Indu-Sol GmbH – Specialist in Industrial Networks

PROmesh B8+F

User Manual

Layer-2-Managed Industrial Ethernet-Switch

PROFIBUS PROFINET INDUSTRIAL ETHERNET CAN DeviceNet SafetyBUS p ASi INTERBUS EMC WIRELESS

Indu-Sol GmbH

Blumenstraße 3

042626 Schmölln

Tel.: +49 (0)34491 / 580 0

Fax: +49 (0)34491 / 580-499

E-mail: info@indu-sol.com

Web: https://www.indu-sol.com

Our **technical support** team can be reached at +49 (0)34491 / 58 18 14, on workdays between 7:30 - 16:30 (CET). Or you can send us an e-mail to: support@indu-sol.com

Your system is standing still? You can reach our emergency service team around the clock at the telephone number:
+49 (0)34491 / 580 0.

Revision overview

Date	Revision	Change(s)
20.02.2023	0	First version

W A R N U N G

Commissioning and operation of this unit may only be carried out by qualified personnel. Qualified personnel in the sense of the safety instructions in this manual are persons who are authorised to commission, earth and label equipment, systems and circuits in accordance with safety engineering standards.

Improper use or configuration of the ***PROmesh P8+F*** in the network can lead to serious physical injury as well as damage to property and material, also due to uncontrolled machine movements.

Table of contents

Revision overview		3
Table of contents		4
1	General information	6
1.1	Overview of the *PROmesh P8+F* - Scope of Functions	6
1.2	Scope of delivery	7
1.3	Safety instructions	7
2	Connections and status indicators on the unit	8
2.1	Device connections	8
2.2	Installation	9
2.3	Installation	9
2.4	Power supply connection and error relay	10
2.5	LED displays	12
2.6	Reset button	12
2.7	Network integration & commissioning	13
2.7.1	Data ports	13
2.7.2	Media selection & connection	13
2.7.3	Wiring	13
2.8	Network topologies & redundancy	14
2.8.1	Network topologies	14
2.8.2	Ring structure	14
3	Web application	16
3.1	Preparations	16
3.2	System Login	17
3.3	Web interface	17
3.4	Start	18
3.5	System information	20
3.6	Diagnosis	20
3.6.1	Line diagnosis	20
3.6.2	Leakage current	22
3.6.3	Network statistics	23
3.6.4	Neighbourhood Detection (LLDP)	24
3.6.5	Port Mirroring	25
3.6.6	Alarm trigger	25
3.6.7	Messages	27
3.7	PROFINET	28

3.8	Switching	28
3.8.1	Port configuration	29
3.8.2	Quality of Service	30
3.8.3	VLAN	31
3.8.4	Bandwidth control	34
3.8.5	Link aggregation	34
3.9	Redundancy	36
3.9.1	MRP	36
3.9.2	RSTP	37
3.9.3	MSTP	40
3.10	System configuration	40
3.10.1	Unit information	41
3.10.2	IP configuration	42
3.10.3	Password	43
3.10.4	Time setting	43
3.10.5	SNMP	44
3.10.6	Access time	45
3.10.7	Backup	46
3.10.8	Restoration	46
3.10.9	Firmware update	46
3.10.10	Factory settings	48
3.10.11	Restart	48
3.11	Support	48
3.12	Troubleshooting tips	48
4	Technical specification en	49

1 General information

Please read this document thoroughly from beginning to end before you start installing and commissioning the device.

1.1 Overview of the *PROmesh P8+F* - Scope of Functions

The ***PROmesh P8+F*** is an industrial Ethernet switch with management and PROFINET functionality that can be configured easily and conveniently via a web application. It supports the effective setup of all network topologies, such as bus, star, and ring structure in your plant, with its comprehensive functions with Store & Forward technology.

Features :

- Web application for configuration
- Reverse polarity protected supply 12-48V DC
- Line diagnosis
- Leakage current monitoring
- Port statistics (network load in ms, errors, discards)
- Alarm management
- 8 x 10/100/1000 Mbit/s RJ45
- Switch technology: Store & Forward
- MAC address table: 16K (16384 addresses)
- PROFINET Conformance Class B
- PROFINET Netload Class III
- Quality of Service (QoS) with eight priority queues
- Prioritisation according to Class of Service (COS), Type of Service (TOS) or port priority
- Limitation of incoming and outgoing packets
- Port Mirroring (Rx / Rx and Tx packets)
- Port-based VLAN with 4096 possible VLAN IDs
- Simple Network Time Protocol (SNTP) Client and NTP Server
- Simple Mail Transfer Protocol (SMTP)
- Internet Group Management Protocol - Snooping (IGMP Snooping)
- Dynamic Host Configuration Protocol (DHCP) Client Function
- Simple Network Management Protocol (SNMP), v1, v2c, v3
- Updating, saving and backing up the system configuration via web interface, TFTP and memory card

1.2 Scope of delivery

The scope of delivery includes the following individual parts:

- ***PROmesh*** P8+F
- 5-pole pluggable terminal block, 2.5mm² (power supply and alarm contact)
- User Quick Start Guide (Hardcopy)
- SD card, for backup and update

Please check the contents of your delivery for completeness before commissioning. If you have any questions, please contact our technical support team immediately before commissioning.

Before using the device for the first time, insert the external memory card into the corresponding slot on the back of the unit (see figure 1).

1.3 Safety instructions

Before putting the unit into operation, check that it is in perfect condition externally. If you suspect damage, return the PROmesh P8+F to your supplier immediately and do not put the unit into operation. If you have any questions, our technical support team will be happy to assist you.

The ***PROmesh P8+F*** has been developed for use in PROFINET applications according to Conformance Class B. To fully support the PROFINET standards, also note the selection of the data lines used according to the standard.

Always observe the technical specification of the unit to ensure safe and optimal use. The unit was developed for protective environments according to IP20. Take appropriate measures in deviating environments to ensure proper operation of the unit.

Do not open the housing under any circumstances. No serviceable parts have been installed. Unauthorised opening of the housing will invalidate any warranty claims.

2 Connections and status indicators on the unit

2.1 Device connections

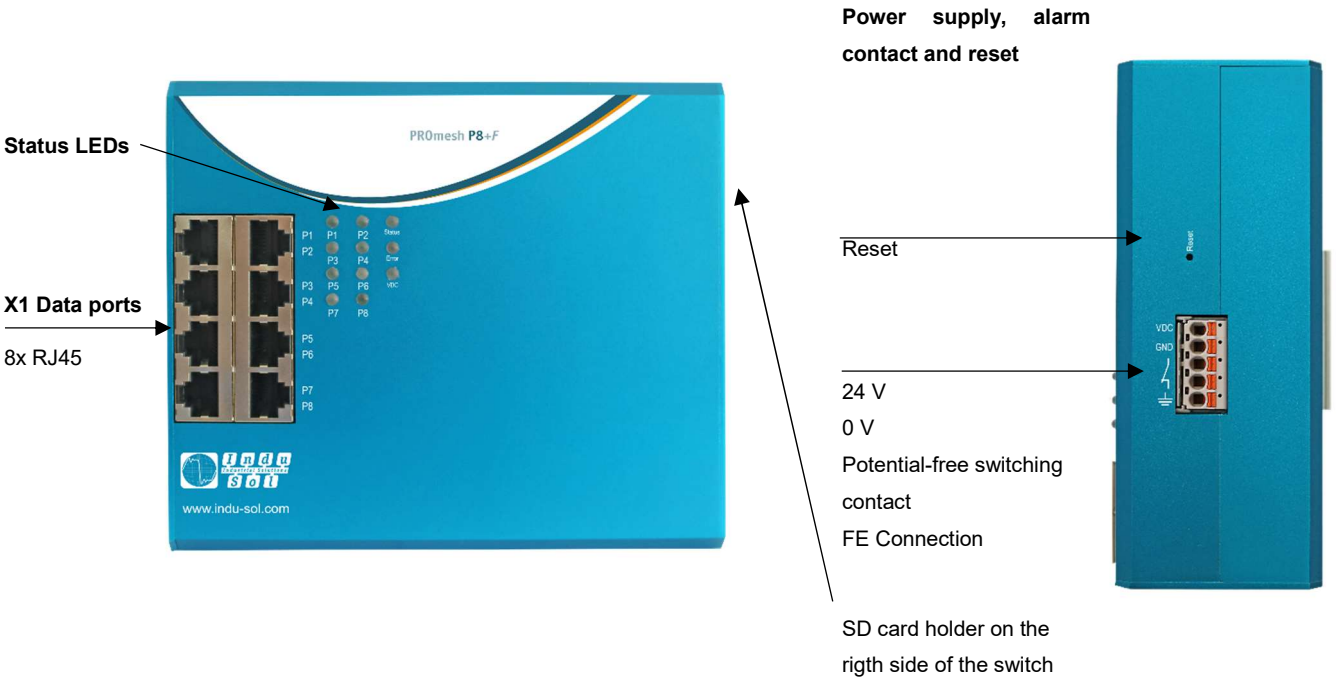

Figure 1: Unit connections

2.2 Installation

The PROmesh P8+F is designed for individual use in control cabinets of various types and can be mounted on a standard 35mm DIN rail.

