up on port 8
At FEB 12 2010 16:51:40 (00:46:06) Coming: Link down on port 8
At FEB 12 2010 16:51:43 (00:46:09) Coming: Link up on port 10
At FEB 12 2010 16:51:43 (00:46:09) Coming: Link down on port 10
At FEB 12 2010 16:51:49 (00:46:15) Coming: Link up on port 5
At FEB 12 2010 16:51:51 (00:46:17) Coming: Link down on port 5
At FEB 12 2010 16:51:53 (00:46:19) Coming: Link up on port 7
```

You can download the Event Table in a tabulator separated list.

Figure 13-10 "Event Table" web page

13.10.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.11.1.14.1 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWInfo(1).flWorkFWInfoEvent(14).flWorkFWInfoEventTable(1)

13.10.3 CLI

The settings can be found in the CLI under "show/eventlog".

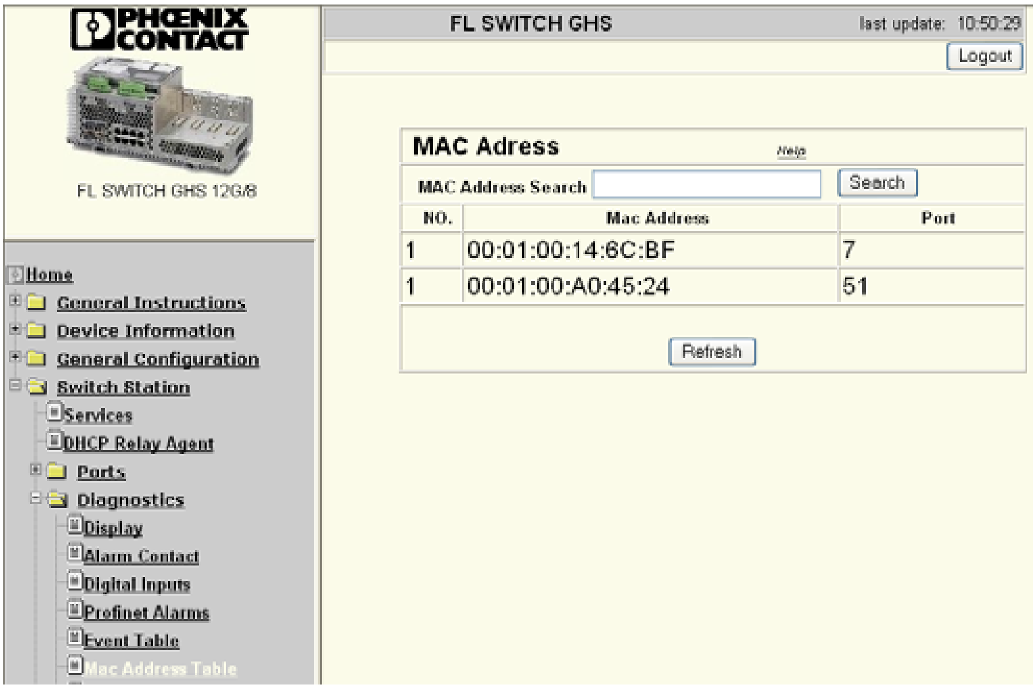
CLI user manual: Unknown source of cross-reference

13.11 Displaying the MAC address table

This page displays the MAC addresses of all devices connected to the device according to their port.

13.11.1 WBM

The MAC addresses of the devices are displayed in the "Switch Station/Diagnostics/MAC Address Table" menu.



last update: 10:50:29

MAC Adress

MAC Address Search:

NO.	Mac Address	Port
1	00:01:00:14:6C:BF	7
1	00:01:00:A0:45:24	51

Figure 13-11 "MAC Address" web page

13.11.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.11.2.8.2.2 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxc FactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrl(2).flWorkFWCtrlSecurity(8).flWorkFWCtrlSecurityPort(2).flWorkFWCtrlSecurityPortMacTable(2)

13.11.3 CLI

The settings can be found in the CLI under "show/mac-address-table".

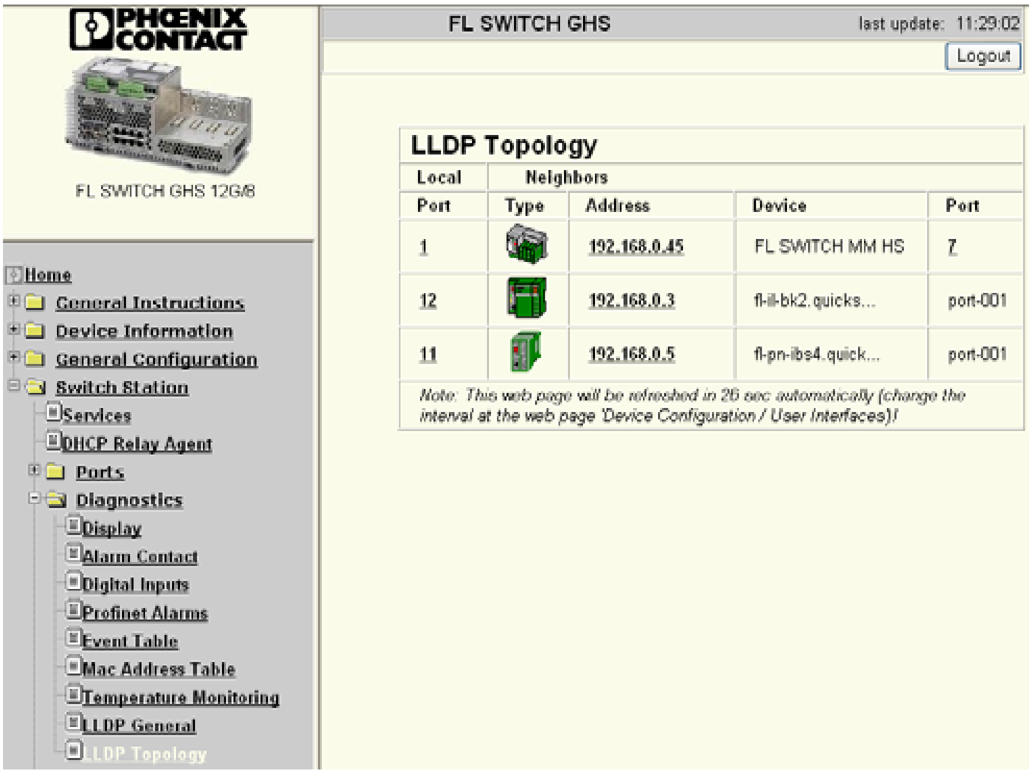
CLI user manual: Unknown source of cross-reference

13.12 LLDP topology

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

13.12.1 WBM

The neighbor information is displayed in the "Switch Station/Diagnostics/LLDP Topology" menu.



LLDP Topology

Local	Neighbors			
Port	Type	Address	Device	Port
1		192.168.0.45	FL SWITCH MM HS	7
12		192.168.0.3	fl-il-bk2.quicks...	port-001
11		192.168.0.5	fl-pn-ibs4.quick...	port-001

Note: This web page will be refreshed in 26 sec automatically (change the interval at the web page 'Device Configuration / User Interfaces)!

Figure 13-12 "LLDP Topology" web page

13.12.2 SNMP

The settings can be found under OID 1.0.8802.1.1.2 under the following path:

Full path: iso(1).std(0).iso8802(8802).ieee802dot1(1).ieee802dot1mibs(1).lldpMIB(2)

13.12.3 CLI

The settings can be found in the CLI under "show/temperature".

CLI user manual: Unknown source of cross-reference

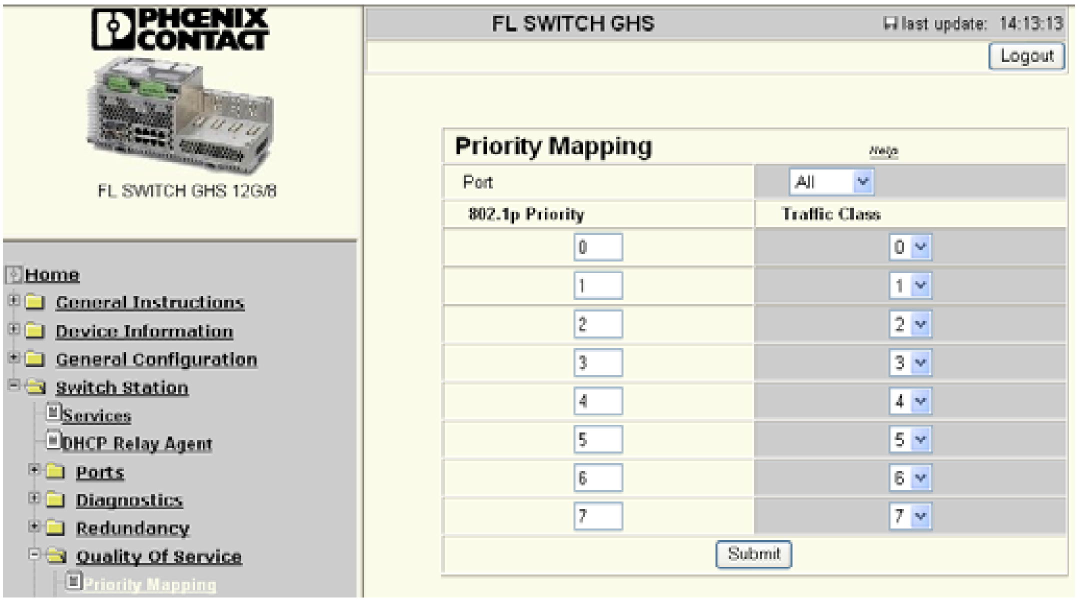
14 Quality of Service

14.1 Configuring priority mapping

This menu is used to assign the value of 802.1p priority information of a data packet to a traffic class according to the specific port.

14.1.1 WBM

The desired assignment can be configured in the "Switch Station/Quality of Service/Priority Mapping" menu.



Priority Mapping

Port: All

802.1p Priority	Traffic Class
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Figure 14-1 "Priority Mapping" web page

14.1.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.15.6.4 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flSwitch(15).flSwitchRateCtrl(6).flSwitchDot3FlowControlMode(4)

14.1.3 CLI

The settings can be found in the CLI under "configure/classofservice/dot1p priority mapping".

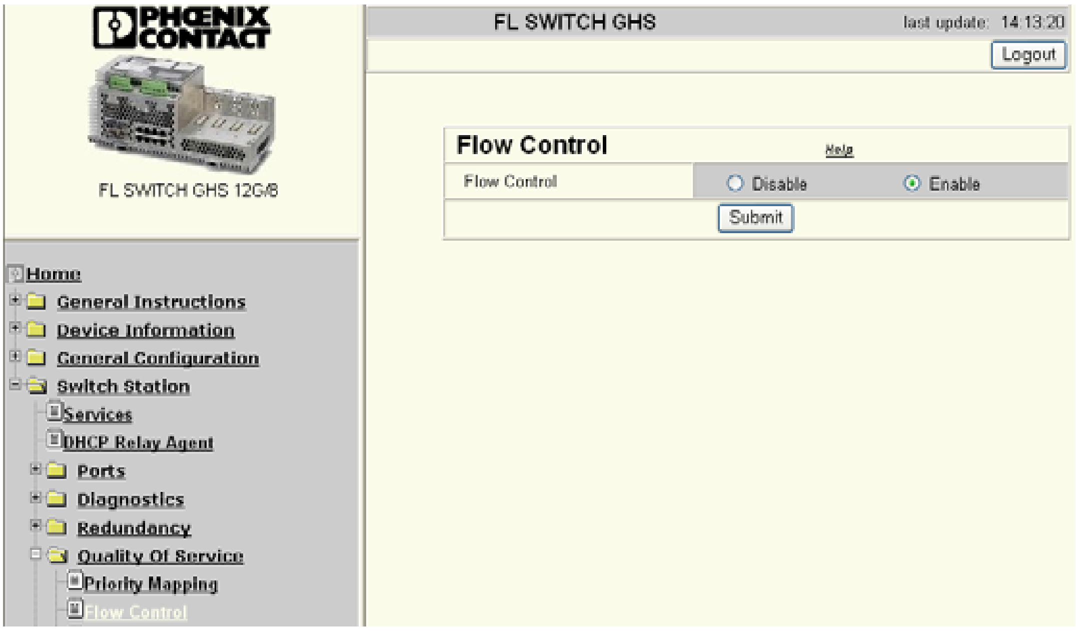
CLI user manual: Unknown source of cross-reference

14.2 Activating/deactivating flow control

This menu is used to activate/deactivate flow control.

14.2.1 WBM

Flow control can be activated/deactivated in the "Switch Station/Quality of Service/Flow Control" menu.



Flow Control

Flow Control ○ Disable ● Enable

Figure 14-2 "Flow Control" web page

14.2.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.15.6.4 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flSwitch(15).flSwitchRateCtrl(6).flSwitchDot3FlowControlMode(4)

14.2.3 CLI

The settings can be found in the CLI under "configure/storm-control flowcontrol".

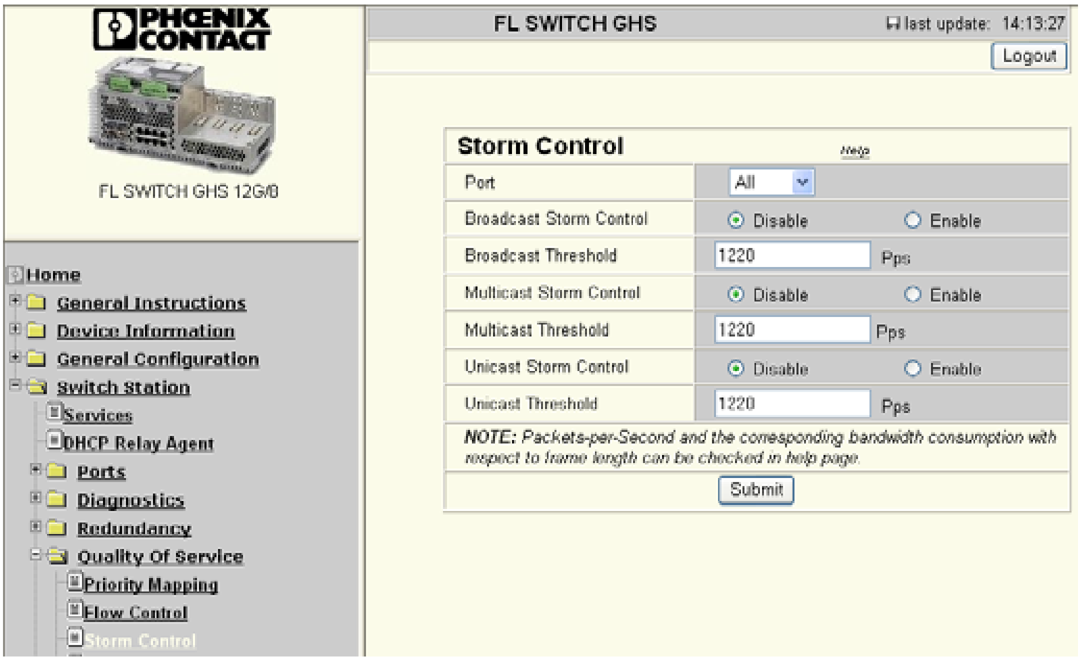
CLI user manual: Unknown source of cross-reference

14.3 Configuring storm control

This menu is used to specify the threshold values of the relevant storm control function according to the specific port and to enable/disable the relevant storm control function.

14.3.1 WBM

The desired function can be configured in the "Switch Station/Quality of Service/Storm Control" menu.



Storm Control

Port	All	
Broadcast Storm Control	● Disable	○ Enable
Broadcast Threshold	1220	Pps
Multicast Storm Control	● Disable	○ Enable
Multicast Threshold	1220	Pps
Unicast Storm Control	● Disable	○ Enable
Unicast Threshold	1220	Pps

NOTE: Packets-per-Second and the corresponding bandwidth consumption with respect to frame length can be checked in help page.

Figure 14-3 "Storm Control" web page

14.3.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.15.6 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flSwitch(15).flSwitchRateCtrl(6)

14.3.3 CLI

The settings can be found in the CLI under "configure/storm-control flowcontrol".

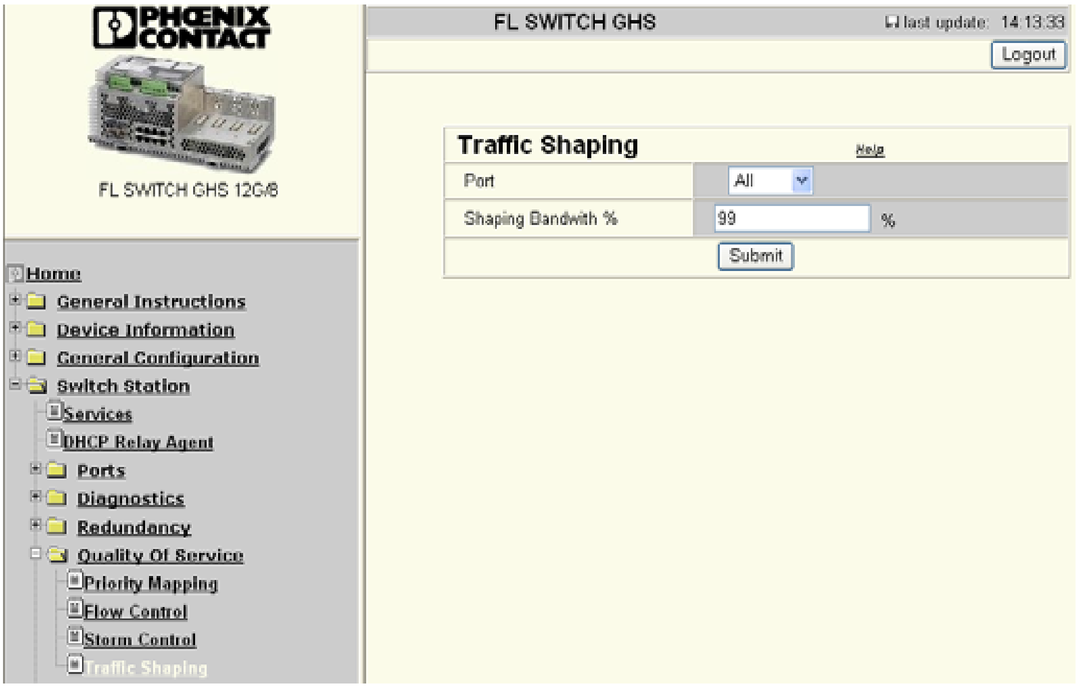
CLI user manual: Unknown source of cross-reference

14.4 Configuring traffic shaping

This menu is used to specify the bandwidth value as a percentage according to the specific port.

14.4.1 WBM

The desired assignment can be configured in the "Switch Station/Quality of Service/Traffic Shaping" menu.



Port: All

Shaping Bandwith %: 99 %

Figure 14-4 "Traffic Shaping" web page

14.4.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.15.7 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flSwitch(15).flSwitchTrafficShaping(7)

14.4.3 CLI

The settings can be found in the CLI under "configure/classofservice/dot1p priority mapping".

CLI user manual: Unknown source of cross-reference

15 PROFIenergy *

15.1 15.1 Principle of PROFIenergy

The energy consumption of a production plant depends on the actual time of day and therefore fluctuates greatly. While energy consumption during production times is 100% or more, there is only very low energy demand during break periods or on non-operational days (see Figure 15-1). However, it is not possible to shut down systems centrally during each break period. This is where PROFIenergy comes in. At the start of the break, a controller sends a "Start_Pause" command defined in the PROFINET standard and all the connected devices that can execute this command switch to energy-saving mode. The display on the Gigabit Modular Switch is dimmed, LEDs of unused ports are switched off, and further port-specific energy-saving modes are activated. The Gigabit ports are thus taken down to 100 Mbps or connected PoE devices are switched off completely. Despite energy-saving mode being activated, communication within the network is still ensured.

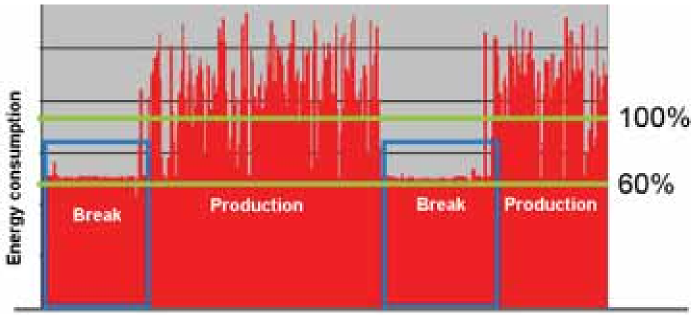


Figure 15-1 Graphical representation of energy consumption

At the end of a break the affected devices exit energy-saving mode and return to the operating state (see Figure 15-2).

The conservation of resources and energy efficiency are important topics in modern society and industry. Therefore despite its high level of performance, the switch is extremely energy efficient. In order to conserve additional resources, the switch is prepared for operation with the PROFIenergy profile. Performance and efficiency are now combined.

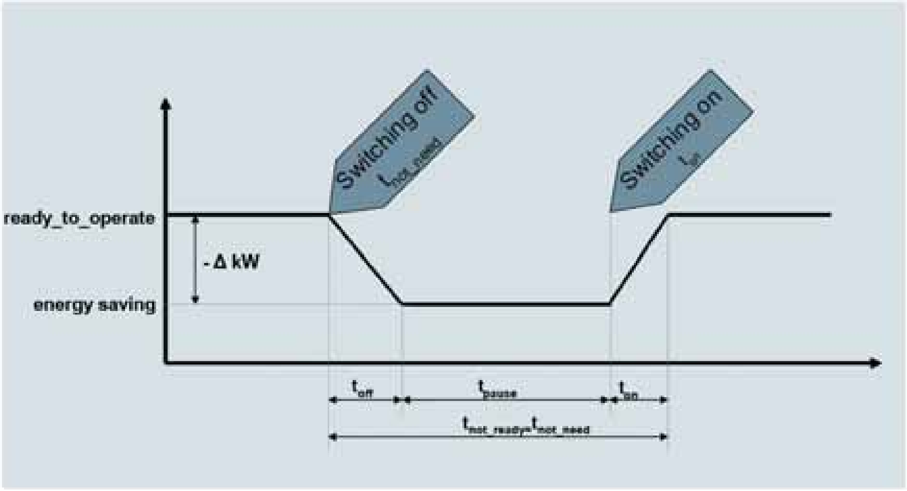
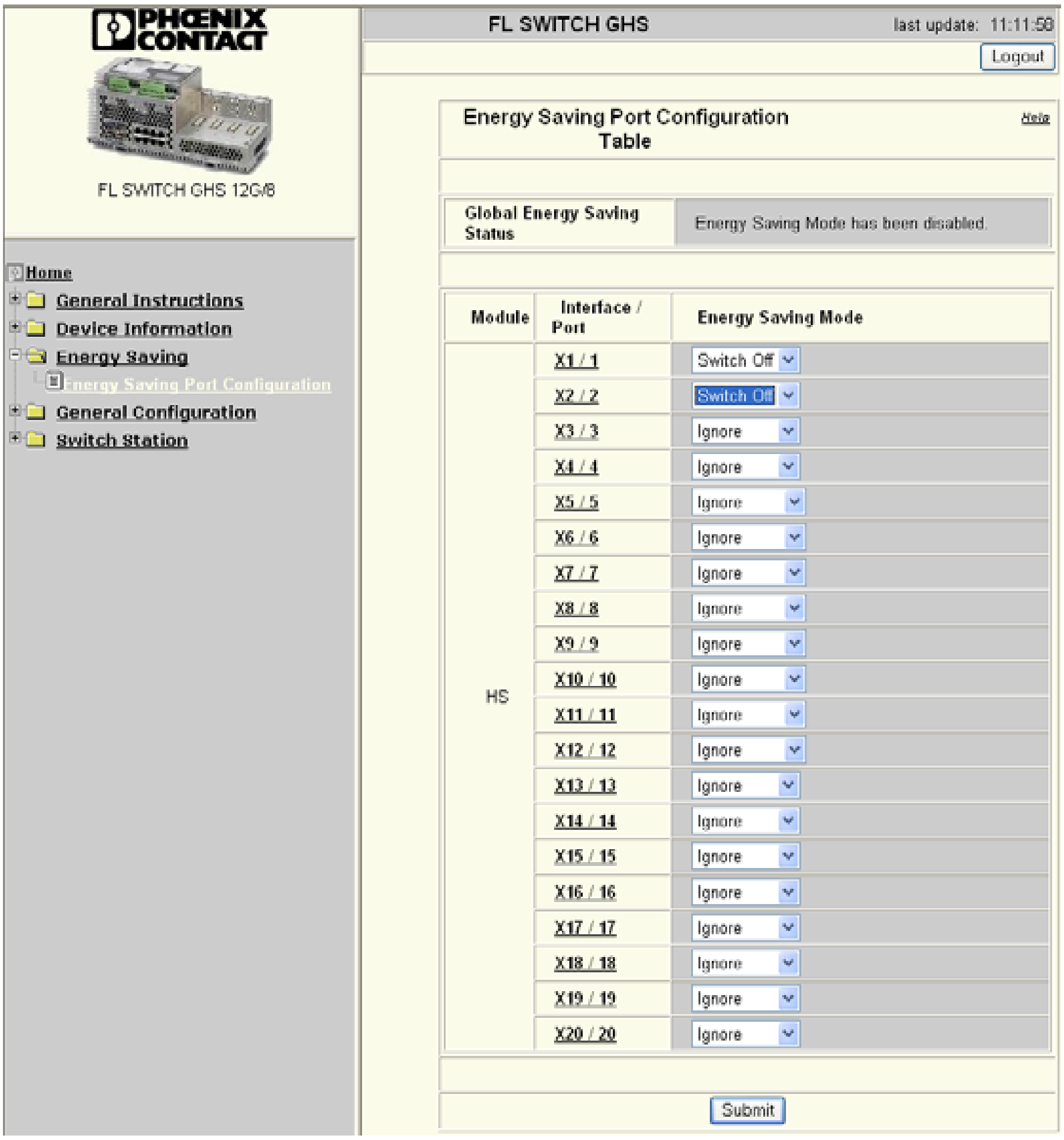


Figure 15-2 Time curve for the switch on/switch off phases

In order to connect company networks to production networks and meet the requirements of both, industrial switches must be of the highest performance class. These requirements demand maximum performance from the technology used, which does not appear compatible with the features of an energy-saving device that conserves resources. With regard to energy saving, the device combines "green IT" aspects with industrial requirements, such as the PROFIenergy concept. This device is therefore able to meet the requirement for the sustainable conservation of resources.

15.2 Configuring Energy Saving

This menu is used to configure the influence of PROFIenergy for the specific ports.



FL SWITCH GHS last update: 11:11:58

Energy Saving Port Configuration Table

Global Energy Saving Status: Energy Saving Mode has been disabled.

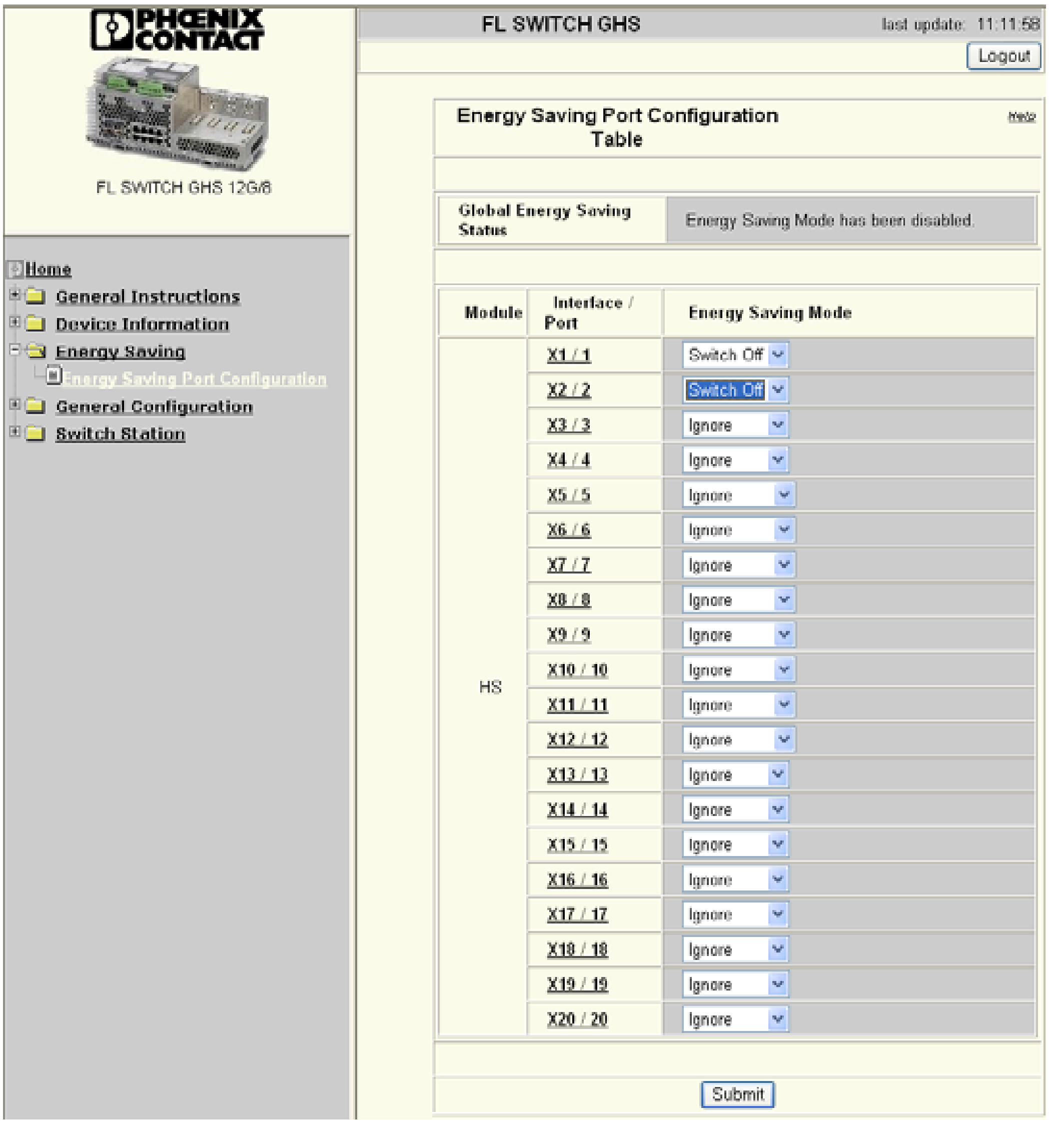
Module	Interface / Port	Energy Saving Mode
HS	X1 / 1	Switch Off
	X2 / 2	Switch Off
	X3 / 3	Ignore
	X4 / 4	Ignore
	X5 / 5	Ignore
	X6 / 6	Ignore
	X7 / 7	Ignore
	X8 / 8	Ignore
	X9 / 9	Ignore
	X10 / 10	Ignore
	X11 / 11	Ignore
	X12 / 12	Ignore
	X13 / 13	Ignore
	X14 / 14	Ignore
	X15 / 15	Ignore
	X16 / 16	Ignore
	X17 / 17	Ignore
	X18 / 18	Ignore
	X19 / 19	Ignore
	X20 / 20	Ignore

Figure 15-3 Configuring Energy Saving

* The "Energy Saving" function is available in firmware Version >= 1.50.

15.2.1 WBM

The desired assignment can be configured in the "Energy Saving" menu.



FL SWITCH GHS last update: 11:11:58

Energy Saving Port Configuration Table

Global Energy Saving Status	Energy Saving Mode has been disabled.

Module	Interface / Port	Energy Saving Mode
HS	X1 / 1	Switch Off
	X2 / 2	Switch Off
	X3 / 3	Ignore
	X4 / 4	Ignore
	X5 / 5	Ignore
	X6 / 6	Ignore
	X7 / 7	Ignore
	X8 / 8	Ignore
	X9 / 9	Ignore
	X10 / 10	Ignore
	X11 / 11	Ignore
	X12 / 12	Ignore
	X13 / 13	Ignore
	X14 / 14	Ignore
	X15 / 15	Ignore
	X16 / 16	Ignore
	X17 / 17	Ignore
	X18 / 18	Ignore
	X19 / 19	Ignore
	X20 / 20	Ignore

Figure 15-4 "Energy Saving Port Configuration" web page

"Switch Off" option: In energy-saving mode, the port and the PoE supply, if applicable, are switched off.

"Ignore" option: The port is not influenced by energy-saving mode.

15.2.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.11.2.17.1 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkFirmware(11).flWorkFWCtrlEnergy

15.2.3 CLI

The settings can be found in the CLI under "configure/interface x/x".

16 DHCP relay agent

16.1 Configuring the DHCP relay agent

The DHCP relay agent offers two functions:

- Local DHCP requests (e.g., DHCP requests of a termination device that wishes to obtain an IP address) can be forwarded to a DHCP server located in another IP subnetwork. This means that it is no longer necessary to maintain a separate DHCP server in each IP subnetwork.
- Topology information about the location of the termination device that wishes to obtain an IP address can be forwarded to the DHCP server using DHCP option 82, which is always active. DHCP option 82 is used by the DHCP server when assigning addresses to identify the requesting termination device via the corresponding physical switch port. In the event of device replacement, DHCP option 82 enables the new device to be assigned the same IP address as the old device due to the physical position in the network.

Sequence:

Every time the switch receives a DHCP discover/request that has been sent by a termination device, the switch extends the "DHCP option 82" field and forwards the data packet to the specific DHCP server. The desired DHCP server should be configured in WBM on the "DHCP Relay Agent" page.