Only use the existing top-hat rail fastening for mounting the unit or, if necessary, purchase appropriate spare parts to ensure sufficient electrical contact and the mechanical load capacity of the unit.

2.3 Installation

The ***PROmesh P8+F*** is mounted vertically in the control cabinet on a 35 mm top-hat rail according to DIN EN 60715.

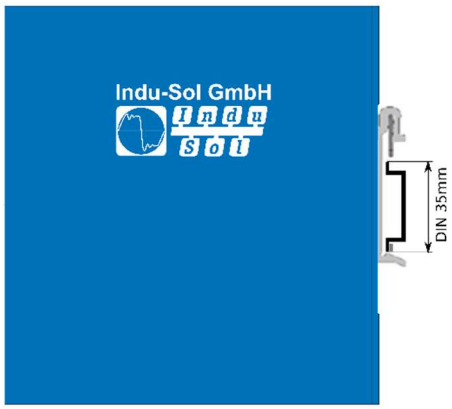

Figure 2: Side view with connection terminal on the right

For correct installation, the following distances to other assemblies must be observed:

- To the left and right: 20 mm
- Upwards and downwards: 50 mm

The assembly and disassembly of the unit is shown in figure 3.

Figure 3: Mounting and dismounting on the top-hat rail

Do not mount the ***PROmesh P8+F switches*** directly next to devices that generate strong electromagnetic interference fields, e.g. transformers, contactors, frequency converters, etc.

Do not mount the ***PROmesh P8+F switches*** directly next to heat-generating devices and protect the switch from direct sunlight to avoid unwanted heating. Protect the PROmesh P8+F from additional heat radiation and observe the approved storage and operating temperature range.

2.4 Power supply connection and error relay

Operate your ***PROmesh P8+F*** with a nominal voltage of DC 12 V to 48 V. Connect the power supply to the correspondingly marked terminals of the supplied 5-pole terminal block adapter (VDC, GND). The power supply must comply with UL60950-1/UL62368-1, Class 2 (NEC), limited energy source (UL61010-1).

The 5-pin 2.5mm² terminal block on the top of the unit is assigned as follows:

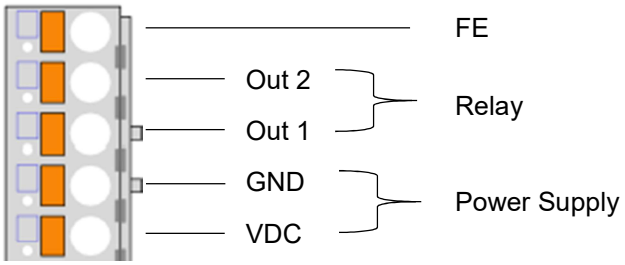

Figure 4: Connector terminal block assignment

The listed labels are also included on the terminal block supplied.

A potential-free error relay contact (break contact) is located at the OUT terminals inside the unit. The relay serves as an alarm receiver and can be linked to various alarm triggers in the software. Depending on the configuration, the relay contact then opens, for example, in the event of a power failure or a change in the status of the port.

2.5 LED displays

There are four diagnostic LEDs on the front panel of the switch.

In addition, each of the 8 data ports has a status LED.

The LEDs show the most important diagnostic information about the device and connection status of the PROmesh P8+F in your PROFINET network (see Table 1).

LED	Status	Meaning
VDC	Green	Voltage at connection sufficient
	Off	Voltage at connection insufficient
Status	Green	Active PROFINET connection to the controller
	Yellow	No PROFINET connection to the controller
Error	Red	Configured alarm active
	Off	No configured alarm active
LED Port 1-8 (green)	Off	No link
	Flashing	Link + data exchange (flashing speed reflects linkspeed)
	On	Link

Table 1: LED- Functions

2.6 Reset button

If the PROmesh P8+F should experience any unforeseen problems that make it inaccessible, the reset button can be used. With its help, the PROmesh P8+F can either be restarted or reset to its factory settings. The following procedure is necessary for this:

- Restart the unit: Press the reset button for 1 second.
- Reset to factory settings: Press the reset button until all LEDs go out (approx. 10s).

2.7 Network integration & commissioning

2.7.1 Data ports

The ***PROmesh P8+F*** is equipped with 8 data ports which, in conformity with PROFINET standard 2.4, enable data transmission at up to 1 Gbit/s. The actual data rate is negotiated by the device using auto-negotiation.

2.7.2 Media selection & connection

The PROmesh P8+F has 8 data ports for connecting RJ-45 copper cables.

When designing, selecting, assigning and assembling your data cable, pay attention to the applicable standards and fixed connections in the connector application to ensure the maximum possible cable length and cascading of network segments according to your media type (copper, fibre optic, ect.).

2.7.3 Wiring

Use twisted pair cables of category 5 (Cat 5) or higher with a maximum cable length of up to 100 m to connect your PROmesh P8+F via the existing RJ-45 data ports. To improve the shielding, we recommend the PROFINET RJ45 connectors from Indu-Sol.

2.8 Network topologies & redundancy

By using different protocols, the devices of the PROmesh ***product family*** can be used in redundant networks, such as meshed networks or rings, in addition to being used in star-shaped switched Ethernet networks.

2.8.1 Network topologies

Classic Ethernet star structures (s. Figure 5) can be connected with the ***PROmesh*** P8+F ***switches*** without additional configuration. The devices are immediately ready for use.

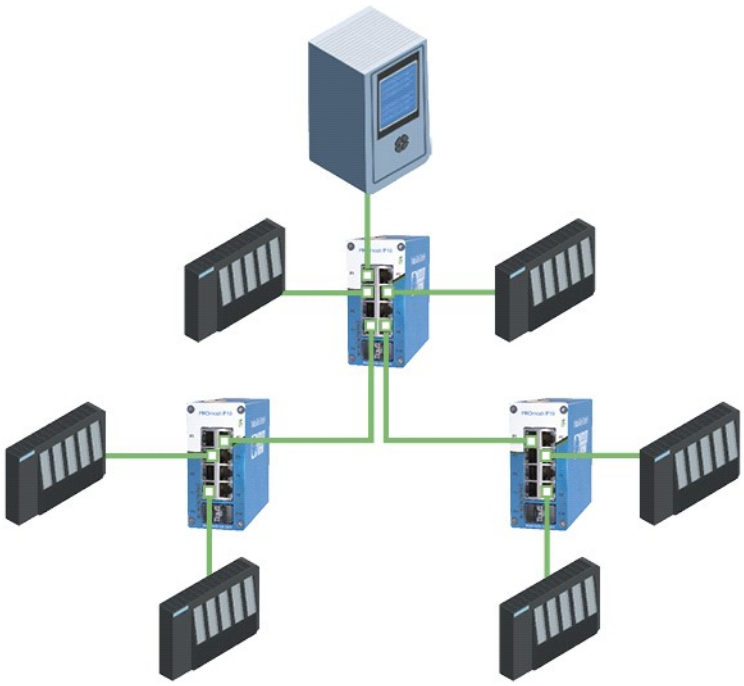

Figure 5: ***PROmesh P8+F*** in a star-shaped network

2.8.2 Ring structure

The ***PROmesh P8+F*** supports the IEC 62439 standard and thus enables deterministic reconfiguration of information forwarding in simple redundancy (ring topologies, see figure 6). Depending on the size of your system, reconfiguration times of up to 200 ms are possible.

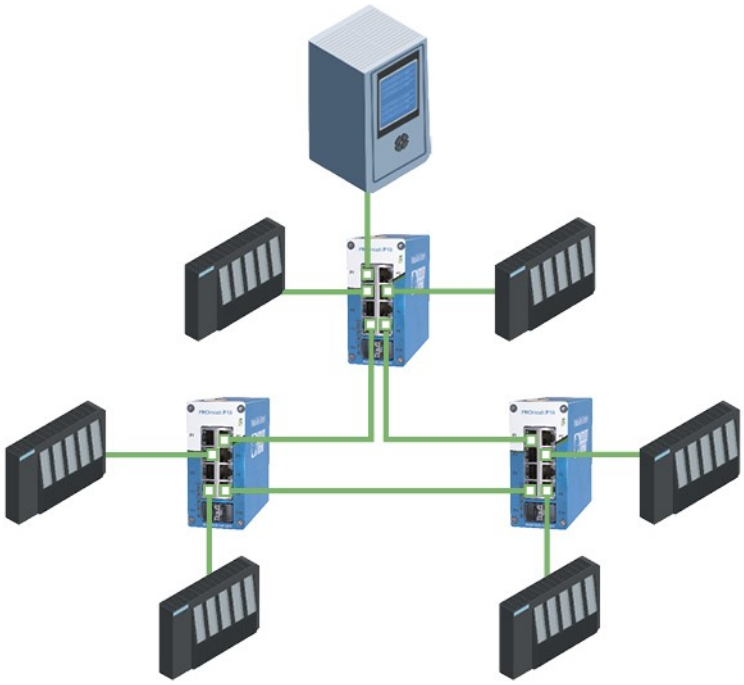

Figure 6: *PROmesh P8+F* in a ring-shaped network

3 Web application

The ***PROmesh P8+F switches*** are equipped with a modern web interface that can be configured conveniently from any web browser.

3.1 Preparations

Before using web management, install the ***PROmesh P8+F*** switch on the network and make sure that the PC intended for configuring the switches can access the switch via the web browser. The PROmesh P8+F and the client PC to be connected must be in the same IP address range and IP subnet. To do this, you must assign a corresponding IP address to your PROmesh P8+F for the first time.

When the unit is delivered, the following IP address, subnet mask, administrator user name and administrator password are set:

- IP address: **0.0.0.0**
- Subnet mask: **0.0.0.0**
- Gateway: **0.0.0.0**
- Username: **admin**
- Password: **admin**

Make sure to change the factory-set password when logging in for the first time. You are responsible for documenting this password and protecting it from unauthorised access.

You can easily set your intended user addresses with the **Indu-Sol ServiceTool.** This is included in the scope of delivery or is available for free download via the following link:
https://sdx.indu-sol.com/s/CtYtsHNW73Z3KCa

Our software is updated regularly. Please make sure you have the latest version.

After installing and opening the software, establish a network connection from your computer to a port of the switch and scan the system with the search setting *PROFINET device.* You can then make the appropriate entries in the input mask and save them.

If you include the switch in a PROFINET system in the hardware configuration of the control, the corresponding address settings are then made automatically via this.

As an alternative to administrator access, user access with lower authorisations and adapted menu navigation is available. The user has no access to the functions Switching, PROFINET and Redundancy as well as their sub-items. Furthermore, the submenus for system configuration are restricted. The access data for this are:

- username: **use**r
- Password: **user**

3.2 System Login

1. Start a web browser on your computer.
2. Enter the IP address of the ***PROmesh P8+F*** switch you are using in the address line of the web browser and confirm your entry with the *Enter* key.
3. The login screen of the unit now appears on the screen.

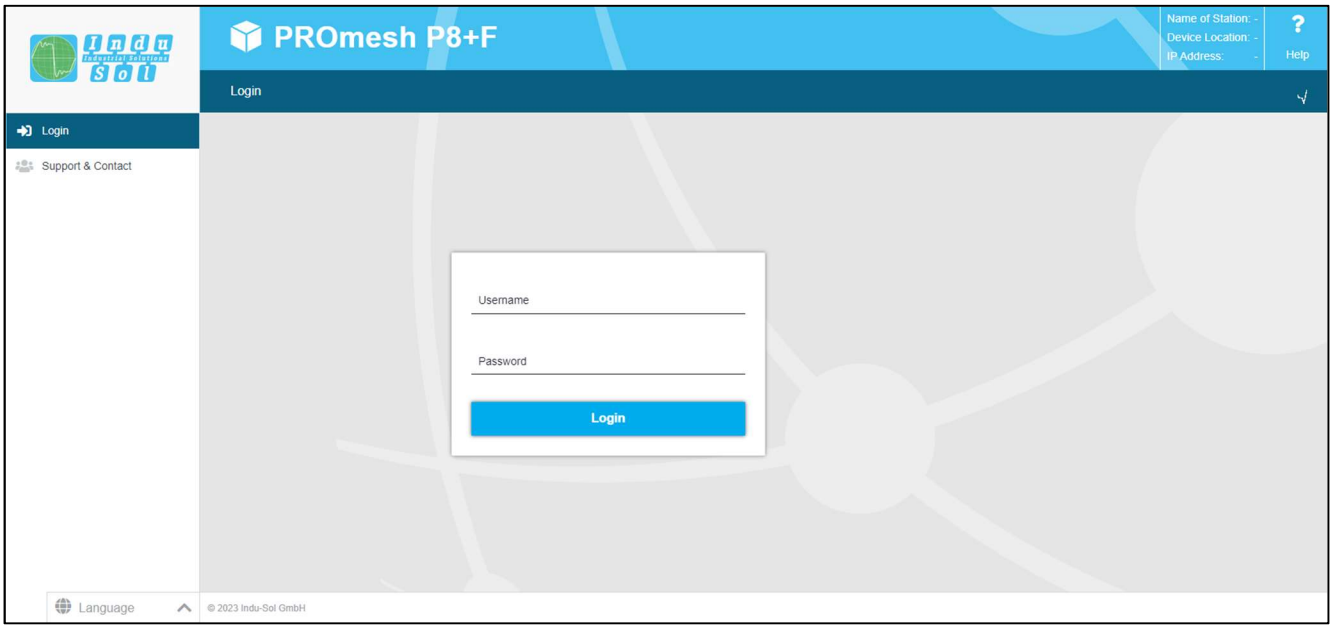

Figure 7: Login mask

4. Select the desired menu language (DE / EN). This can be changed at any time in any menu of the web interface.
5. Then enter the user name and password.
6. By pressing the *Enter* key and clicking on *Login,* you can access the web interface of the switch.

3.3 Web interface

The following symbols are used in the web interface for a simple status display of the individual ports:

No error: The communication works flawlessly.

Warning: At least one communication error (discards, error) has occurred on the corresponding port, which has not yet led to a failure. The cause of these events should be located and corrected.

Error: A critical malfunction has occurred at the corresponding port, resulting in a communication interruption. Urgent action is required to eliminate the fault.

There is no communication at the respective port. Either no device is connected (possibly also line interruption) or no telegram traffic can be detected (serious disturbance in the network) or the devices are no longer communicating.

3.4 Start

After successful login, you will be taken to the main overview with the information bar, in which the unit name, installation location and IP address can be seen. Under the logout button at the right end of the bar, the current user is displayed. You can log out by pressing the button. The help button displays notes and explanations for the individual pages.

The port statistics provide you with an overview of the status of the existing ports since the switch was started or reset (history) and within the last minute (current). You can choose between two views. In the Overview view:

- Current partners
- Transmission speed
- Diagnostic messages

is displayed. In the Details view, in addition to the parameters of the overview:

- Mains load per s
- Discards
- Errors
- Line quality value

displayed.

The number of messages that have occurred is displayed in the message window. With a mouse click on the alarm bell, the entries in the message list are automatically called up. The messages as well as the counter status of the ports can be deleted with the corresponding buttons.

The leakage current overview displays the current value between the RJ45 ports and the top-hat rail of the unit. For this purpose, it is possible to switch between the display of the peak value (Peak) and the effective value (RMS). This information makes interference currents visible at an early stage, which can lead to direct communication disturbances.

In order to measure the leakage current correctly, the top-hat rail must have been earthed properly.

The selection in the menu bar allows you to call up the individual pages and make settings there. The menu items displayed are subdivided into further sub-items.

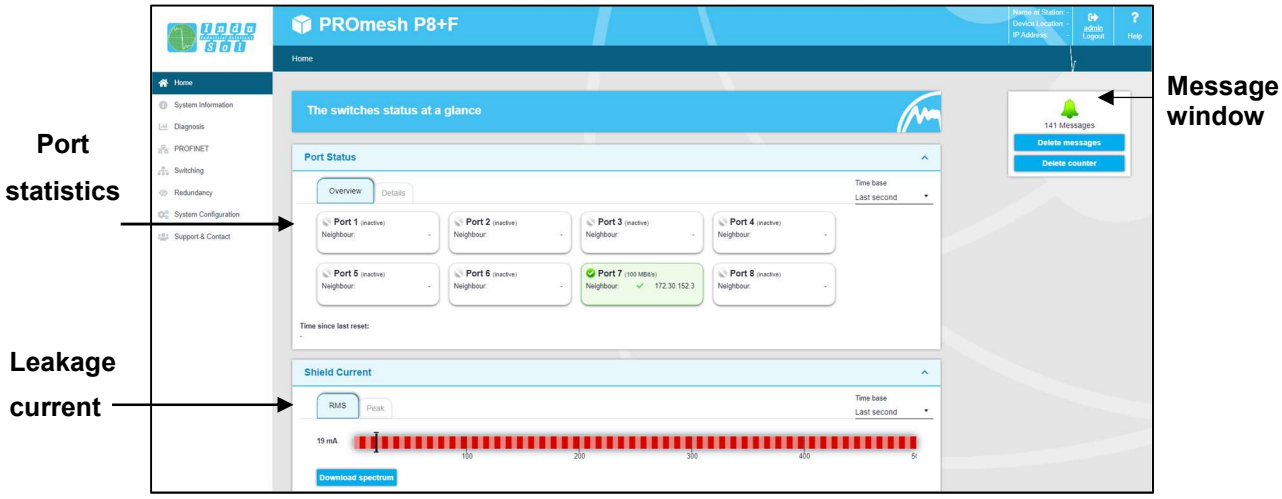

Figure 8: Start

3.5 System information

In addition to the unit information, an overview of the activated or deactivated protocols and functions is displayed under this menu item. By selecting the respective edit button, you can switch directly to the corresponding protocols and functions in order to make settings there.