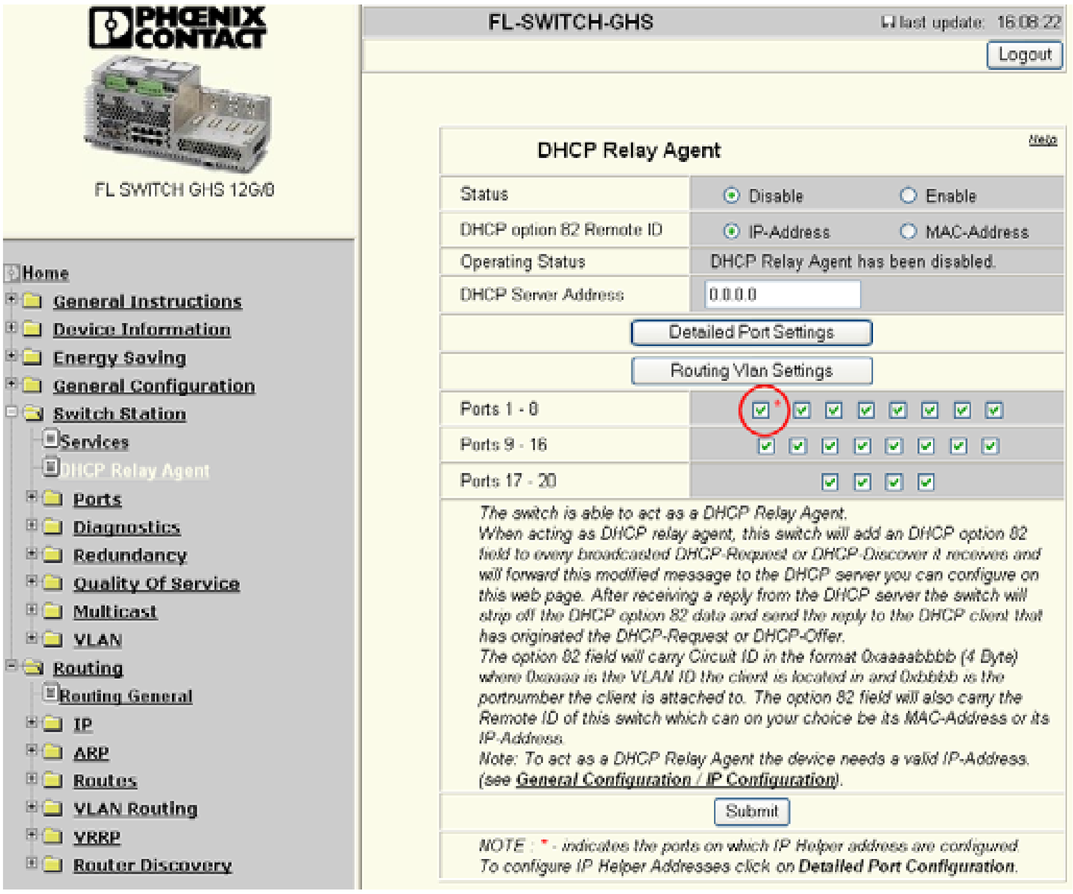
When routing is activated globally, more than one DHCP server address can be configured per port for the DHCP relay agent. These additional configurable IP addresses are known as IP helper addresses and can be configured for each port. In routing mode, links are available for the IP helper configuration.

The DHCP server can generate a response using option 82 information and can send this to the relay agent. The switch then removes the DHCP option 82 data from the DHCP server response and forwards the DHCP response to the termination device that triggered the request.

Configuration of IP helper addresses

To configure IP helper addresses, click on "Detailed Port Settings" and then on "Helper-IP Address". Following configuration, the "*" (asterisk) symbol next to a port checkbox indicates that IP helper addresses have been configured for this port.

.



DHCP Relay Agent

Status	● Disable	○ Enable
DHCP option 82 Remote ID	● IP-Address	○ MAC-Address
Operating Status	DHCP Relay Agent has been disabled.	
DHCP Server Address	0.0.0.0	
Ports 1 - 8	☑ * ☑ ☑ ☑ ☑ ☑ ☑ ☑	
Ports 9 - 16	☑ ☑ ☑ ☑ ☑ ☑ ☑ ☑	
Ports 17 - 20	☑ ☑ ☑ ☑	

The switch is able to act as a DHCP Relay Agent.
When acting as DHCP relay agent, this switch will add an DHCP option 82 field to every broadcasted DHCP-Request or DHCP-Discover it receives and will forward this modified message to the DHCP server you can configure on this web page. After receiving a reply from the DHCP server the switch will strip off the DHCP option 82 data and send the reply to the DHCP client that has originated the DHCP-Request or DHCP-Offer.
The option 82 field will carry Circuit ID in the format 0xaaaabbbb (4 Byte) where 0xaaaa is the VLAN ID the client is located in and 0xbbbb is the portnumber the client is attached to. The option 82 field will also carry the Remote ID of this switch which can on your choice be its MAC-Address or its IP-Address.
Note: To act as a DHCP Relay Agent the device needs a valid IP-Address.
(see General Configuration / IP Configuration).

*NOTE : * - indicates the ports on which IP Helper address are configured.*
To configure IP Helper Addresses click on **Detailed Port Configuration.**

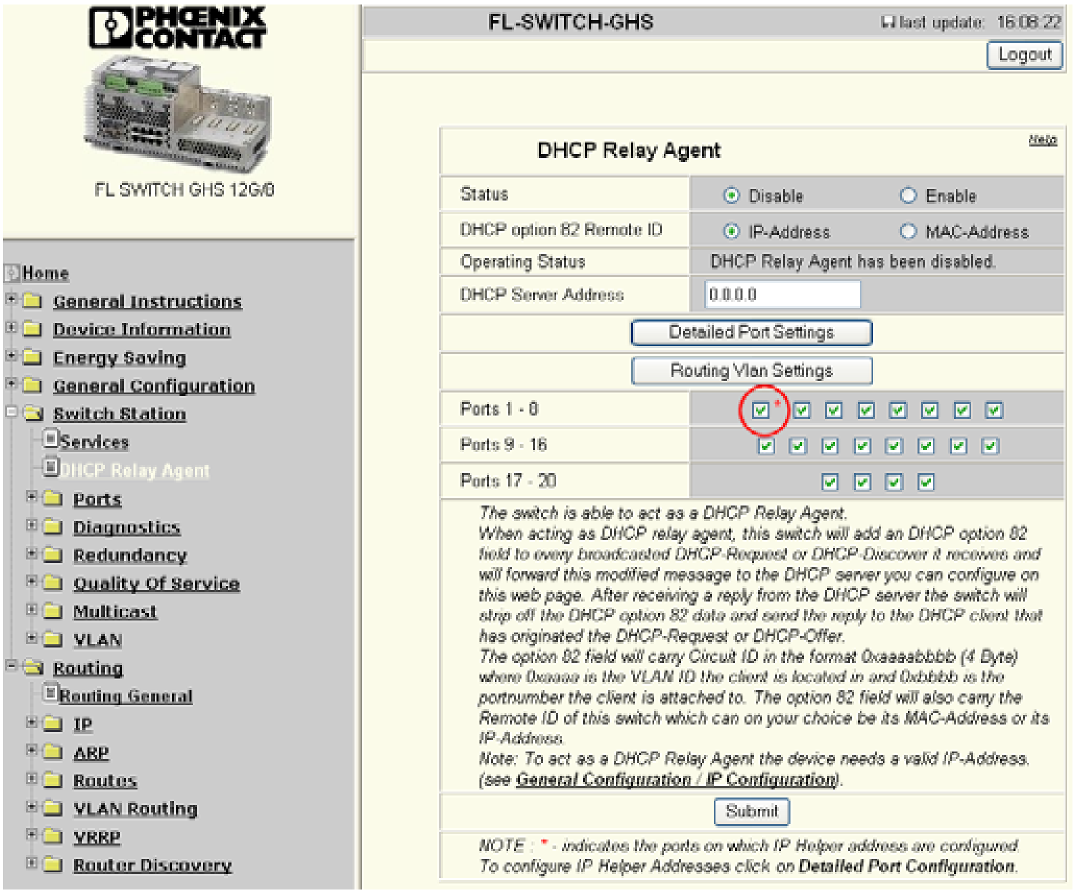
Figure 16-1 "DHCP Relay Agent" web page in routing mode with configured helper addresses

Information in the DHCP option 82 field:

The switch extends the VLAN ID in the DHCP option 82 field for the VLAN to which the termination device is assigned and the switch port to which the termination device is connected. In addition, the switch enters its own DHCP option 82 remote ID in the field. The DHCP option 82 remote ID can be configured by the user and contains the IP or MAC address of the switch.

16.1.1 WBM

The desired assignment can be configured in the "Switch Station/DHCP Relay Agent" menu.



DHCP Relay Agent

Status	● Disable	○ Enable
DHCP option 82 Remote ID	● IP-Address	○ MAC-Address
Operating Status	DHCP Relay Agent has been disabled.	
DHCP Server Address	0.0.0.0	

Detailed Port Settings

Routing Vlan Settings

Ports 1 - 8	☑ * ☑ ☑ ☑ ☑ ☑ ☑ ☑
Ports 9 - 16	☑ ☑ ☑ ☑ ☑ ☑ ☑ ☑
Ports 17 - 20	☑ ☑ ☑ ☑

The switch is able to act as a DHCP Relay Agent. When acting as DHCP relay agent, this switch will add an DHCP option 82 field to every broadcasted DHCP-Request or DHCP-Discover it receives and will forward this modified message to the DHCP server you can configure on this web page. After receiving a reply from the DHCP server the switch will strip off the DHCP option 82 data and send the reply to the DHCP client that has originated the DHCP-Request or DHCP-Offer. The option 82 field will carry Circuit ID in the format 0xaaaabbbb (4 Byte) where 0xaaaa is the VLAN ID the client is located in and 0xbbbb is the portnumber the client is attached to. The option 82 field will also carry the Remote ID of this switch which can on your choice be its MAC-Address or its IP-Address. Note: To act as a DHCP Relay Agent the device needs a valid IP-Address. (see General Configuration / IP Configuration).

Submit

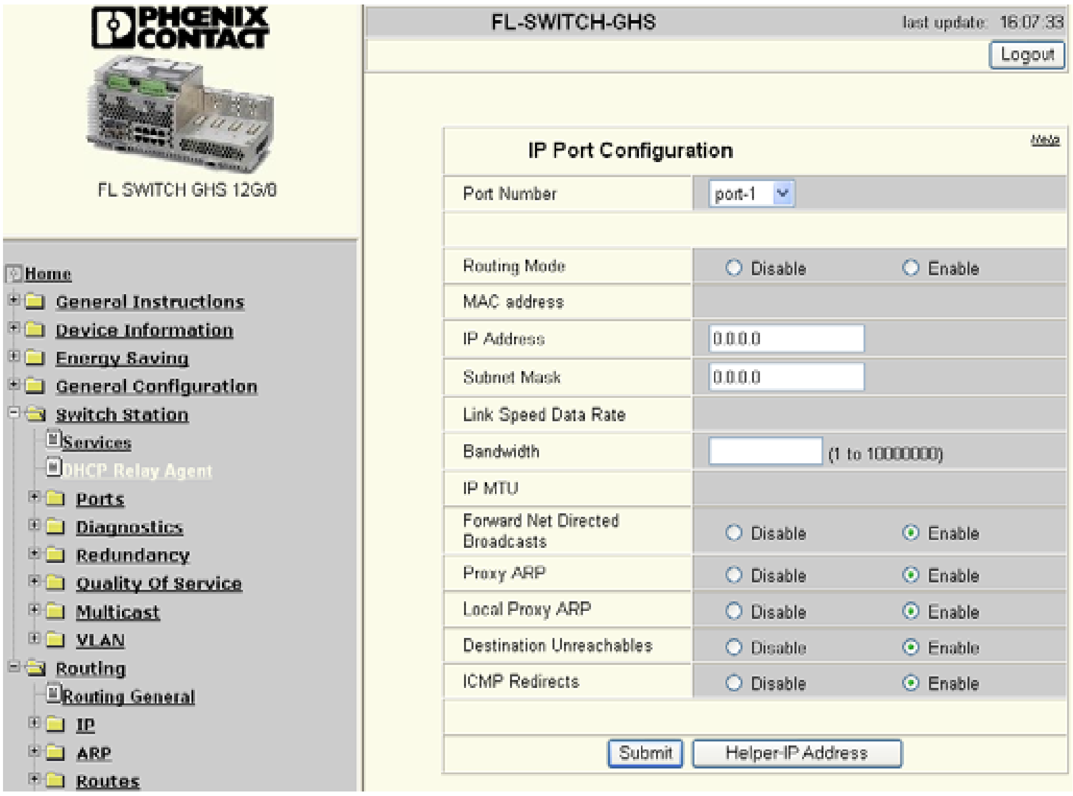
*NOTE : * - indicates the ports on which IP Helper address are configured To configure IP Helper Addresses click on **Detailed Port Configuration**.*

Figure 16-2 "DHCP Relay Agent" web page in router mode

To configure IP helper addresses, click on "Detailed Port Settings" and then on "Helper-IP Address". Following configuration, the "*" (asterisk) symbol next to a port checkbox indicates that IP helper addresses have been configured for this port.

Routing VLAN settings

A routing VLAN becomes a virtual port, which is not listed in the checkbox list of physical ports. For a routing VLAN, the DHCP server address can only be configured using IP helper addresses.

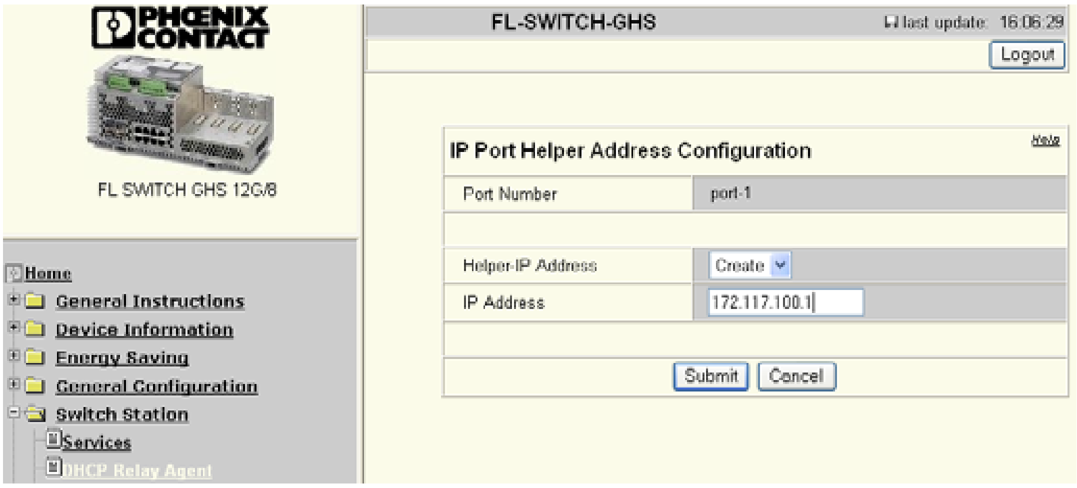


FL-SWITCH-GHS last update: 16:07:33

IP Port Configuration

Port Number	port-1	
Routing Mode	○ Disable	○ Enable
MAC address		
IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Link Speed Data Rate		
Bandwidth	(1 to 10000000)	
IP MTU		
Forward Net Directed Broadcasts	○ Disable	● Enable
Proxy ARP	○ Disable	● Enable
Local Proxy ARP	○ Disable	● Enable
Destination Unreachables	○ Disable	● Enable
ICMP Redirects	○ Disable	● Enable

Figure 16-3 "IP Port Configuration" web page



FL-SWITCH-GHS last update: 16:06:29

IP Port Helper Address Configuration

Port Number	port-1
Helper-IP Address	Create
IP Address	172.117.100.1

Figure 16-4 "IP Port Helper Address Configuration" web page

16.1.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.15.5 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flSwitch(15).flSwitchRelayAgentDhcp(5)

16.1.3 CLI

The settings can be found in the CLI under "ip/dhcp/relay-agent".

CLI user manual: "Config Commands for POE and DHCP Relay Agent in Interface Config Mode" on page 6-28.

17 Routing

A license is required in order to use the routing functions. This license is located on an SD card, which can be ordered using order designation/Order No. FL SD FLASH/L3/MRM, 2700607 To activate and use the routing functions, make sure that:

1. Firmware 2.0 or later is installed on your device
2. You have a valid FL SD FLASH/L3/MRM license
3. You are using one of the following devices: FL SWITCH GHS 4G/12-L3 or FL SWITCH GHS 12G/8-L3

17.1 Inserting the SD card

Insert the SD card into the card slot according to Figure 17-1.

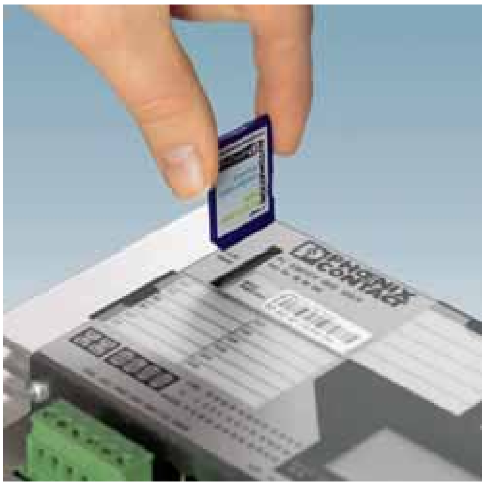


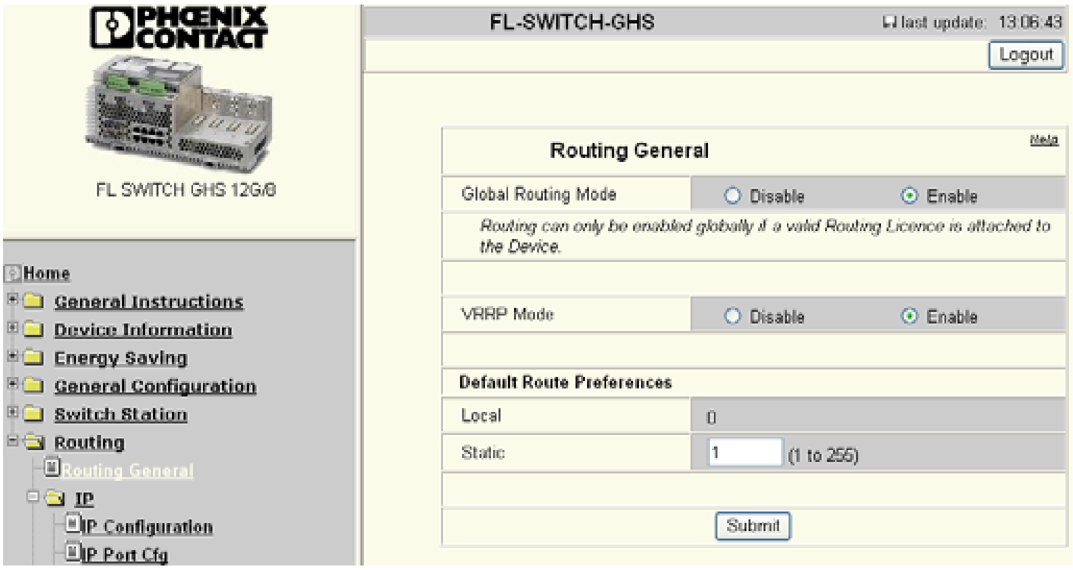
Figure 17-1 Inserting the SD card

On the FL SWITCH GHS 4G/12-L3 and the FL SWITCH GHS 12G/8-L3, the necessary Layer 3/routing license is already pre-installed. Activation with SD card is not necessary.