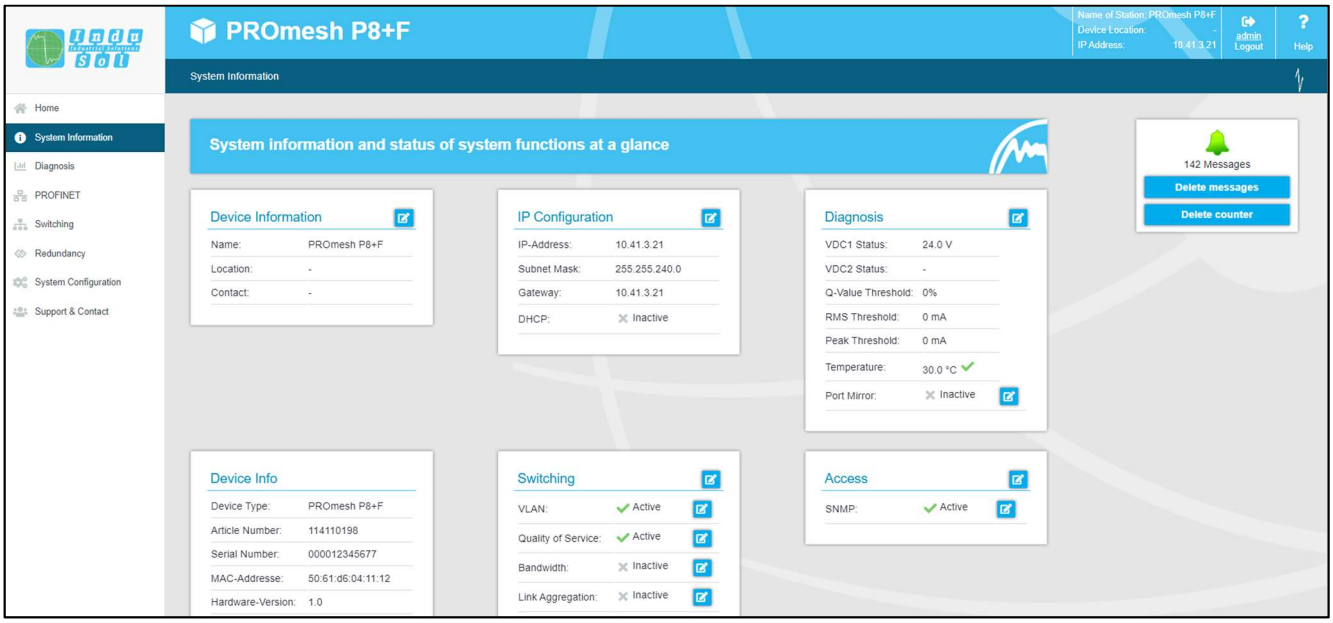

Figure 9: Status and diagnosis

3.6 Diagnosis

The Diagnostics page provides an overview of the status of configured alarm triggers (alarm trigger configured or not) for the individual recorded diagnostic data of the PROmesh P8+F. Furthermore, the status of topology detection and port mirroring is displayed.

3.6.1 Line diagnosis

The line diagnosis is available for ports 1 - 8. The quality of the connected connections is checked cyclically (every second). The line quality can lie between the values 100 and 0 %, whereby 0 % corresponds to a defective cable, i.e. no data exchange is possible.

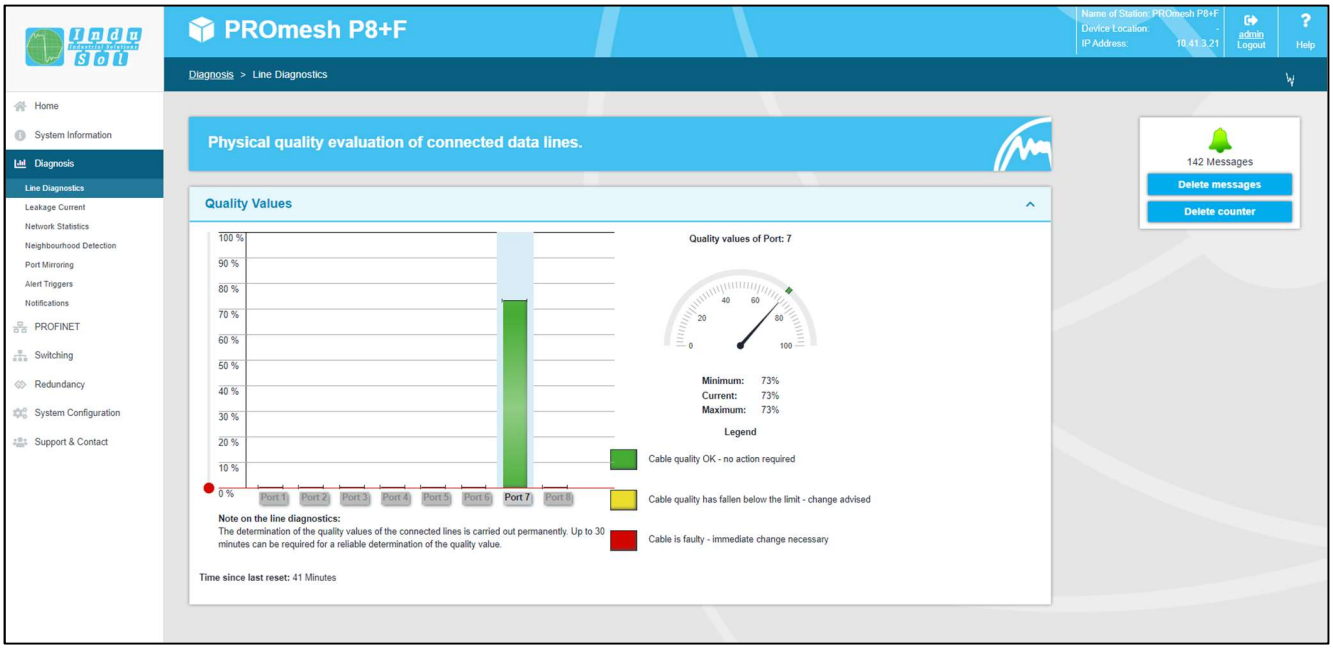

Figure 10: Quality value

Information Bar Chart

3 values are displayed per bar.

The grey coloured part of each bar shows its maximum value. The colour-saturated part, which is bordered by a black line, shows the current quality value. The coloured saturated part, which is bordered by a line with 2 arrows, shows the worst quality value of the connection so far. The colouring of the bars is based on this, which is done according to the traffic light colour principle green-yellow-red:

- Green: The line quality is OK, no measures are required.
- Yellow. The defined threshold value of 30 % has been undercut. The line quality is not sufficient. The connection should be checked at the next maintenance interval.
- Red: Data exchange is no longer possible. Check the plug contacts and the data line.

A cable designation can be stored for each port in the Port Configuration menu. This can be displayed with a mouse-over (move the mouse pointer over the port).

Miscellaneous

The threshold value, which colours the bar yellow and recommends checking the connection, can be adjusted by the user. It is not recommended to set the threshold below 30 %. In the Alarms menu, alarms can be defined for the line quality value, which send messages via relay, SNMP, PROFINET or e-mail if the value falls below a threshold.

3.6.2 Leakage current

The leakage current monitoring (Figure 11) makes it possible to permanently record and evaluate the sum of all shield currents of the PROFINET lines which are discharged via the device into the equipotential bonding system. For this purpose, in addition to the current value, the associated spectrum with the respective frequency components is indicated. With this function, the PROmesh series offers mechanisms for detecting EMC interference or coupling.

Other functions:

- Download of the frequency spectrum after a threshold value has been exceeded
- Switching the axes between decimal and logarithmic scaling

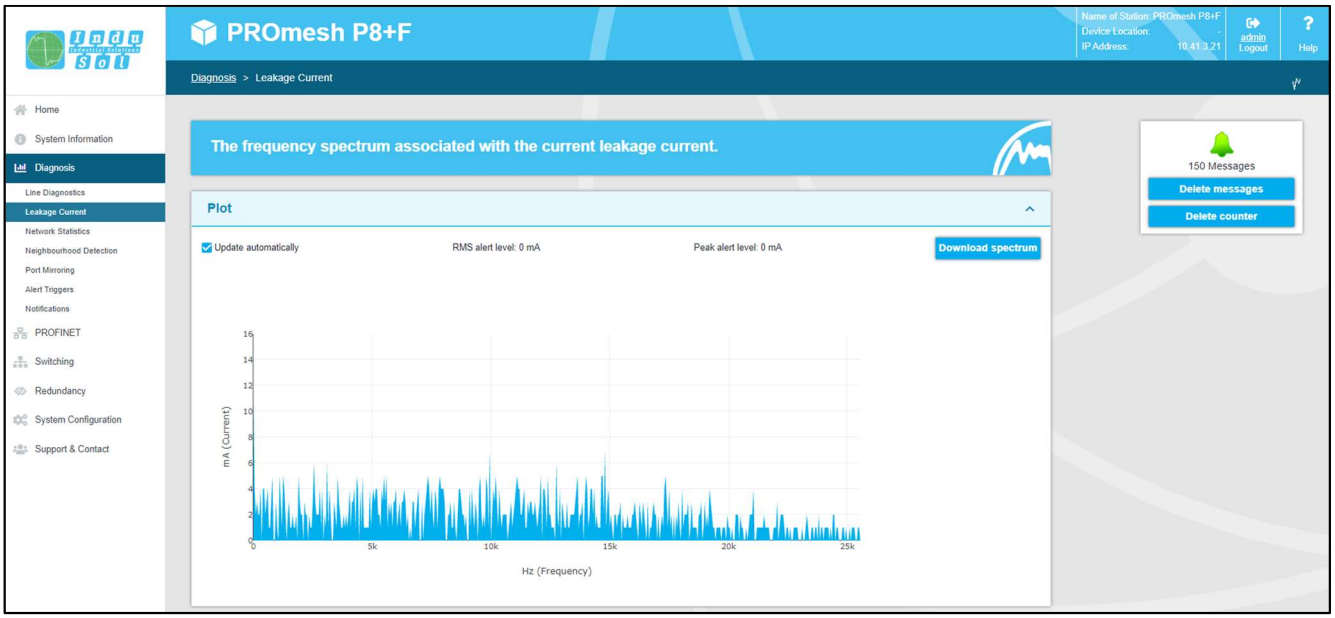

Figure 11: Leakage current

3.6.3 Network statistics

The Port Statistics page provides information about the data traffic of the individual ports. This information is useful for diagnostic purposes or in case of network problems.
In the main overview of the port statistics, the following information is provided for each port:

- Received data packets
- Data packets sent
- Maximum mains load
- CRC error (destroyed telegrams)
- Discards (rejected telegrams due to too much data)

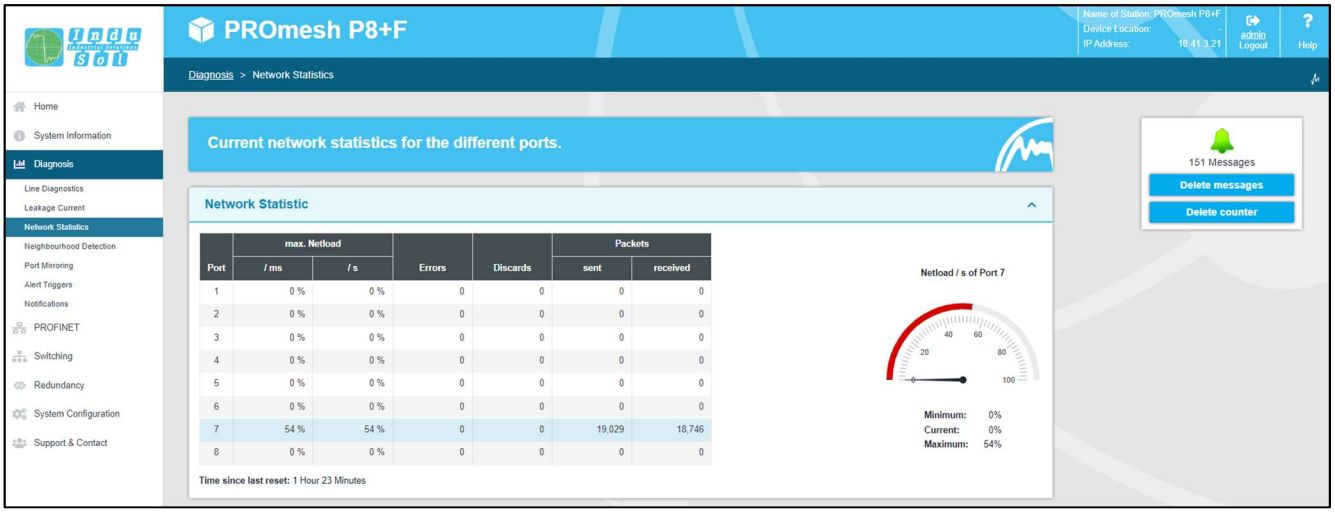

Figure 12: Port statistics

Resetting the values

In the upper right part of the web interface is the button "Clear counter". By pressing this button, the values of the table can be reset.

Detailed port statistics

In the statistics details, the size of the individual packets is recorded statistically up to various limit values. (up to 64, 127, 255, 511, 1023, or 1518 bytes).

A distinction is made between the sent packets:

- Number of unicast packets (packets to one receiver)
- Number of non-unicast packets

A distinction is made between the received packets:

- Number of all packages
- Total bytes received
- Number of fragments received

The line *Packets up to bytes* provides information about the number of packets in different sizes. Here the number of received packets up to 63, 127, 255, 511, 1023, or 1518 bytes in size is recorded.

In addition, parcel collisions are recorded and post:

- Late (a collision that occurs after more than 512 bits)
- Total

split. Such collisions and the associated data loss always occur when several participants want to send simultaneously on one medium.

3.6.4 Neighbourhood Detection (LLDP)

The Link Layer Discovery Protocol (LLDP) is a manufacturer-independent layer 2 protocol that offers the possibility to exchange information (addresses, names and descriptions) between neighbouring devices. An LLDP agent operates on every device that supports LLDP. This agent periodically sends information about its own status and receives information from neighbouring devices.

Since this is done independently, the LLDP is also called a one-way protocol.

The following information is compiled and sent by LLDP:

- Port name
- Device name
- IP address
- Device description

MAC table

The forwarding database provides information about which MAC address is connected to which port of the switch.

Settings

The LLDP interval parameter can be used to define the time intervals (in seconds) at which the device's own LLDP telegram is sent to the neighbouring devices. The default setting is 5 seconds.

3.6.5 Port Mirroring

Port mirroring is a method of simultaneously directing the traffic of one port (source) to a second port (destination) in networks and thus checking it. This means that the received and sent packets of the source port are duplicated to the monitoring port.

The monitoring of the source ports is done without influencing the data traffic of this port. The resulting mirror port can be connected to a LAN analyser or used for diagnostic and debugging purposes.

- Port and port name: All ports are displayed here in order to select a destination port and one or more source ports.
- Destination port: If port mirroring is activated, select a port on which the data is mirrored. The mirrored packets can be forwarded to exactly one destination port.
- Source port: Here you can select which ports are to be monitored and forward their packets to the destination port. It is possible to forward only sent packets (TX for transmit/send) to the destination port or to monitor both directions, i.e. sent (TX for transmit/send) and received (RX for receive/receive) packets. You can select a maximum of eight source ports at the switch. Select the respective checkbox to select a port.

After you have set the respective parameters, click on the Apply button to save and apply the settings.

3.6.6 Alarm trigger

The Alarms menu item is used to configure alarm triggers and alarm receivers. Alarms can be created for the following events:

- Changing the status of a port
- Temperature too high or too low
- Failure of a supply voltage
- MRP protocol event
- Exceeding of a leakage current
- Exceeding the network load on a port
- Incorrect connected neighbour (can only be configured via the configuration software)
- Falling below the line quality value
- Voltage value of the 24 V power supply too high or too low

The alarms created can be linked to one or more alarm receivers, these include:

- Error relay
- SNMP traps
- E-mail addresses
- PROFINET (only configurable via configuration software)

If one of the created alarms is detected and triggered, the software forwards the event to the corresponding alarm receiver and also documents the event as a syslog message.