Following installation, the functions described below are available.

17.2 Global activation/deactivation of routing/VRRP

Both routing and VRRP can be activated or deactivated globally on the "Routing General" web page.



Routing General

Global Routing Mode ○ Disable ● Enable

Routing can only be enabled globally if a valid Routing Licence is attached to the Device.

VRRP Mode ○ Disable ● Enable

Default Route Preferences

Local	0
Static	1 (1 to 255)

Submit

Figure 17-2 "Routing General" web page

> The routing functions must be activated and configured for each port. Routing interfaces can be individual ports or VLANs that are configured as routing VLANs. The routing function must be activated and configured for each port or the routing parameters must be configured for each routing VLAN.

17.2.1 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.23.1.1 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkRouting(23).flWorkRoutingIp(1).flWorkRoutingIpRoutingMode(1)

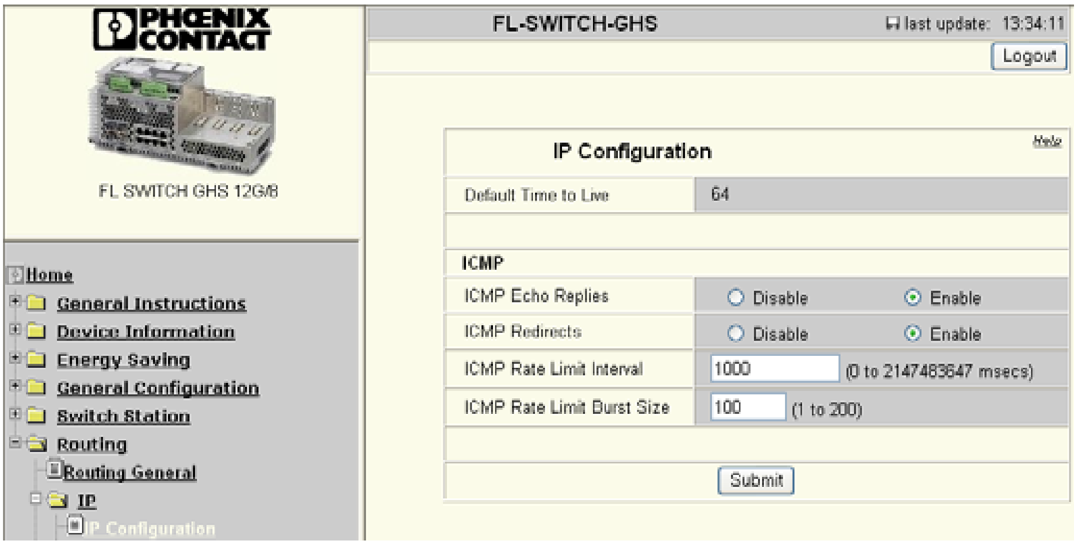
17.2.2 CLI

The settings can be found in the CLI under "routing mode".

CLI user manual: Unknown source of cross-reference

17.3 IP configuration for routing (global)

The global IP settings for routing are made on the "Routing/IP Configuration" page.



FL-SWITCH-GHS last update: 13:34:11

IP Configuration

Default Time to Live	64	
ICMP		
ICMP Echo Replies	○ Disable	● Enable
ICMP Redirects	○ Disable	● Enable
ICMP Rate Limit Interval	1000 (0 to 2147483647 msecs)	
ICMP Rate Limit Burst Size	100 (1 to 200)	

Figure 17-3 "Routing/IP Configuration" web page

ICMP Echo Replies (ping)

Select whether or not ICMP echo requests (pings) from the routing interface of the switch (e.g., a port with routing enabled and an IP address to which a ping can be sent) are answered.

ICMP Redirects

Select whether this device may specify an alternative (often "better") route to the destination to the sender of data packets (hosts).

ICMP Rate Limit Interval

This is the interval in ms during which one ICMP burst maximum is sent. The value 1000 therefore means a maximum of one burst per second. This setting is used, for example, to prevent Denial of Service (DOS) attacks.

ICMP Rate Limit Burst Size

The maximum number of ICMP packets that are sent per burst. These packets include, for example, ICMP Destination Unreachable messages. A value of 100 means, for example, that a maximum of 100 devices per burst (and therefore per ICMP rate limit interval) are notified via ICMP Destination Unreachable message that they are trying to contact an unreachable device for which no route is known, for example. This setting is used, for example, to prevent Denial of Service (DOS) attacks.

17.3.1 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.23.1.3.1 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkRouting(23).flWorkRoutingIp(1).flWorkRoutingIpInterfaceTable(3).flWorkRoutingIpInterfaceEntry(1)

17.3.2 CLI

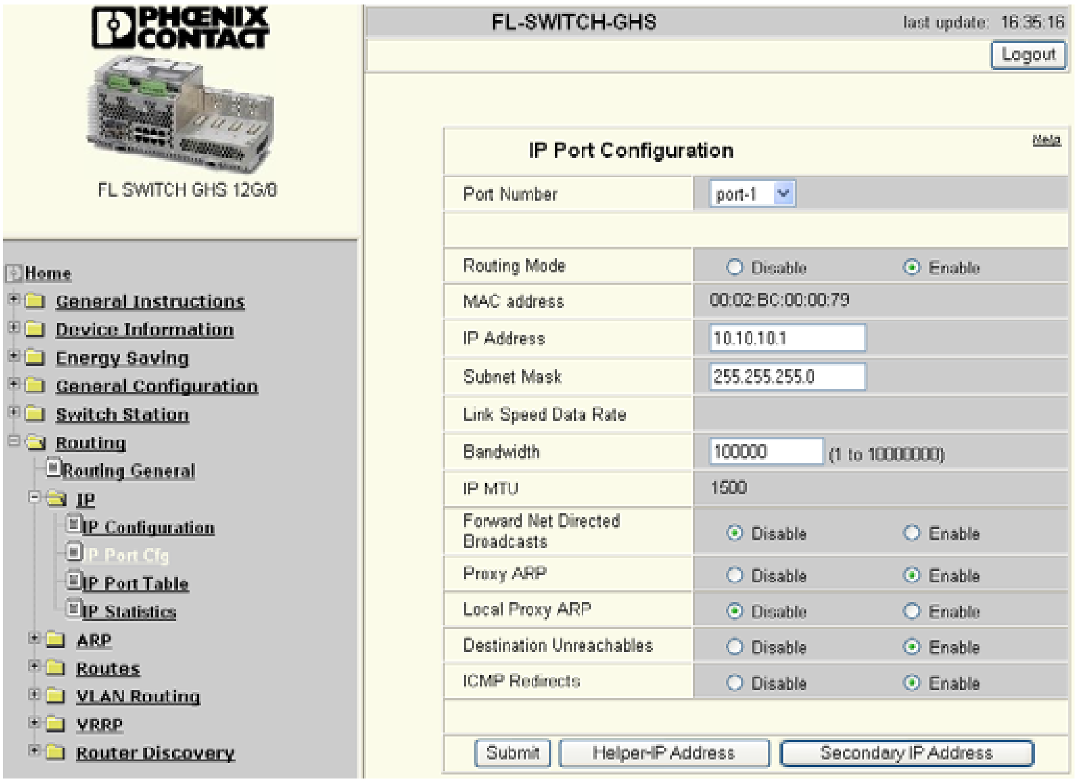
The settings can be found in the CLI under "ip/routing".

CLI user manual: Unknown source of cross-reference

17.3.3 IP configuration for routing (port-specific or VLAN-specific)

> The VLAN function must be enabled globally first (see Section 10 "Activating a VLAN").

The individual settings for each port are made on this web page. Physical ports or VLANs (previously configured as routing VLANs) are selected from the drop-down field. The routing functionality cannot be enabled or disabled here for a routing VLAN, it is always active because the VLAN has been configured for routing.



IP Port Configuration

Port Number	port-1	
Routing Mode	○ Disable	● Enable
MAC address	00:02:BC:00:00:79	
IP Address	10.10.10.1	
Subnet Mask	255.255.255.0	
Link Speed Data Rate		
Bandwidth	100000 (1 to 10000000)	
IP MTU	1500	
Forward Net Directed Broadcasts	● Disable	○ Enable
Proxy ARP	○ Disable	● Enable
Local Proxy ARP	● Disable	○ Enable
Destination Unreachables	○ Disable	● Enable
ICMP Redirects	○ Disable	● Enable

Figure 17-4 "IP Port Configuration" web page

Routing Mode

Enable/disable routing at this port.

IP Address

Specify the IP address of this port for the relevant subnetwork here. The IP address set here is used to access the management interface of the switch and can be used as a gateway address for the connected subnetwork in order to use the routing functionality.

Subnet Mask

Specify the corresponding subnet mask here. Together with the IP address, the subnet mask defines the connected subnetwork, which is automatically applied in the routing table of the device. For example, the combination of IP = 172.16.29.1 and netmask = 255.255.255.0 means that the subnetwork with subnet address 172.16.29.0 is connected to this port or routing VLAN.

Link Speed Data Rate/Bandwidth

For future applications with dynamic routing protocols.

Forward Net Directed Broadcasts

Select whether broadcasts that are addressed to the network broadcast address of the connected subnetwork are forwarded in the subnetwork or whether they are rejected.

The network broadcast address of the network configured as follows with IP = 172.16.29.1 and netmask = 255.255.255.0 is 172.16.29.255, for example.

Proxy ARP

Allows the switch to respond to certain ARP requests.

If no default gateway has been configured for a client, the client can send an ARP request to an IP address that is located in a completely different subnetwork (if the client's operating system supports this). If it recognizes a route in this subnetwork, the switch then answers the ARP request with its own MAC address and thus dynamically declares a gateway for the client.

Local Proxy ARP

Select whether local data traffic within a network segment is transmitted directly between the clients or via the router port of the switch.

If activated, the switch answers all ARP requests of the network segment and therefore routes all data traffic via its router port.

Destination Unreachables

Select whether feedback is sent to the sender of a data packet if the data packet cannot be delivered because there is no known route to the destination address.

ICMP Redirects

Select whether this device may specify an alternative (often "better") route to the destination to the sender of data packets (hosts).

IP helper address

An IP helper address is the IP address of a server which responds to special requests, such as DHCP requests, DNS requests, etc. The maximum number is four.

> In addition to the globally set server address, the DHCP relay agent also uses the IP helper addresses.

Secondary IP Address (with subnet mask)

Means that more than one subnetwork with a routing interface
(physical port or routing VLAN) can be connected ("multinetting" to support multiple subnetworks at one port).

The maximum number of secondary IP addresses is 31 per port plus primary IP address (in total a maximum of 28 ports x 32 subnetworks = 896 subnetworks).

17.3.4 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.23.2 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkRouting(23).flWorkRoutingArp(2)

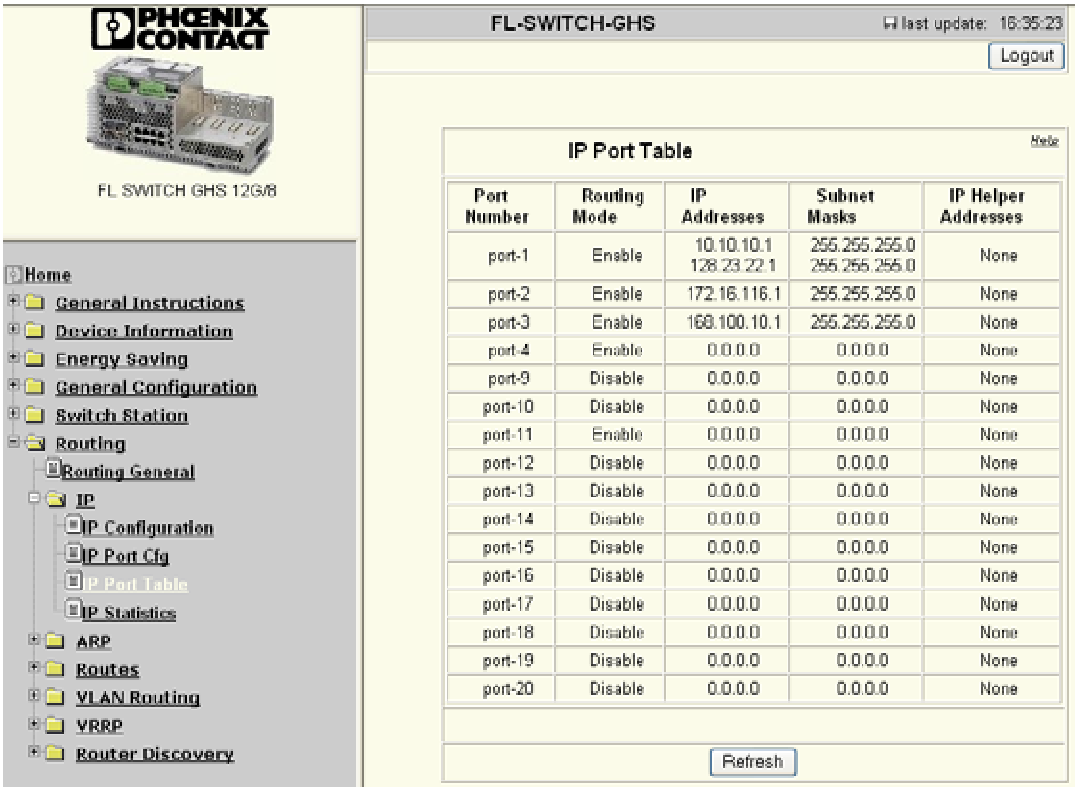
17.3.5 CLI

The settings can be found in the CLI under "show ip interface".

CLI user manual: Unknown source of cross-reference

17.3.6 Overview of the router port settings

An overview of the relevant port configuration can be found on the "Routing/IP Port Table" web page.



IP Port Table

Port Number	Routing Mode	IP Addresses	Subnet Masks	IP Helper Addresses
port-1	Enable	10.10.10.1 128.23.22.1	255.255.255.0 255.255.255.0	None
port-2	Enable	172.16.116.1	255.255.255.0	None
port-3	Enable	168.100.10.1	255.255.255.0	None
port-4	Enable	0.0.0.0	0.0.0.0	None
port-9	Disable	0.0.0.0	0.0.0.0	None
port-10	Disable	0.0.0.0	0.0.0.0	None
port-11	Enable	0.0.0.0	0.0.0.0	None
port-12	Disable	0.0.0.0	0.0.0.0	None
port-13	Disable	0.0.0.0	0.0.0.0	None
port-14	Disable	0.0.0.0	0.0.0.0	None
port-15	Disable	0.0.0.0	0.0.0.0	None
port-16	Disable	0.0.0.0	0.0.0.0	None
port-17	Disable	0.0.0.0	0.0.0.0	None
port-18	Disable	0.0.0.0	0.0.0.0	None
port-19	Disable	0.0.0.0	0.0.0.0	None
port-20	Disable	0.0.0.0	0.0.0.0	None

Figure 17-5 "Routing/IP Port Table" web page

17.3.7 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.23.1.3 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkRouting(23).flWorkRoutingIp(1).flWorkRoutingIpInterfaceTable(3)

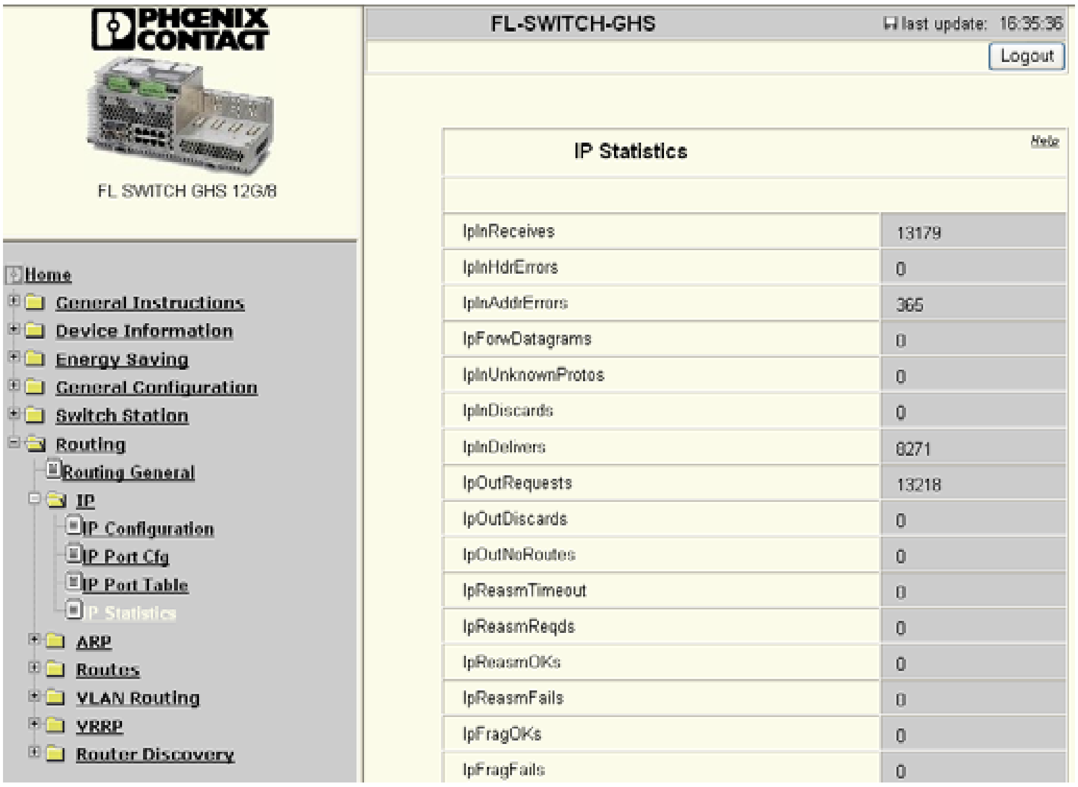
17.3.8 CLI

The settings can be found in the CLI under "show ip brief".

CLI user manual: Unknown source of cross-reference

17.3.9 Summary of data traffic

A statistical summary of the data traffic can be found on the "IP Statistics" web page. These statistics present an evaluation of the IP packets in table form. The same data can be read and used, e.g., for a visualization, from MIB2 via SNMP. The specified data is used exclusively for data traffic diagnostics and does not reflect the quality of the data traffic within the device.



IP Statistics

IpInReceives	13179
IpInHdrErrors	0
IpInAddrErrors	365
IpForwDatagrams	0
IpInUnknownProtos	0
IpInDiscards	0
IpInDelivers	8271
IpOutRequests	13218
IpOutDiscards	0
IpOutNoRoutes	0
IpReasmTimeout	0
IpReasmReqds	0
IpReasmOKs	0
IpReasmFails	0
IpFragOKs	0
IpFragFails	0

Figure 17-6 "IP Statistics" web page

17.3.10 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.23.1.3.1 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkRouting(23).flWorkRoutingIp(1).flWorkRoutingIpInterfaceTable(3).flWorkRoutingIpInterfaceEntry(1)

17.3.11 CLI

The settings can be found in the CLI under "show ip brief".

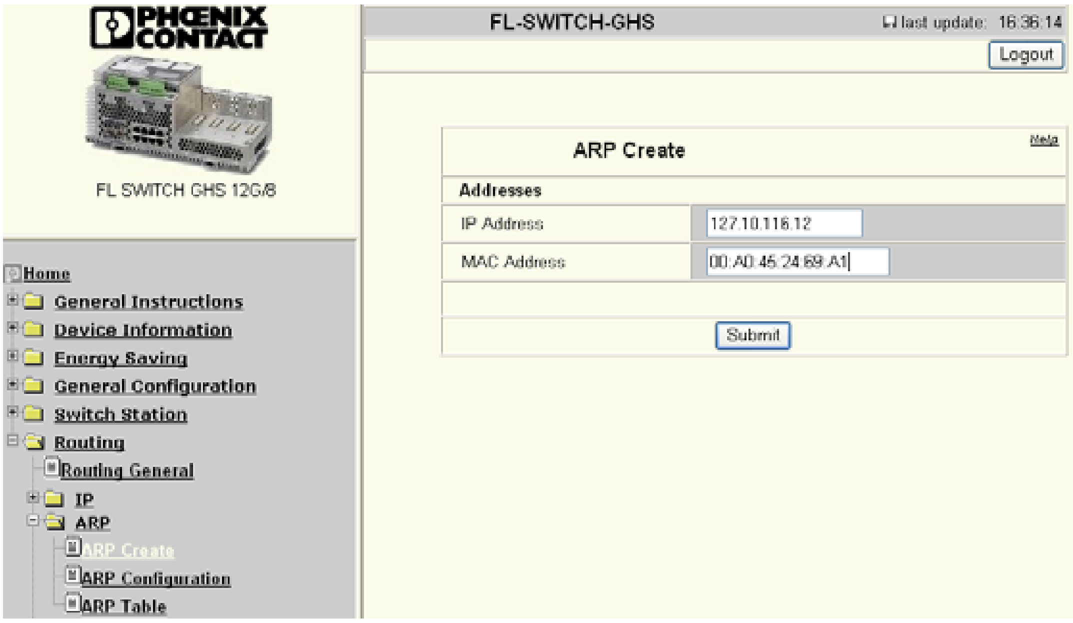
CLI user manual: Unknown source of cross-reference

17.4 ARP configuration for routing

17.4.1 Creating an ARP entry

An entry can be created in the ARP table on the "ARP Create" web page using the IP address and the MAC address of a device. In order to save time when delivering data packets, the ARP entries do not have to be requested or renewed dynamically, instead they can also be assigned statically.

These entries are useful for the MAC addresses of network components that are available statically in the network, e.g., neighbor routers.



ARP Create

Addresses

IP Address: 127.10.116.12

MAC Address: 00:A0:45:24:69:A1

Figure 17-7 "ARP Create" web page

17.4.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.23.2 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkRouting(23).flWorkRoutingArp(2)

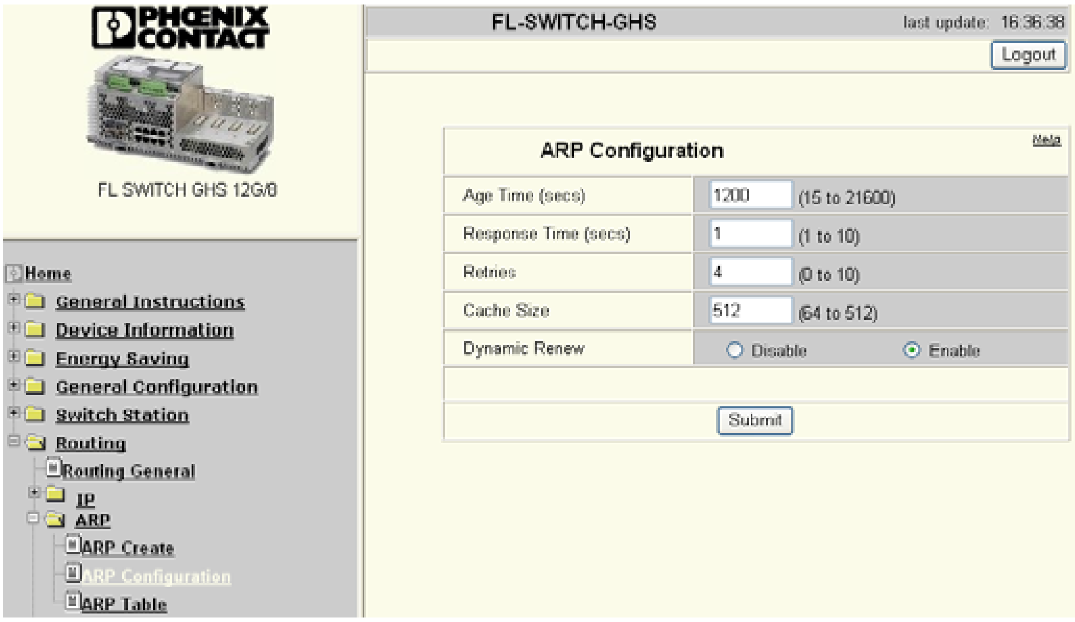
17.4.3 CLI

The settings can be found in the CLI under "arp".

CLI user manual: Unknown source of cross-reference

17.4.4 ARP configuration (global)

The global ARP configuration settings are made on the "ARP Configuration" web page.



ARP Configuration

Age Time (secs)	1200	(15 to 21600)
Response Time (secs)	1	(1 to 10)
Retries	4	(0 to 10)
Cache Size	512	(64 to 512)
Dynamic Renew	○ Disable	● Enable

Figure 17-8 "ARP Configuration" web page

Age Time

Specifies the time in seconds during which an ARP entry is valid.

Response Time

Specifies the time the switch waits for an ARP response before it repeats the ARP request.

Retries

Number of retries of an ARP request.

Cache Size

Maximum number of ARP entries.

Dynamic Renew

Select whether the switch should automatically attempt to renew the ARP entries when their Age Time expires.

17.4.5 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.23.2 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkRouting(23).flWorkRoutingArp(2)

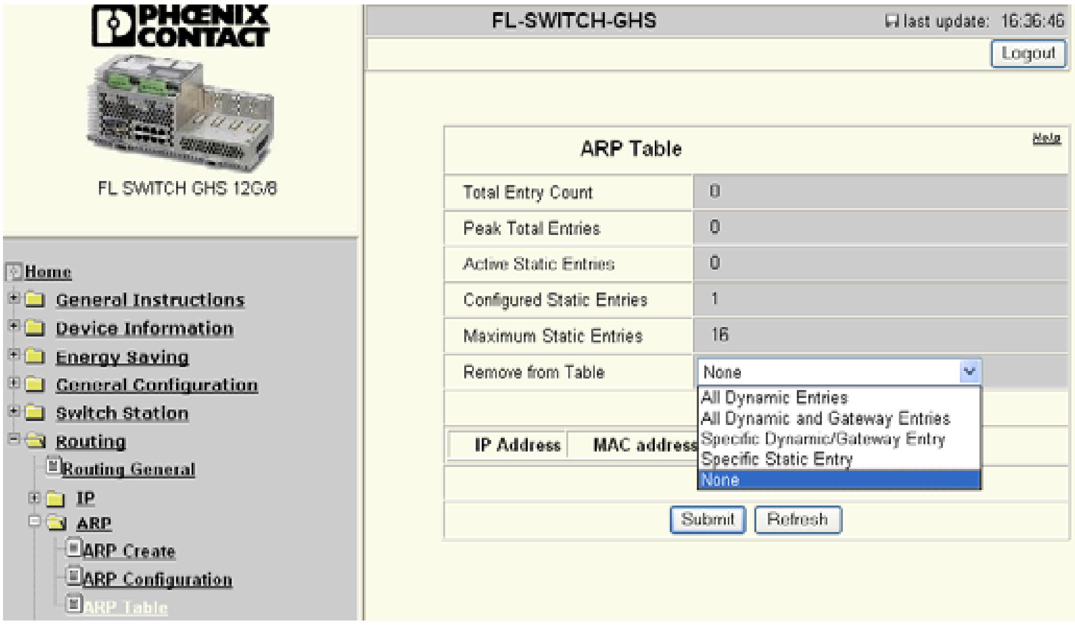
17.4.6 CLI

The settings can be found in the CLI under "arp".

CLI user manual: Unknown source of cross-reference

17.4.7 The ARP table

The "ARP Table" web page displays the ARP table of the switch and offers the option of deleting ARP entries. Deletion is necessary in order to delete static routes. For example, if a new device with a new MAC address is used in the system following device replacement, the previously defined ARP settings must be deleted..



ARP Table

Total Entry Count	0
Peak Total Entries	0
Active Static Entries	0
Configured Static Entries	1
Maximum Static Entries	16
Remove from Table	None

IP Address	MAC address

Figure 17-9 "ARP Table" web page

17.4.8 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.23.2.10 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkRouting(23).flWorkRoutingArp(2).flWorkRoutingArpTable(10)

17.4.9 CLI

The settings can be found in the CLI under "show arp".

CLI user manual: Unknown source of cross-reference

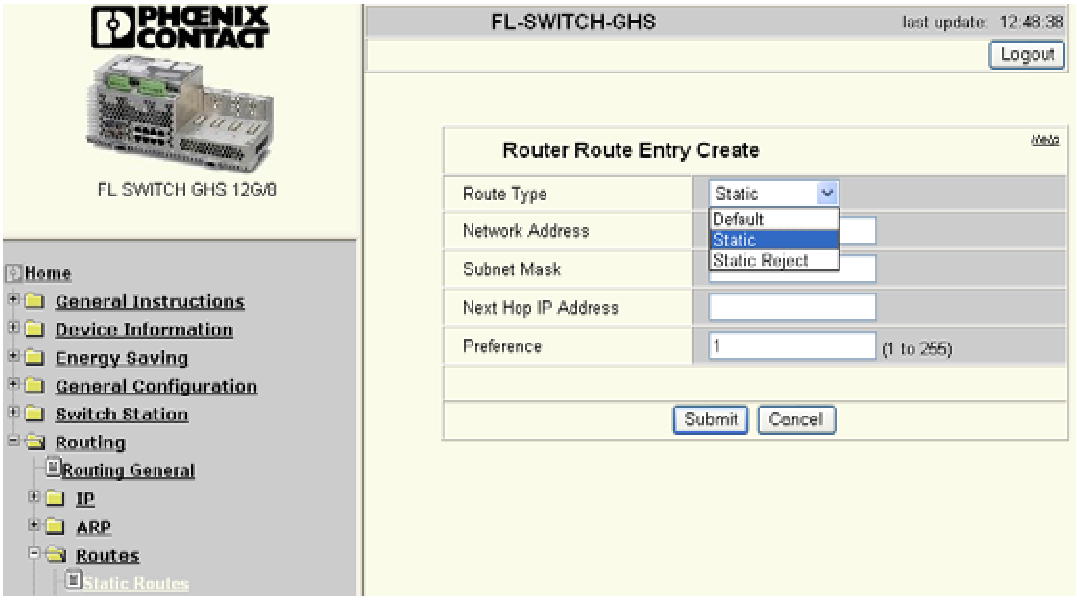
17.5 Route configuration

17.5.1 Static routes

All routes that are currently configured can be seen on the "Routing/Routes/Static Routes" web page and you have the option of creating new routes and deleting existing routes.

Three selection options are available for static routes:

- **Default:** All packets whose destination network is not configured in other routes are sent to the default routes.
- **Static:** A static route is used if a specific network is to be accessed via this route.
- **Static Reject:** Data packets from this network are not routed.



Router Route Entry Create

Route Type	Static
Network Address	
Subnet Mask	
Next Hop IP Address	
Preference	1 (1 to 255)

Figure 17-10 "Routing/Routes/Router Route Entry Create" web page

17.5.2 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.23.1.3 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkRouting(23).flWorkRoutingIp(1).flWorkRoutingIpInterfaceTable(3)

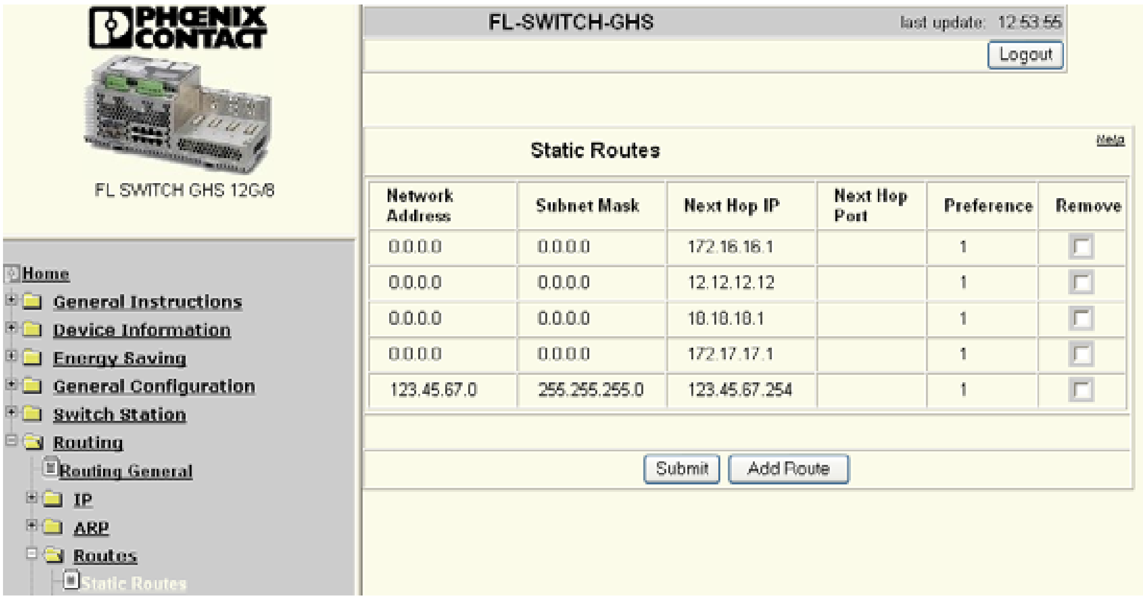
17.5.3 CLI

The settings can be found in the CLI under "route".

CLI user manual: Unknown source of cross-reference

17.5.4 Displaying existing routes

The "Routing/Routes/Static Routes" web page displays all routes that have been created (see Figure 17-11 on page 17-13). The first four routes, for which no network address or subnet mask have been specified, are default routes.



Static Routes

Network Address	Subnet Mask	Next Hop IP	Next Hop Port	Preference	Remove
0.0.0.0	0.0.0.0	172.16.16.1		1	□
0.0.0.0	0.0.0.0	12.12.12.12		1	□
0.0.0.0	0.0.0.0	10.10.10.1		1	□
0.0.0.0	0.0.0.0	172.17.17.1		1	□
123.45.67.0	255.255.255.0	123.45.67.254		1	□

Figure 17-11 "Static Routes" web page

Created routes cannot be modified, instead they must be deleted and created again.

17.5.5 Displaying routes

The "Static Routes" web page displays all the routes known by the device. The "Best Routes" web page displays the route with the lowest preference for a destination network.

17.5.6 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.23.1.5 under the following path:
Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkRouting(23).flWorkRoutingIp(1).flWorkRoutingIpVlanTable(5)

17.5.7 CLI

The settings can be found in the CLI under "show routes".