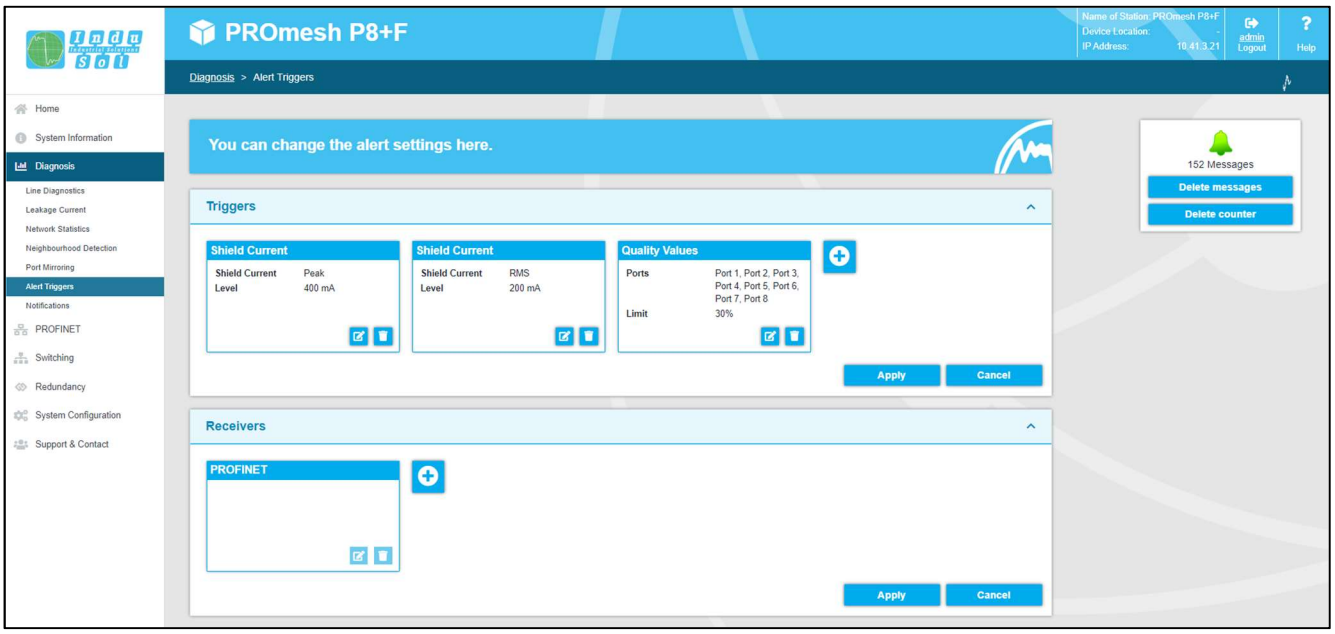

Figure 13: Alarm trigger

The configured alarm assignments are displayed in lists with consecutive ID.

- Alarm triggers with assigned receivers
- Alarm receiver with assigned triggers

Add and edit alarm triggers

By clicking on the button with the "+" symbol, new alarms and messages can be added. If alarms are already present, the user has the possibility to edit or delete them by clicking on the button. In the upper part of the "Alarm Trigger" pop-up, the user can select the different alarms. While creating and editing the alarms, the associated recipients can be selected in the lower part of the pop-up and linked to the alarm trigger in this way, provided the alarm recipients have already been defined.

Add and edit alarm receivers

By clicking on the button with the "+" symbol, new alarm receivers can be added. The relay is already present as an alarm receiver and cannot be deleted, but only linked to alarm triggers. In addition to this, the recipients e-mail, SNMP and PROFINET can also be selected. The associated alarm triggers can be linked to the current receiver in the lower part of the pop-up.

- With Simple Network Management Protocol (SNMP), error notifications are generated by the unit and sent unsolicited to a management station. Since the packets are not acknowledged, the unit cannot determine whether the manager has received the information.
- When using the e-mail function, the user can specify an e-mail address and an SMTP (Simple Mail Transfer Protocol) server. The unit sends an e-mail to the user when an alarm occurs. Optionally, authentication can be activated. For this, the necessary access data must be entered.
- Once the switch has been integrated and parameterised in a Profinet network, the "PROFINET" alarm receiver is permanently set in the system and cannot be changed in the device. The alarm triggers for the individual events are activated in the hardware configuration of the control unit. If a trigger is triggered, the switch sends an alarm message to the controller. This information can then be processed programmatically within the PLC.

3.6.7 Messages

The messages serve as an aid for the user to view status and error messages of the various functions. The messages are displayed in the overview with date and time, as well as a code, type, description and reference. Since the log entries are not stored in the unit, they are no longer available after a unit restart or a power interruption. To archive the messages permanently, it is possible to use an external syslog server or the SD card.

Statistics

This tab provides a summary of the individual error codes that have occurred and their frequency.

Settings

- Syslog server: To save the messages on a syslog server, activate this function. Enter the IP address of the syslog server in decimal point notation, select "File" under Media Type and save the settings using the Apply button. Please check whether the server is accessible and saves the messages in a file.
- Media type SD card: To save the messages on the SD card, make sure that an SD card is inserted. Then select "SD card" under Media type and save the settings using the Apply button.

Please check whether there is enough memory available on the SD card and whether the messages are saved in a file.

Resetting the entries

- The button "Delete entries" removes all entries from the table. The time at which the entries were deleted can then be viewed as the first entry with the description "Logfile reset by User!" and reference "logFileReset()".

3.7 PROFINET

The abbreviation Profinet stands for Process Field Network and refers to the open Industrial Ethernet standard for automation.

The device is developed as a Profinet IO device for connecting decentralised peripherals to a Profinet controller. The device supports Conformance Class B. On this page you can make the port settings for DCP and download the configuration file.

DCP settings:

- You can specify for each port whether it supports the Discovery and Configuration Protocol (DCP). With the help of DCP, the addresses and names in a Profinet IO system are distributed to the individual participants.

Additional information

The configuration file stored on this page is used to describe Profinet field devices. The file is written in General Station Description Markup Language (GSDML). The file serves as a basis for planning the configuration of a Profinet IO system.
Furthermore, the current status of the device in PROFINET, the assigned PROFINET name and its controller (if available) are displayed.

3.8 Switching

This page provides you with an overview of the activated and deactivated functions in the Switching area. You can see directly which functions are currently activated. By clicking on the edit button, you can go directly to the various pages and make further settings there.

Port configuration

The table provides an overview of the current configuration of the individual ports. The columns Enabled, Autonegotiation, Flow Control and Designation are also editable. The page is regularly updated and reloaded.

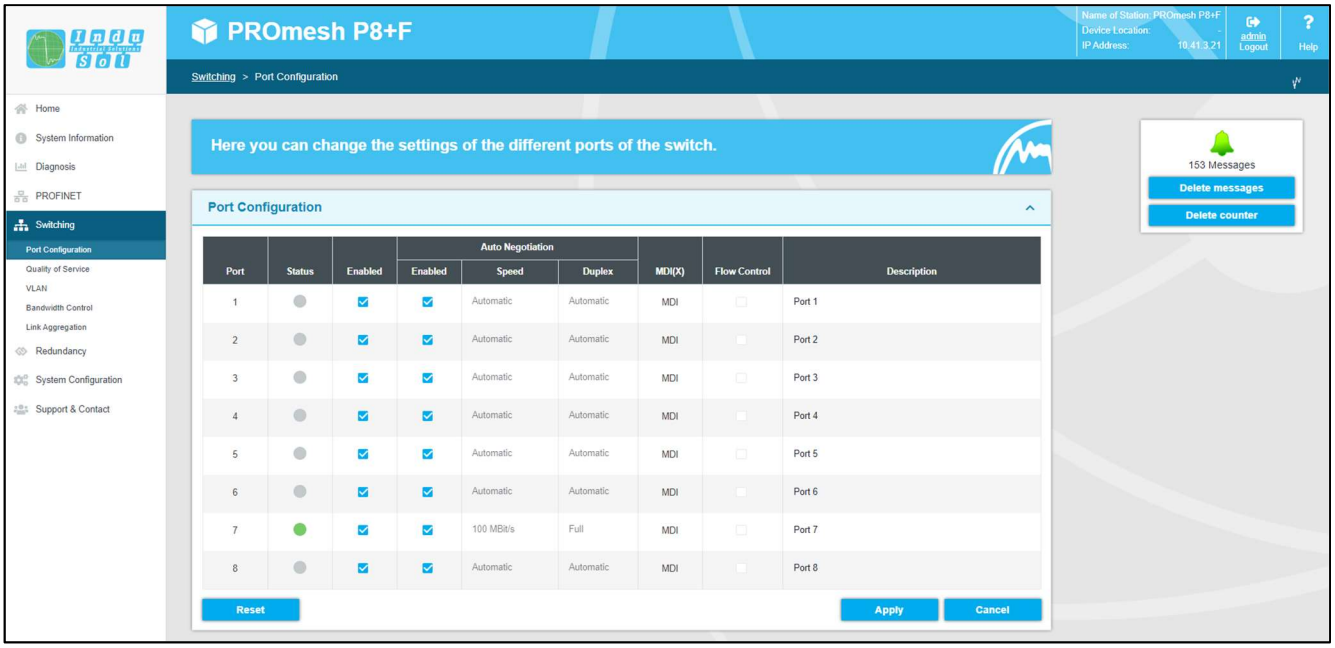

Figure 14: Port configuration

The columns in detail:

- Port: Indicates the port number, which is also marked on the housing.
- Enabled: The individual ports can be activated or deactivated. This determines whether a port can be used or not.
- Status: Status signals the current state of the ports:
  - green: The port is activated and a connection exists.
  - grey: The port is inactive or deactivated.
- Autonegotiation: If this function is activated, the transmission speed and duplex mode are configured automatically. The machine and the connected remote terminal negotiate the settings automatically. If autonegotiation is deactivated, the settings can be fixed manually:
  - Speed: The data rate of the ports can be fixed. It is possible to set a data rate of 10 Mbps or 100 Mbps.
  - Duplex: The duplex mode can be switched between half and full duplex. This setting is thus fixed for a connection.
- MDI(X): The unit can perform autocrossover detection by default. This means that the switch automatically detects whether the subscriber is connected via a crossover or non-crossover cable.

- Flow control: Flow control ensures that if a port is overloaded, the received data packets are ignored and the connected device is signalled to stop sending.
- Designation: In this column you can give the ports a name. The names are displayed throughout the configuration and facilitate the selection of the correct settings as well as diagnosis in the event of an error. Click directly on the port designation and edit the name in the line.

3.8.2 Quality of Service

Quality of Service (QoS) summarises all procedures that influence the data flow in the device. With the assignment to different prioritised queues, certain user data can be treated preferentially. For example, real-time data, control data, audio or video data can be given priority over file transmissions.

The switch supports eight different queues that are processed with different priorities. It is possible to use only one of the classification methods listed below or to combine several.

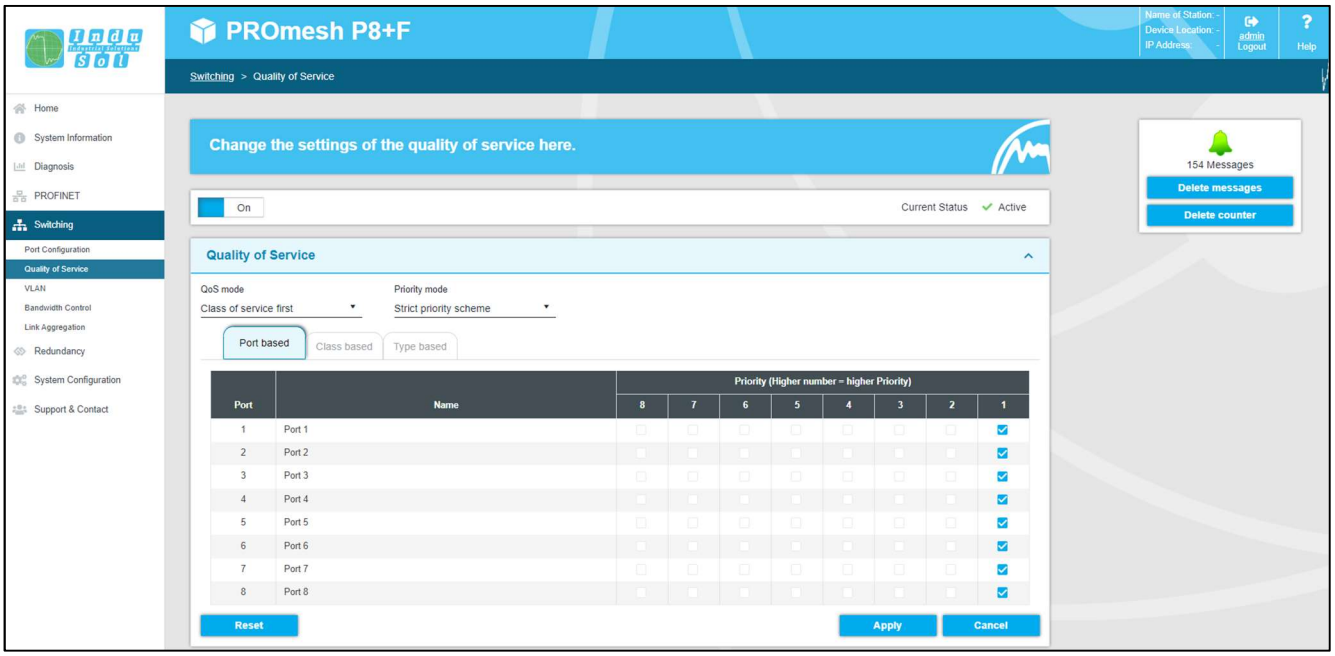

Figure 15: Quality of Service

QoS Mode and Priority Scheme

The QoS mode distinguishes between the following settings:

- Port based: You can set a priority for data transmission for each port and the switch will forward the data packets of the respective port according to your priority.
- Class-based (COS): The COS uses a data field with priority information available in the VLAN tag. Eight different priority values are specified from Best Efford (BE,0-low) to Network Control

(NC,7-high). Assign the COS priorities to the four queues of the switch as you need it in your application.

- Type based (TOS): TOS uses a Differentiated Services Code Point (DSCP) data field in the IP header of the packets, which can have up to 64 different priorities. As with COS, you can use these priorities to prioritise, for example, real-time control data, Voice over IP (VoIP) or audio data over normal data transfer. Adjust the settings to your requirements.
- QoS mode:
    - Port based only: Prioritisation is based solely on the priority of the ports.
    - Class of Service only: Prioritisation is based solely on the Class of Service data field of the packets.
    - Type of Service only: Prioritisation is based solely on the Type of Service data field of the packets.
    - Class of Service first: With this variant, prioritisation is first decided on the basis of COS, then (if necessary) by TOS and finally by port.
    - Type of Service first: Here the prioritisation is decided first by TOS, then (if necessary) by COS and finally by port.
- Priority scheme:
    - Strict priority scheme: With the strict priority scheme, all packets leave a port until the associated priority queue is empty. Only then are packets sent from the lower priority queues. If packets arrive permanently in the highest priority queue, packets from the lowest priority queue may never be sent. This mode is recommended when there are very high real-time requirements.
    - Weighted order: This approach prevents low priority packets from never being sent when there are permanent high priority packets to be sent. There is only a slightly higher latency for the high-priority packets. The switch primarily sends high-priority packets and also processes all low-priority queues in one send cycle.

VLAN

A virtual LAN (VLAN) is a logical group of network participants. It allows the isolation of a network part. Any data traffic from network participants of a VLAN group is only transferred within the VLAN group.

In the VLAN menu, you can choose between the VLANs and Ports view. Via the VLANs overview, you can add new VLANs and configure ports as "untagged", "tagged" or as no participant in the VLAN. Via the Ports page, you can also store a PVLAN ID for each port.

- Tagged (configurable in the VLANs tab): Ports that are configured as tagged in a VLAN provide ports with a VLAN tag. As a rule, switch - switch connections are configured as tagged. A port can be configured as a tagged port in several VLANs. This means that VLANs are not limited to individual switches, but can also be operated across several switches.

- Untagged (configurable in the VLANs tab): Ports that are stored as untagged in a VLAN can receive and forward packets of this VLAN ID. A port can be stored in several VLANs as an untagged port if the devices connected to this port are to communicate with several VLANs.
- PVID (configurable in the Ports tab): Only one PVID can be assigned for each port. The PVID determines to which switch-internal VLAN group the incoming packet is assigned. The VLAN tag of the packet header is not yet changed by this. Only when the packet leaves the switch via a tagged port is the VLAN tag entered according to the PVID of the incoming port.

If the VLAN 802.1Q function is activated, you can add a new VLAN using the Add button. You can also select an existing VLAN from the list and edit or delete it using a button.

The following additional data will be displayed:

- VLAN ID: This identification number is uniquely assigned to a VLAN. VLAN IDs between 1 and 4094 are possible. Make sure that the ID is not used by another VLAN in your network.
- VLAN Description: Enter the name for the new VLAN here. Maximum allowed length of the VLAN name is 50 characters.
- Port ID: corresponds to the port number marked on the housing.
- Status: Is the port active or not occupied.
- Description: A more detailed explanation of the port is possible here. This can be adjusted under Port Configuration.
- Ignore: The port ignores the ID tag of the current VLAN and cannot communicate with this VLAN.
- Untagged: see page 33
- Tagged: see page 33

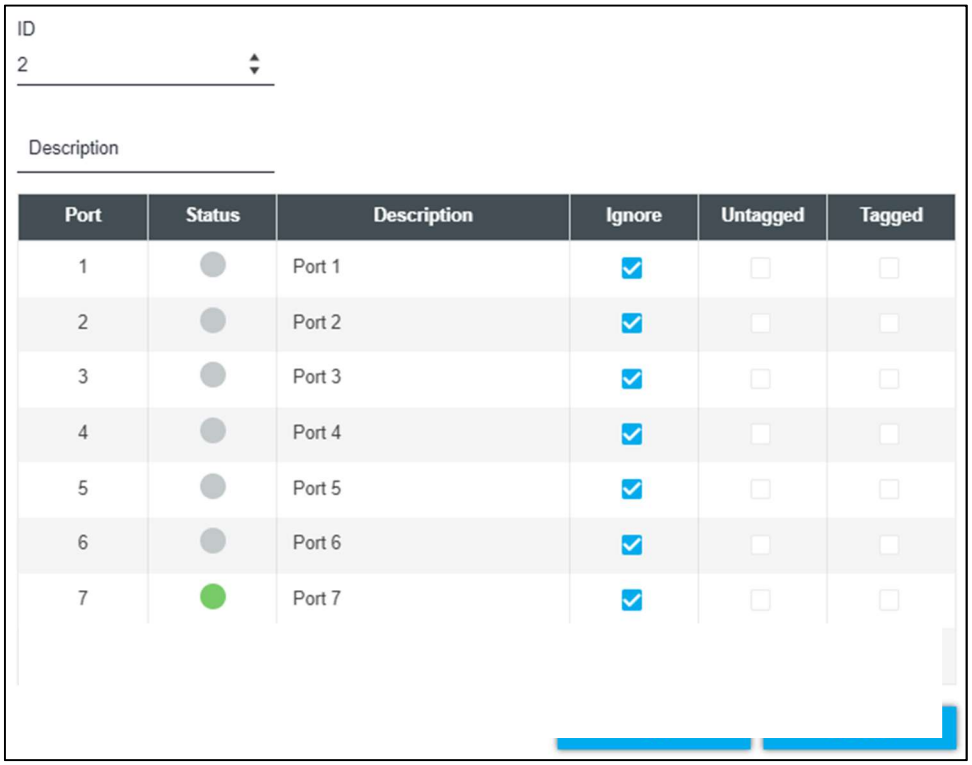

Figure 16: Add new VLAN

The Ports tab gives you an overview of the current configurations. Furthermore, you can determine the PVID.