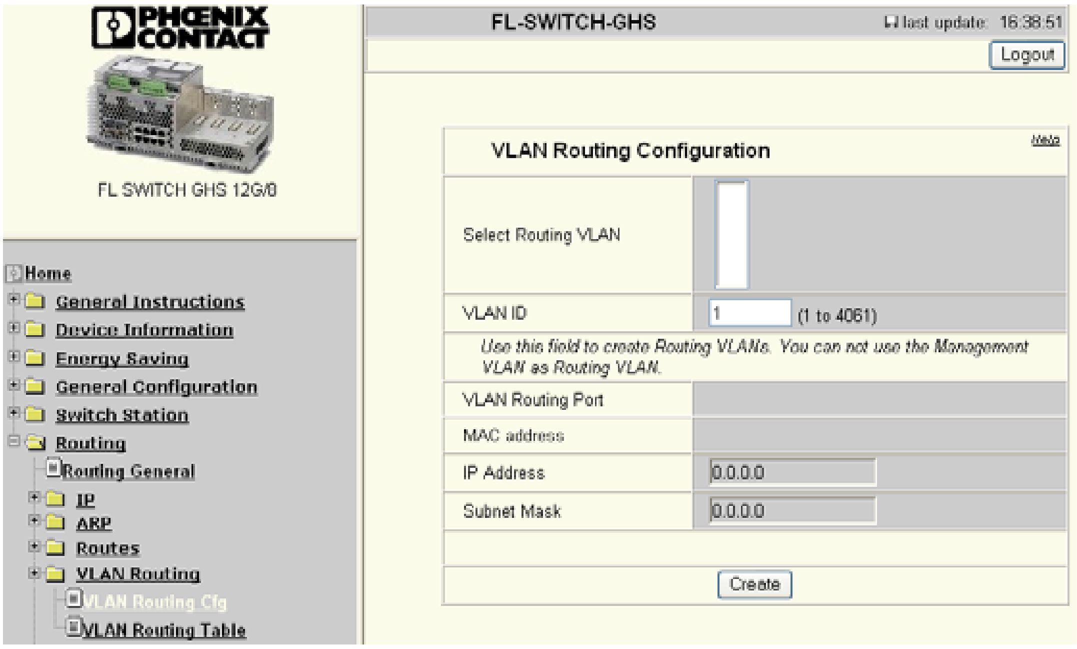
CLI user manual: Unknown source of cross-reference

17.6 VLAN routing

ℹ The VLAN function must be enabled globally first (see Section 10 "Activating a VLAN").

In a VLAN, several ports, to which devices are connected, are linked together. Communication between the devices of a VLAN takes place on Layer 2. If data packets are routed to a network segment other than the local VLAN, VLAN routing is required. A routing IP address and subnet mask are assigned to a VLAN port.

ℹ Routing VLANs can only be set up if corresponding VLANs have first been configured as Layer 2 VLANs in the "Switch Station" menu.



FL-SWITCH-GHS last update: 16:38:51

VLAN Routing Configuration

Select Routing VLAN	
VLAN ID	1 (1 to 4061)
Use this field to create Routing VLANs. You can not use the Management VLAN as Routing VLAN.	
VLAN Routing Port	
MAC address	
IP Address	0.0.0.0
Subnet Mask	0.0.0.0

Figure 17-12 "VLAN Routing Configuration" web page

17.6.1 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.23.1.5 under the following path:
Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkRouting(23).flWorkRoutingIp(1).flWorkRoutingIpVlanTable(5)

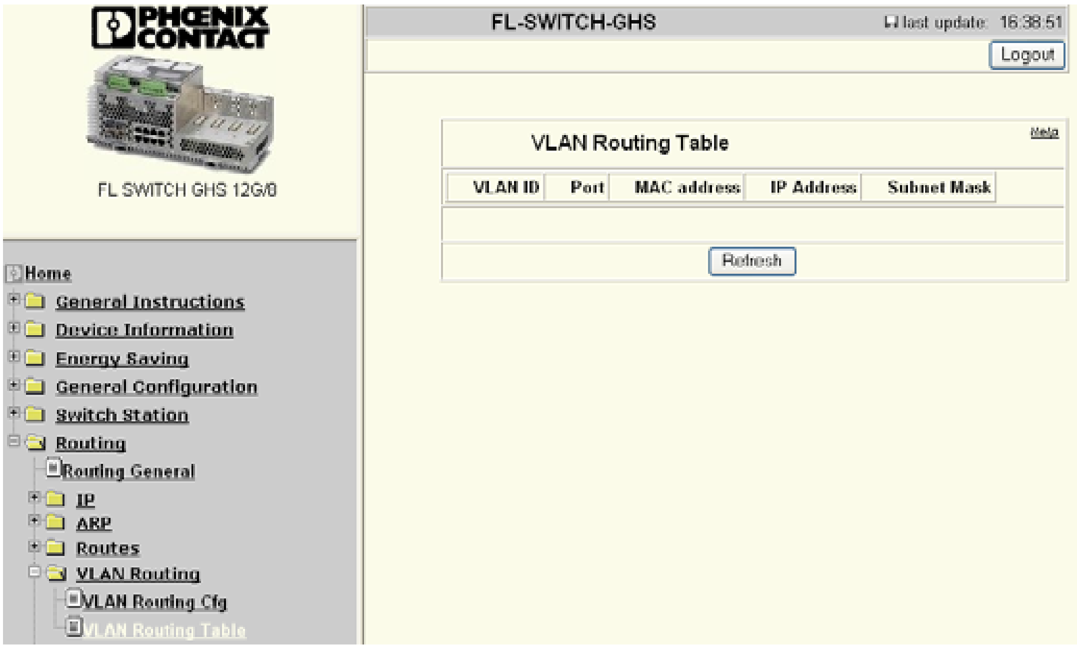
17.6.2 CLI

The settings can be found in the CLI under "vlan routing".

CLI user manual: Unknown source of cross-reference

17.6.3 Displaying the VLAN routing configuration

All configured routing VLANs are listed on the "VLAN Routing Table" web page.



VLAN Routing Table

VLAN ID	Port	MAC address	IP Address	Subnet Mask

Figure 17-13 "VLAN Routing Table" web page

17.6.4 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.23.1.5 under the following path:
Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkRouting(23).flWorkRoutingIp(1).flWorkRoutingIpVlanTable(5)

17.6.5 CLI

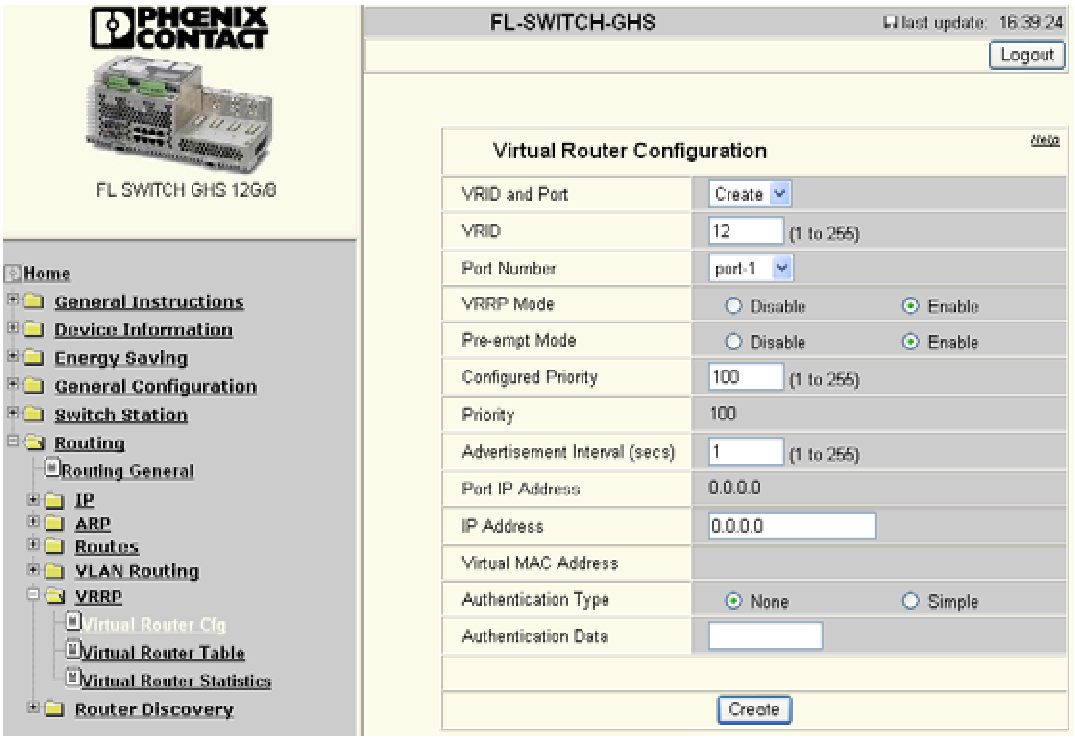
The settings can be found in the CLI under "vlan routing".

CLI user manual: Unknown source of cross-reference

17.7 Virtual Router Redundancy Protocol (VRRP)

With VRRP, two or more physical routers are combined to create a virtual router. The virtual router has an IP and MAC address which are used for communication. If one of the physical routers fails, the virtual addresses of another router are used. For this, one of the routers in the group is defined as the master.

Please note that VRRP must be enabled globally (see Figure 17-2 on page 17-2).



Virtual Router Configuration

VRID and Port	Create	
VRID	12 (1 to 255)	
Port Number	port-1	
VRRP Mode	○ Disable	● Enable
Pre-empt Mode	○ Disable	● Enable
Configured Priority	100 (1 to 255)	
Priority	100	
Advertisement Interval (secs)	1 (1 to 255)	
Port IP Address	0.0.0.0	
IP Address	0.0.0.0	
Virtual MAC Address		
Authentication Type	● None	○ Simple
Authentication Data		

Figure 17-14 "Virtual Router Configuration" web page

VRID and Port/Create

Create a new virtual router by selecting "Create" or select an existing virtual router.

VRID

ID of the virtual router.

Port Number

Specifies the port that belongs to the virtual router.

VRRP Mode

Select whether VRRP should be active.

Pre-empt Mode

Select whether the master function should be applied if the local priority is found to be higher than the master priority.

Configured Priority

Specify the priority of this router in a VRRP group. The higher the value the higher the priority. Value range from 1 to 254.
A value of 255 is set automatically if the IP address of the port matches that of the virtual router.

Advertisement Interval (secs)

Specify in seconds how frequently the router should send a sign of life.

Port IP Address

IP address of this port.

IP Address

Virtual IP address as the communication IP for the virtual router.

Virtual MAC Address

Virtual MAC address as the communication MAC for the virtual router.

Authentication Type

This parameter specifies the type of authorization.

Authentication Data

This value contains the password if "Simple" has been specified as the authentication type.

17.7.1 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.23.3 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkRouting(23).flWorkRoutingVrrp(3)

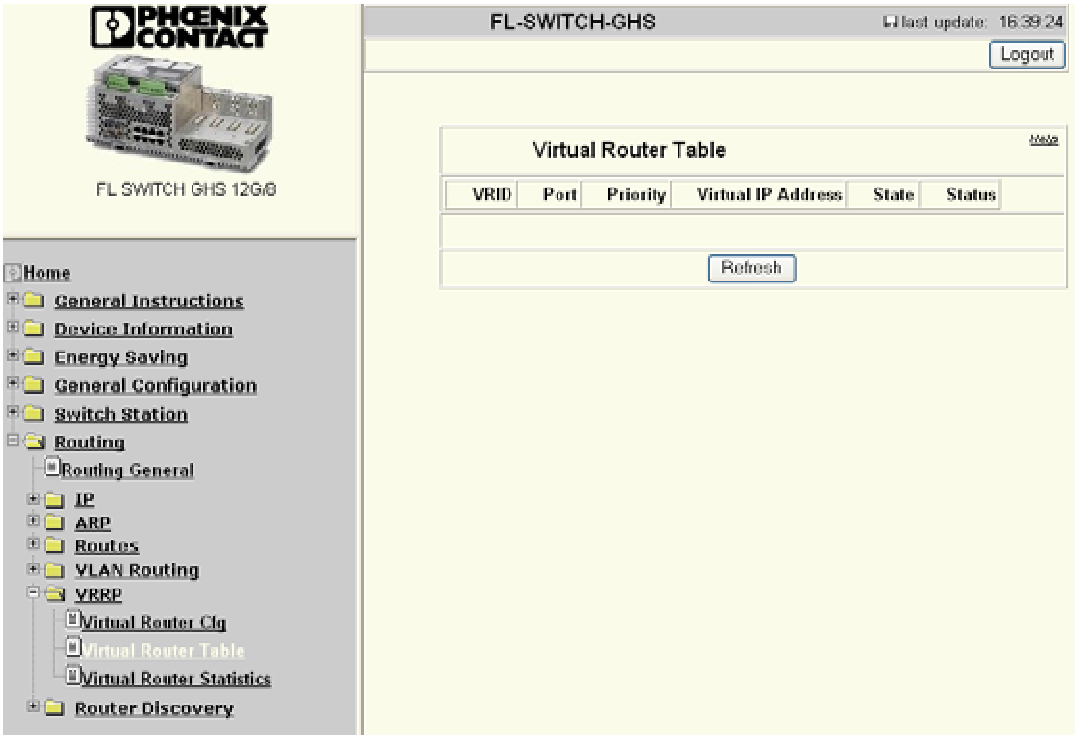
17.7.2 CLI

The settings can be found in the CLI under "ip vrrp".

CLI user manual: Unknown source of cross-reference

17.8 Displaying VRRP groups

All configured VRRP groups are listed on the "Virtual Router Table" web page.



Virtual Router Table

VRID	Port	Priority	Virtual IP Address	State	Status

Figure 17-15 "Virtual Router Table" web page

17.8.1 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.23.3 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkRouting(23).flWorkRoutingVrrp(3)

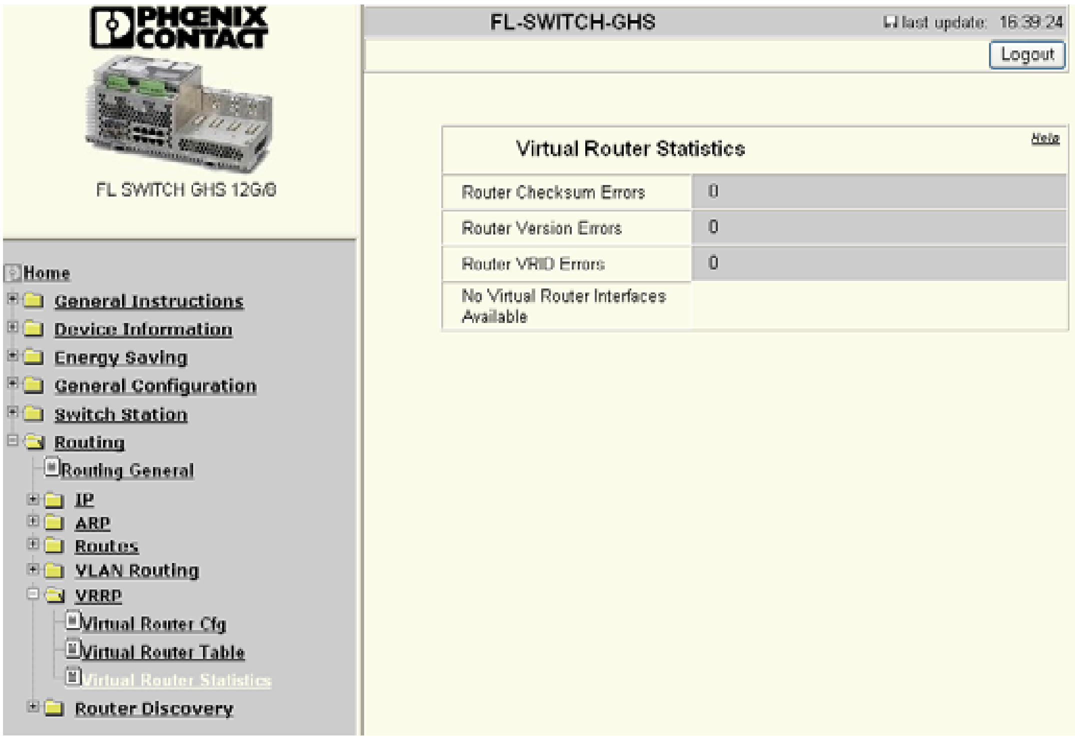
17.8.2 CLI

The settings can be found in the CLI under "show ip vrrp".

CLI user manual: Unknown source of cross-reference

17.8.3 Summary of VRRP data traffic

A statistical summary of the VRRP data traffic can be found on the "Virtual Router Statistics" web page. This page can provide an initial indication of possible network errors.



Virtual Router Statistics

Router Checksum Errors	0
Router Version Errors	0
Router VRID Errors	0
No Virtual Router Interfaces Available	

Figure 17-16 "Virtual Router Statistics" web page

17.8.4 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.23.3 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkRouting(23).flWorkRoutingVrrp(3)

17.8.5 CLI

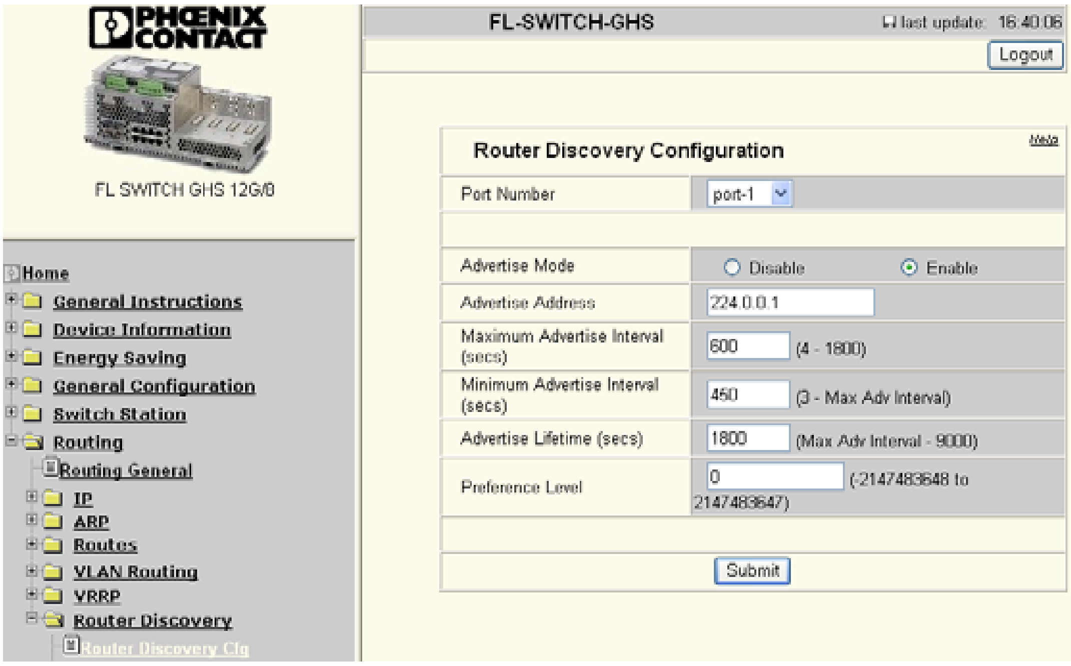
The settings can be found in the CLI under "show ip vrrp".

CLI user manual: Unknown source of cross-reference

17.9 Router Discovery

The ICMP Router Discovery Protocol (IRDP) enables clients in the network to locate existing routers. To do this, the router sends what are known as router advertisements and router solicitation messages from its interfaces. These messages are sent as ICMP packets.

The advertisements are sent to multicast address 224.0.0.1. The clients send the solicitations to multicast IP 224.0.0.2.



Router Discovery Configuration

Port Number	port-1
Advertise Mode	○ Disable ● Enable
Advertise Address	224.0.0.1
Maximum Advertise Interval (secs)	600 (4 - 1800)
Minimum Advertise Interval (secs)	450 (3 - Max Adv Interval)
Advertise Lifetime (secs)	1800 (Max Adv Interval - 9000)
Preference Level	0 (-2147483648 to 2147483647)

Figure 17-17 "Router Discovery Configuration" web page

Port Number

Select the physical ports.

Advertise Mode

Select whether the Router Discovery Protocol should be activated.

Advertise Address

Address to which the router information is sent. Possible addresses are multicast address 224.0.0.1 and broadcast address 255.255.255.255.

Maximum Advertise Interval

Maximum time between two items of router information.

Minimum Advertise Interval

Minimum time between two items of router information.

Advertise Lifetime (secs)

Lifetime of the router information.

Preference Level

Indicates the priority of the router compared to other routers in the same subnetwork. Higher values are preferred.

17.9.1 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.23.1.4 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkRouting(23).flWorkRoutingIp(1).flWorkRoutingIpRouterDiscoveryTable(4)

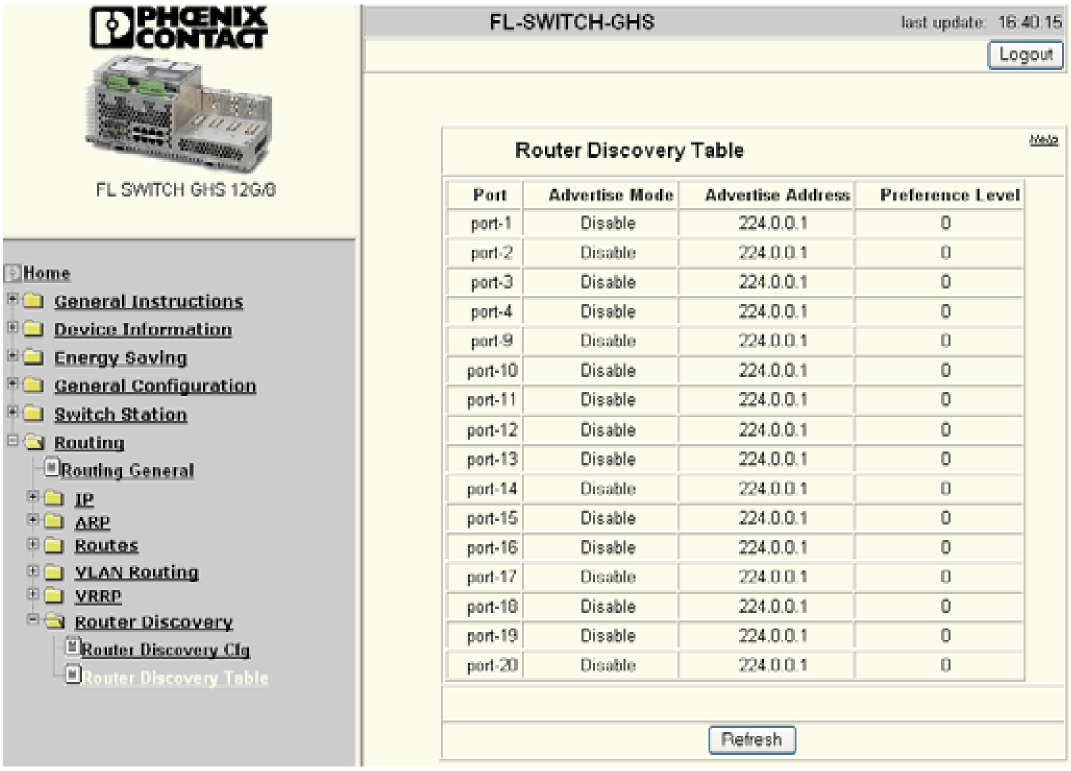
17.9.2 CLI

The settings can be found in the CLI under "ip irdp".

CLI user manual: Unknown source of cross-reference

17.9.3 Summary of the Routing Discovery Protocol

A summary of the ports for which the Routing Discovery Protocol is activated can be found on the "Router Discovery Table" web page.



Router Discovery Table

Port	Advertise Mode	Advertise Address	Preference Level
port-1	Disable	224.0.0.1	0
port-2	Disable	224.0.0.1	0
port-3	Disable	224.0.0.1	0
port-4	Disable	224.0.0.1	0
port-9	Disable	224.0.0.1	0
port-10	Disable	224.0.0.1	0
port-11	Disable	224.0.0.1	0
port-12	Disable	224.0.0.1	0
port-13	Disable	224.0.0.1	0
port-14	Disable	224.0.0.1	0
port-15	Disable	224.0.0.1	0
port-16	Disable	224.0.0.1	0
port-17	Disable	224.0.0.1	0
port-18	Disable	224.0.0.1	0
port-19	Disable	224.0.0.1	0
port-20	Disable	224.0.0.1	0

"Router Discovery Table" web page

17.9.4 SNMP

The settings can be found under OID 1.3.6.1.4.1.4346.11.11.23.1.4 under the following path:

Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).phoenixContact(4346).pxcFactoryLine(11).flWorkDevice(11).flWorkRouting(23).flWorkRoutingIp(1).flWork-RoutingIpRouterDiscoveryTable(4)

17.9.5 CLI

The settings can be found in the CLI under "show ip irdp".

CLI user manual: Unknown source of cross-reference

18 Multicast filtering

18.1 Basics

Multicast

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

Advantages:

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

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

> A maximum of 128 multicast groups can be created automatically for IGMP snooping. In addition, a maximum of 20 static groups can be created.

18.2 Enabling the web pages for multicast filtering in WBM

Activate WBM for the switches, e.g., using Factory Manager. Switch to the "General Configuration" menu, then the "User Interfaces" page. Activate "Multicast Filtering" and confirm by entering your password.

> When activating "Multicast Filtering" under "General Configuration/User Interfaces", the multicast mechanism is **not** activated. In the WBM menu, the "Multicast" page - under which the function can be configured and activated - is enabled.

18.3 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.

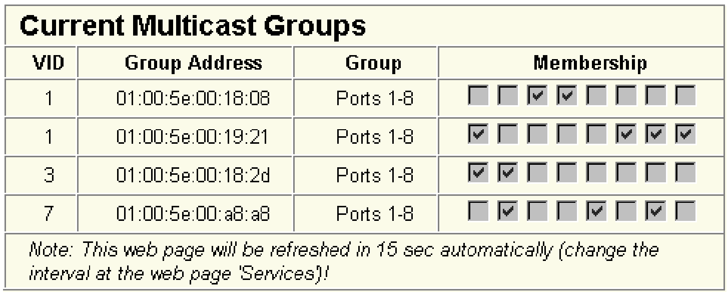
2 No querier required (see "Query" on page 18-7).

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.

18.3.1 "Current Multicast Groups" web page

The table on this web page provides an overview of the current multicast groups created on this MMS. These include multicast groups that are assigned as a result of IGMP snooping and groups that are statically created.



Current Multicast Groups

VID	Group Address	Group	Membership
1	01:00:5e:00:18:08	Ports 1-8	□ □ ☑ ☑ □ □ □ □
1	01:00:5e:00:19:21	Ports 1-8	☑ □ □ □ □ ☑ ☑ ☑
3	01:00:5e:00:18:2d	Ports 1-8	☑ ☑ □ □ □ □ □ □
7	01:00:5e:00:a8:a8	Ports 1-8	□ ☑ □ □ ☑ □ ☑ □

Note: This web page will be refreshed in 15 sec automatically (change the interval at the web page 'Services')!

Figure 18-1 "Current Multicast Groups" web page

These checkboxes indicate which port has been assigned to each individual group.

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

The overview for group membership is based on the "dot1qTpGroupTable" SNMP group. This table contains all groups (static entries and IGMP) and their members.

18.3.2 Creating static multicast groups

This web page is used to create and manage statically configured multicast groups. In order to create a multicast group, enter the MAC address provided (see "Multicast addresses" on page 18-4) 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 802.1 D/p.

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

Conversion

The guidelines for converting a multicast IP addresses 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, you should avoid using IP addresses that differ by 128 in the third byte from the right. Example:

		3rd byte from the right	
1st multicast IP address:	228 .	30	. 117 . 216
2nd multicast IP address:	230 .	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.

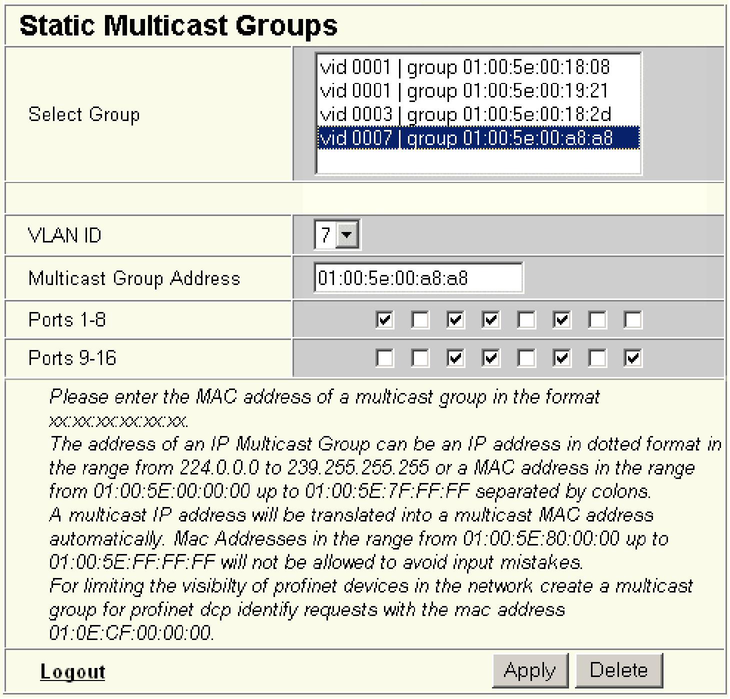
Settings are not automatically saved permanently. The active configuration can be saved permanently by selecting "Save current configuration" on the "Configuration Management" web page.

Port assignment

After entering a new group in the "Multicast Group Address" field, add the ports of the group members by selecting the corresponding checkboxes. Confirm by entering your password and clicking on "Apply".

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 activated checkboxes and can be modified, if required. An action is completed by entering a password and clicking on "Apply" or "Delete".



Static Multicast Groups

Select Group	vid 0001 | group 01:00:5e:00:18:08 vid 0001 | group 01:00:5e:00:19:21 vid 0003 | group 01:00:5e:00:18:2d vid 0007 | group 01:00:5e:00:a8:a8
VLAN ID	7
Multicast Group Address	01:00:5e:00:a8:a8
Ports 1-8	☑ □ ☑ ☑ □ ☑ □ □
Ports 9-16	□ □ ☑ ☑ □ ☑ □ ☑

Please enter the MAC address of a multicast group in the format xx:xx:xx:xx:xx:xx.
The address of an IP Multicast Group can be an IP address in dotted format in the range from 224.0.0.0 to 239.255.255.255 or a MAC address in the range from 01:00:5E:00:00:00 up to 01:00:5E:7F:FF:FF separated by colons.
A multicast IP address will be translated into a multicast MAC address automatically. Mac Addresses in the range from 01:00:5E:80:00:00 up to 01:00:5E:FF:FF:FF will not be allowed to avoid input mistakes.
For limiting the visibilty of profinet devices in the network create a multicast group for profinet dcp identify requests with the mac address 01:0E:CF:00:00:00.

Figure 18-2 "Static Multicast Groups" menu

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 checkboxes.

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 are separated by a full stop (.).

18.3.3 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 the following table, the ports (for each switch) to which the receivers of the multicast data are connected are indicated with an "X". See example configuration Figure 18-3 on Page 18-6.

Table 18-1 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	X
Port 3							
Port 4					X		X
Port 5				X			
Port 6						X	
Port 7	X						
Port 8			X		X		

Please note that possible redundant paths resulting from Rapid Spanning Tree must be taken into consideration for multicast group creation.

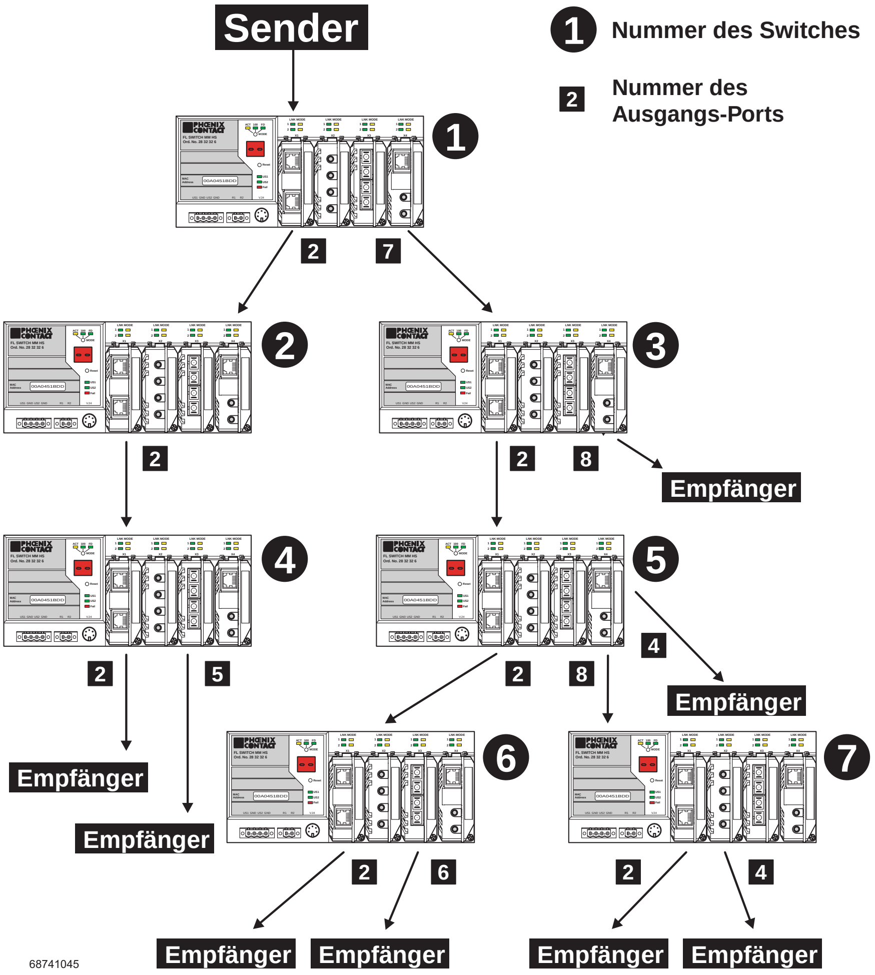


Figure 18-3 Configuration example

Possible redundant paths resulting from Rapid Spanning Tree must be taken into consideration for multicast group creation.

18.4 Dynamic multicast groups

18.4.1 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 IP level (Layer 3).

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

Query

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

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

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

IGMP snooping

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

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

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

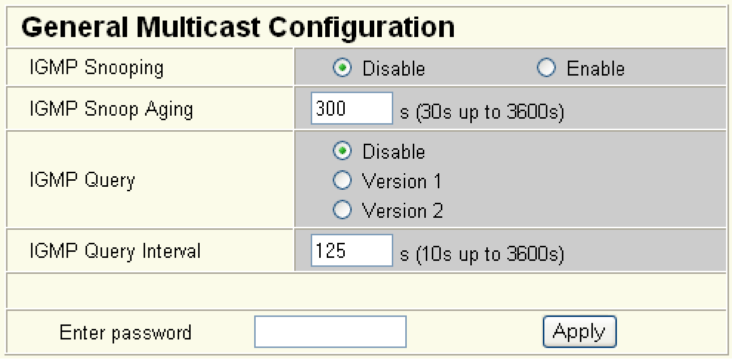
18.4.1.1 Extended multicast filtering

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

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

18.4.2 "General Multicast Configuration" web page

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



General Multicast Configuration

IGMP Snooping	● Disable ○ Enable
IGMP Snoop Aging	300 s (30s up to 3600s)
IGMP Query	● Disable ○ Version 1 ○ Version 2
IGMP Query Interval	125 s (10s up to 3600s)

Figure 18-4 "General Multicast Configuration" web 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
An MMS/MCS with activated query function actively sends queries at "query intervals" and evaluates the received reports. The MMS/MCS only sends IGMP query reports if IGMP snooping is enabled and only in the management VLAN.

19 Technical data and ordering data

19.1 Technical data

General data	
Function	Gigabit Modular Switch; conforms to standard IEEE 802.3
Switch principle	Store-and-forward
Address table	16,000 MAC addresses
SNMP	Version 1, 2, 2c, and 3
Transmission capacity per port 64-byte packet size, half duplex	At 10 Mbps: 14,880 pps (packets per second) At 100 Mbps: 148,800 pps At 1000 Mbps 1,488,000 pps
Supported MIBs	MIB II, RMON MIB, Bridge MIB, If MIB, Etherlike MIB, and Phoenix Contact private SNMP objects
Housing dimensions (width x height x depth) in mm	
Head station	287 x 125 x 115 (depth from top edge of DIN rail)
Permissible operating temperature	-20°C to +55°C
Permissible storage temperature	-20°C to +70°C
Degree of protection	IP20, DIN 40050, IEC 60529
Protection class according to EN 61131-2, IEC 61131-2	3
Laser protection - fiber optic interface modules	Class 1 according to EN 60825-1
Humidity	
Operation	10% to 95%, no condensation
Storage	10% to 95%, no condensation
Air pressure	
Operation	80 kPa to 108 kPa, 2000 m above sea level
Storage	70 kPa to 108 kPa, 3000 m above sea level
Mounting position	Perpendicular to a standard DIN rail
Connection to protective earth ground	Snapped onto a grounded DIN rail
Weight of head station	2700 g, typical

Supply voltage (US1/US2 redundant)	
Connection	Via COMBICON; maximum conductor cross section = 2.5 mm^2
Nominal value	24 V DC (SELV/PELV)
Permissible voltage range	18.5 V DC to 30.5 V DC
Test voltage	500 V DC for one minute
Typical current consumption on US at 24 V DC	0.8 ... 2.5 A/2.7 A, depending on configuration (extensions/interface modules)
Typical power consumption	19.2 W ... 60 W/65 W, depending on configuration (extensions/interface modules); see example on Page 19-5

Interfaces at the head station	
Number of slots for interface modules	4
Connection medium	Via interface modules, flexible media support
Number of Ethernet ports	

Interfaces at the head station (Fortsetzung)

FL SWITCH GHS 12G/8 head station	4 x Gigabit fiber optic ports in SFP format 8 x Gigabit copper ports in RJ45 format 8 x 100 Mbps ports via FL IF interface modules
FL SWITCH GHS 4G/12 head station	4 x Gigabit fiber optic ports in SFP format or Gigabit copper ports in RJ45 format 4 x 100 Mbps copper ports in RJ45 format 8 x 100 Mbps ports via FL IF interface modules
V.24 (RS-232) communication interface	
Connection format	Mini-DIN female connector
Floating alarm contact	
Number	2
Voltage	24 V DC
Current carrying capacity	100 mA, maximum
Digital inputs	
Number	2
Voltage for sensor supply	24 V DC
Current	100 mA, maximum

Interfaces on the extension module

Number of slots for interface modules	4
Connection medium	Via interface modules, flexible media support
Number of Ethernet ports	8
System interface for extension module	Incoming system bus interface
Transmitted signals	Supply voltage, control signals, data

RJ45 interfaces via FL IF ...

Number	2
Connection format	8-pos. RJ45 female connector on the module
Connection medium	Twisted-pair cable with a conductor cross section of 0.14 mm^2 to 0.22 mm^2
Cable impedance	100 Ohm
Transmission speed	10/100 Mbps
Maximum network segment expansion	100 m

RJ45 interfaces – Power over Ethernet IEEE 802.3af via FL IF ...

Number	2
Connection format	8-pos. RJ45 female connector on the switch
Connection medium	Twisted-pair cable with a conductor cross section of 0.14 mm^2 to 0.22 mm^2
Cable impedance	100 Ohm
Transmission speed	10/100 Mbps
Maximum network segment expansion	100 m
Connection of the PoE supply	Via COMBICON; maximum conductor cross section = 2.5 mm^2
Nominal value	48 V DC (SELV/PELV)
Permissible voltage range	45.5 V DC to 53 V DC

RJ45 interfaces – Power over Ethernet IEEE 802.3af via FL IF ... (Fortsetzung)

Test voltage	500 V AC for one minute
Maximum current consumption on US at 48 V DC	900 mA
Typical power consumption	40 W

Ethernet interface (SC) – Multi-mode via FL IF ...

Number	2
Connection format	SC duplex female connector on the switch
Wavelength	1300 nm
Laser protection	Class 1 according to DIN EN 60825-1:2001-11
Minimum transmission length including 3 dB system reserve	6.4 km fiberglass with F-G 50/125 0.7 dB/km F1200 2.8 km fiberglass with F-G 50/125 1.6 dB/km F800 10 km fiberglass with F-G 62.5/125 0.7 dB/km F1000 3.0 km fiberglass with F-G 62.5/125 2.6 dB/km F1000
(Average) dynamic transmission power (fiber type) in link mode	
Minimum	-23.5 dBm (50/125 µm)/-20 dBm (62.5/125 µm)
Maximum	-14 dBm (50/125 µm)/-14 dBm (62.5/125 µm)
Static transmission power (fiber type)	
Minimum	-20.5 dBm (50/125 µm)/-17 dBm (62.5/125 µm)
Maximum	-11 dBm (50/125 µm)/-11 dBm (62.5/125 µm)
Minimum receiver sensitivity	-31 dBm (dynamic)/-28 dBm (static)
Maximum overrange	-14 dBm (dynamic)/-11 dBm (static)
Transmission speed	100 Mbps

Ethernet interfaces (SC) – Single mode via FL IF ...

Number	2
Connection format	SC duplex female connector on the switch
Wavelength	1300 nm
Laser protection	Class 1 according to DIN EN 60825-1:2001-11
Minimum transmission length including 3 dB system reserve	36 km fiberglass with F-G 9/125 0.36 dB/km 32 km fiberglass with F-G 9/125 0.4 dB/km 26 km fiberglass with F-G 9/125 0.5 dB/km
(Average) dynamic transmission power (fiber type) in link mode	
Minimum	-15.0 dBm (9/125 µm)
Maximum	-8.0 dBm (9/125 µm)
Minimum receiver sensitivity	> -31 dBm (9/125 µm)
Maximum overrange	> -7 dBm (9/125 µm)
Transmission speed	100 Mbps

Ethernet interfaces – SCRJ with optical diagnostics via FL IF ...

Number	2 (FL IF 2POF SCRJ-D)
Connection format	SC-RJ female connectors on the interface module
Data transmission rate	10/100 Mbps (100 Mbps according to PROFINET standard)
Wavelength	660 nm
Laser protection	Class 1 according to DIN EN 60825-1
Minimum cable length	1 m

Ethernet interfaces – SCRJ with optical diagnostics via FL IF ... (Fortsetzung)

Transmission length including 3 dB system reserve	50 m polymer fiber with F-K 980/1000 230 dB/km at 10/100 Mbps, maximum 100 m HCS fiber with F-S 200/230 8 dB/km at 100 Mbps, maximum
(Average) dynamic transmission power (fiber type) in link mode	
Minimum	-8.0 dBm (980/1000 µm)
(Average) dynamic receiver sensitivity (fiber type) in link mode	
Minimum	-23.0 dBm (980/1000 µm)
Optical overrange	1.0 dBm (980/1000 µm)

Cable lengths

Twisted pair	100 m
Polymer fiber (POF)	Depends on the interface module 1 m, minimum
HCS	Depends on the interface module
Fiberglass 1300 nm (multi-mode)	6400 m with fiberglass with F-G 50/125 0.7 dB/km F1200 2800 m with fiberglass with F-G 50/125 1.6 dB/km F800 10,000 m with fiberglass with F-G 62.5/125 0.7 dB/km F1000 3000 m with fiberglass with F-G 62.5/125 2.6 dB/km F600
Fiberglass 1300 nm (single mode)	36,000 m with fiberglass with F-G 9/125 0.36 dB/km 32,000 m with fiberglass with F-G 9/125 0.4 dB/km 26,000 m with fiberglass with F-G 9/125 0.5 dB/km

Mechanical tests

Shock test according to IEC 60068-2-27	Operation: 25g, 11 ms period, half-sine shock pulse Storage/transport: 50g, 11 ms period, half-sine shock pulse
Vibration resistance according to IEC 60068-2-6	Operation/storage/transport: 5g, 10 - 150 Hz, Criterion 3
Free fall according to IEC 60068-2-32	1 m

Conformance with EMC Directives

Noise emission according to EN 55011	Class A
Warning: The limit values of the electromagnetic noise emission according to EN 55011, Class A are only observed by the module if it is installed in a grounded metal control cabinet.	
Radio interference field strengths according to EN 55022	Class A
Electrostatic discharge (ESD) according to EN 61000-4-2	Class 3; Criterion B
Electromagnetic fields according to IEC 61000-4-3	10 V/m; Criterion A
Conducted interference according to IEC 61000-4-6	10 V_{RMS}; Criterion A
Fast transients (burst) according to IEC 61000-4-4	Data lines: 1 kV; Criterion A Power supply lines: 2.2 kV; Criterion B
Surge voltages according to IEC 61000-4-5	Data lines: ±1 kV asymmetrical; Criterion B Power supply lines: ±0.5 kV symmetrical/asymmetrical; Criterion B

19.1.1 Revision history of this user manual

Differences between this version and previous versions

Rev. 00 - First version
Rev. 01: DHCP relay agent, routing, devices, and display codes added

19.2 Typical current consumption - GHS (example)

Typical module current consumption	
FL SWITCH GHS [1]	400 mA
FL FXT [2]	350 mA
FL IF 2TX VS-RJ ... [3]	0 mA
FL IF 2HCS 100 ... [4]	100 mA
FL IF 2FX (SM) SC or ST ... [5]	200 mA
FL IF 2PSE ...	30 mA (from GHS, additional 850 mA, maximum from external 48 V PoE supply)
FL IF 2POF SCRJ-D	200 mA

Example structures

Station with 2 FX modules and 2 TX modules

350 mA [1] + (2 x 200 mA [5]) + (2 x 0 mA [3]) = 750 mA

19.3 Ordering data

19.3.1 Ordering data - GHS

Products

Description	Order designation	Order No.	Pcs. / Pkt.
Gigabit Modular Switch	FL SWITCH GHS 12G/8 FL SWITCH GHS 4G/12	2989200 2700271	1
Gigabit Modular Switch with integrated Layer 3 function	FL SWITCH GHS 12G/8-L3 FL SWITCH GHS 4G/12-L3	2700787 2700786	
Extension module with four slots for eight ports	FL FXT	2989307	1
Plug-in parameterization memory with MRP manager function, 256 MB SD Flash	FL SD FLASH/MRM	2700270	1
Plug-in parameterization memory, 256 MB SD Flash	FL SD FLASH	2988120	1
SFP slot module in SFP format - multi-mode	FL SFP SX	2891754	1
SFP slot module in SFP format - single mode	FL SFP LX	2891767	1
SFP slot module in SFP format - single mode long haul	FL SFP LX LH	2989912	1
Configuration cable, for connecting the switch to a PC, V.24 (RS-232)	PRG CAB MINI DIN	2730611	1
Universal end clamp	E/AL-NS 35	1201662	1
Interface module with 2 × twisted pair 10/100 Mbps in RJ45 format for connection on the **front**	FL IF 2TX VS-RJ-F	2832344	1
Interface module with 2 × twisted pair 10/100 Mbps in RJ45 format for connection on the **bottom**	FL IF 2TX VS-RJ-D	2832357	1
Interface module with 2 × fiberglass (multi-mode) 100 Mbps in SC format for connection on the **front**	FL IF 2FX SC-F	2832412	1
Interface module with 2 × fiberglass (multi-mode) 100 Mbps in SC format for connection on the **bottom**	FL IF 2FX SC-D	2832425	1
Interface module with 2 × fiberglass (multi-mode) 100 Mbps in ST/BFOC format for connection on the **bottom**	FL IF 2FX ST-D	2884033	1
Interface module with 2 × fiberglass (single mode) 100 Mbps in SC format for connection on the **front**	FL IF 2FX SM SC-D-F	2832205	1
Interface module with 2 × twisted pair 10/100 Mbps in RJ45 format and **Power over Ethernet** for connection on the **front**	FL IF 2PSE-F	2832904	1
Interface module with 2 × polymer fiber 10/100 Mbps in SC-RJ format for connection on the **bottom** and **optical diagnostics**	FL IF 2POF SCRJ-D	2891084	1

19.3.2 Accessories

Description	Order designation	Order No.	Pcs. / Pkt.
RJ45 connector with additional latching	VS-08-T-G-RJ45/IP20	1652295	5
Gray RJ45 connector set for linear cable	FL PLUG RJ45 GR/2	2744856	2
Green RJ45 connector set for crossed cable	FL PLUG RJ45 GN/2	2744571	2
Assembly tool for RJ45 connectors	FL CRIMPTOOL	2744869	1
Network monitoring with HMI/SCADA systems	FL SMNP OPC SERVER	2832166	1
Angled patch connector with eight RJ45 CAT5e network connections including Layer 1 security elements	FL PF SEC 8TX	2832690	1
Angled patch connector with two RJ45 CAT5e network connections	FL PF 2TX CAT5E	2891165	1
Angled patch connector with eight RJ45 CAT5e network connections	FL PF 8TX CAT5E	2891178	1

Description (Fortsetzung)	Order designation	Order No.	Pcs. / Pkt.
Angled patch connector with two RJ45 CAT6 network connections	FL PF 2TX CAT 6	2891068	1
Angled patch connector with eight RJ45 CAT6 network connections	FL PF 8TX CAT 6	2891071	1
Patch cable, CAT**6**, pre-assembled, 0.3 m long	FL CAT6 PATCH 0,3	2891181	10
Patch cable, CAT**6**, pre-assembled, 0.5 m long	FL CAT6 PATCH 0,5	2891288	10
Patch cable, CAT**6**, pre-assembled, 1.0 m long	FL CAT6 PATCH 1,0	2891385	10
Patch cable, CAT**6**, pre-assembled, 1.5 m long	FL CAT6 PATCH 1,5	2891482	10
Patch cable, CAT**6**, pre-assembled, 2.0 m long	FL CAT6 PATCH 2,0	2891589	10
Patch cable, CAT**6**, pre-assembled, 3.0 m long	FL CAT6 PATCH 3,0	2891686	10
Patch cable, CAT**6**, pre-assembled, 5.0 m long	FL CAT6 PATCH 5,0	2891783	10
Patch cable, CAT**6**, pre-assembled, 7.5 m long	FL CAT6 PATCH 7,5	2891880	10
Patch cable, CAT**6**, pre-assembled, 10 m long	FL CAT6 PATCH 10	2891887	10
Patch cable, CAT**6**, pre-assembled, 12.5 m long	FL CAT6 PATCH 12,5	2891369	5
Patch cable, CAT**6**, pre-assembled, 15 m long	FL CAT6 PATCH 15	2891372	5
Patch cable, CAT**6**, pre-assembled, 20 m long	FL CAT6 PATCH 20	2891576	5
Patch cable, CAT5, pre-assembled, 0.3 m long	FL CAT5 PATCH 0,3	2832250	10
Patch cable, CAT5, pre-assembled, 0.5 m long	FL CAT5 PATCH 0,5	2832263	10
Patch cable, CAT5, pre-assembled, 1.0 m long	FL CAT5 PATCH 1,0	2832276	10
Patch cable, CAT5, pre-assembled, 1.5 m long	FL CAT5 PATCH 1,5	2832221	10
Patch cable, CAT5, pre-assembled, 2.0 m long	FL CAT5 PATCH 2,0	2832289	10
Patch cable, CAT5, pre-assembled, 3.0 m long	FL CAT5 PATCH 3,0	2832292	10
Patch cable, CAT5, pre-assembled, 5.0 m long	FL CAT5 PATCH 5,0	2832580	10
Patch cable, CAT5, pre-assembled, 7.5 m long	FL CAT5 PATCH 7,5	2832616	10
Patch cable, CAT5, pre-assembled, 10.0 m long	FL CAT5 PATCH 10	2832629	10
Polymer fiber connectors (two duplex connectors in the set)	PSM-SET-SCRJ-DUP/2-POF	2708656	1
Polishing set for polymer fiber connectors (required to assemble polymer fiber connectors)	VS-SCRJ-POF-POLISH	1656673	1
Fiber optic polymer fiber cable for indoor installation	PSM-LWL-KDHEAVY	2744319	1
HCS fiber connectors (two duplex connectors in the set)	PSM-SET-SCRJ-DUP/2-HCS	2313070	1
Tool kit for HCS connectors (required to assemble HCS fiber connectors)	PSM-HCS-KONFTOOL/SCRJ	2708876	1
Fiber optic HCS cable for indoor installation	PSM-LWL-HCS-RUGGED-200/230	2799885	1
Fiber optic HCS cable for outdoor installation	PSM-LWL-HCSO-200/230	2799445	1
HCS GI cable, duplex, 200/230 µm, for indoor installation, suitable for use in drag chains, compliant with PROFINET installation guidelines, sold by the meter without connectors	FL FOC PN-C-HCS-GI-200/230	2313410	1
HCS GI cable, duplex, 200/230 µm, for indoor installation, suitable for use in drag chains, compliant with PROFINET installation guidelines, cable with pre-assembled connectors	FL FOC PN-C-HCS-GI	2313504	1

HOTLINE:

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

☎ + 49 - 5281 - 9-462888