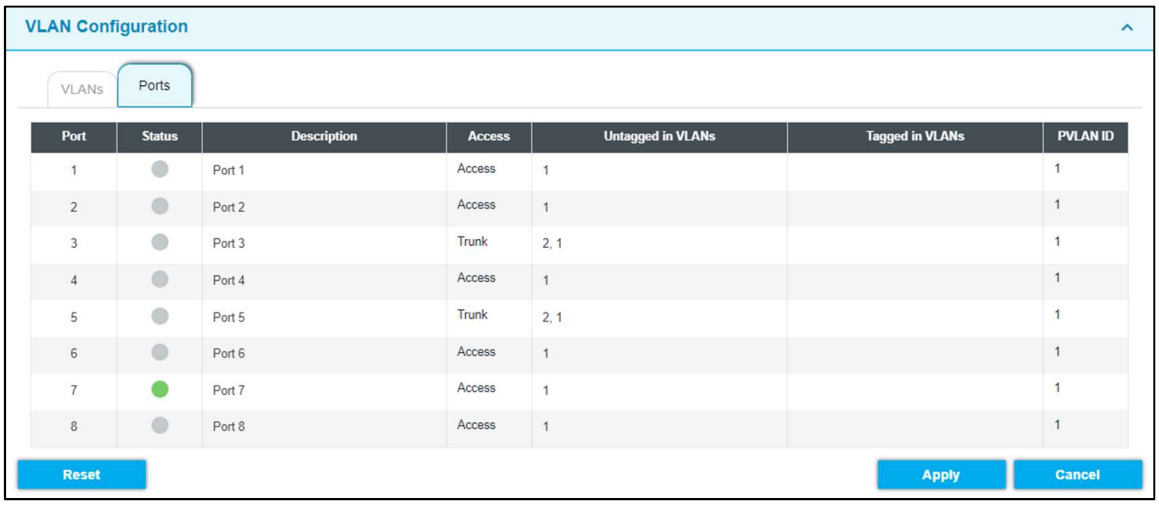

Figure 17: VLAN overview

3.8.4 Bandwidth control

Bandwidth control allows you to enforce bandwidth limits on a port. You can set different send and receive rates for each port (incoming / outgoing packets) and apply them to specific packet types.

The tabular overview offers you the following settings:

- ID: Indicates the port number, which is also marked on the housing.
- Package Type: Select a package type to filter by.
  - All: The set limits are observed for all packets transported via the port.
  - Broadcasts: The set limits apply to all broadcast packets (to all devices in the network).
  - Broadcast & Multicasts: The set limits apply to all broadcast and multicast packets (to all or several devices in the network).
  - Broadcast, Multicast & Unknown Unicasts: The limits apply to all broadcast, multicast and unknown unicast packets (to one subscriber).
- Limit incoming packets: Select the effective ingress rate of the port. Possible are 128 kbit/s, 256 kbit/s, 512 kbit/s, 1 Mbit/s, 2 Mbit/s, 4 Mbit/s and 8 Mbit/s. No limit" is defined as the default value.
- Limit of outgoing packets: The data rates for outgoing packets refer to all packet types. Select the effective egress rate of the port. Possible are 128 kbit/s, 256 kbit/s, 512 kbit/s, 1 Mbit/s, 2 Mbit/s, 4 Mbit/s and 8 Mbit/s. No limit" is defined as the default value.

After you have made the desired settings, click on "Apply" to save them.

3.8.5 Link aggregation

Using the Link Aggregation function, several physical connections can be combined into one logical connection. This allows you to transfer larger amounts of data between 2 units. (If you combine 2 physical connections between 2 PROmesh P8+F using Link Aggregation, then up to 2x 1Gbit/s can be transferred instead of 1 x 1Gbit/s).

Link aggregation can be static or dynamic.

Static

You can add a new link aggregation group via the "+" button. You can then:

- Group ID: Each link aggregation group has an ID (1-14).
- Type: specifies whether static or dynamic link aggregation is used
- Ports: Here you can select the physical ports that should belong to a link aggregation group (a logical connection).

With the "Apply" button, the settings can be accepted and applied.

Dynamic (LACP)

In this menu you can decide whether LACP is executed dynamically, statically or not at all.

The following settings must be made for this:

- Type: Select whether LACP is to be executed dynamically, statically or not.
- Group ID: This setting is relevant if you want to use static link aggregation. To do this, combine ports into one group by entering the same group ID. This setting is not required for dynamic link aggregation.
- Mode: This setting is relevant for dynamic LACP. In active mode, the LACP protocol is active for the port. In passive mode, the LACP protocol is only active for the port if the remote station of the port connection is also in passive mode. The protocol is sent to bridge a link failure without packet loss. With dynamic link aggregation, at least one side of the connection must be configured as the active part.
- Port priority: This setting is relevant for dynamic LACP. If another port is required for a logical connection, the free dynamic port with the highest port priority is selected. The lower the number, the higher the priority.

3.9 Redundancy

This page provides you with an overview of the available redundancy protocols and their status. It is not possible for several redundancy protocols to run at the same time, so only one can be activated. With the help of the edit buttons, you can access the protocols and carry out the configuration there.

The following protocols are available:

- MRP: The Media Redundancy Protocol is a ring protocol for highly available networks, which is achieved by inserting redundant paths.
- RSTP: The Rapid Spanning Tree Protocol is a standardised method to manage mixed structures in the network and contains a mechanism for automatic reconfiguration.
- MSTP: In principle, MSTP can be used to create a separate spanning tree for each VLAN.

The use of redundancy protocols guarantees your network increased reliability and availability in the event of a failure. The failure of a component is absorbed and the participants not affected by the failure can continue to communicate.

3.9.1 MRP

The Media Redundancy Protocol is a ring protocol for highly available networks. The high availability is made possible by redundant communication paths, which are switched off during normal operation. The participants connected in the network operate in a line topology, although physically it is a ring. In the event of a fault, communication can take place via the previously deactivated path after a very short recovery time.

MRP uses a redundancy manager that tests the continuity of the ring using special test packets and reconfigures the network in the event of an error and informs the participants. The guaranteed reconfiguration time, with up to 50 devices in the ring, is 200 ms. In a typical application, the reconfiguration time is usually less than 50 ms.

Ring configuration

Please note that the ring must not be physically closed until MRP is fully configured. One device per ring must be configured as a manager. The other devices must be configured as clients. The following settings are required for MRP:

- First Ring Port: Please select a port to work as the primary ring port.
- Second Ring Port: Set a second port to work as a secondary ring port. Please note that the secondary ring port and the primary ring port must be different.

- This unit operates as: Please specify whether the unit is to act as a manager or as a client. Please note that only one manager may be used per ring.

3.9.2 RSTP

The Rapid Spanning Tree Protocol (RSTP) is a standardised method to manage mixed structures, including a ring, in the network. It prevents network loops that can result from redundant transmission paths and includes a mechanism for automatic reconfiguration after a device or connection failure.

Activate the RSTP function globally before configuring the corresponding parameters.

Root Bridge Information

The following parameters are displayed in this field:

- Root Port: Shows which port works as the root port. The shortest path to the root bridge runs via this port.
- Root Bridge ID: Identification number of the current root bridge negotiated between the units.
- Designated cost: Path cost calculated for the connection to the root bridge.
- Root Bridge MAC Address: Displays the MAC address of the root bridge.

Device settings

Configure the protocol for your application...:

- Forward Delay: The time a port waits before switching from RSTP Learning and Listening status to Forwarding status. Enter a value between 4 and 30 seconds.
- Maximum Age: The time a bridge waits before attempting reconfiguration without receiving Spanning Tree Configuration Protocol messages. Enter a value between 6 and 40 seconds.
- Bridge Priority: This value is used for negotiating the root bridge. The bridge with the lowest value has the highest priority and is chosen as the root bridge. The value must be between 0 and 61440 and a multiple of 4096.
- Hello Time: The time interval at which the switch sends BPDU (Bridge Protocol Data Unit) packets to check the current status of the RSTP. Enter a value between 1 and 10 seconds.
- TX Hold Count: Specifies the maximum number of Hello packets transmitted within an interval. A minimum of 1 and a maximum of 10 packets are permitted.

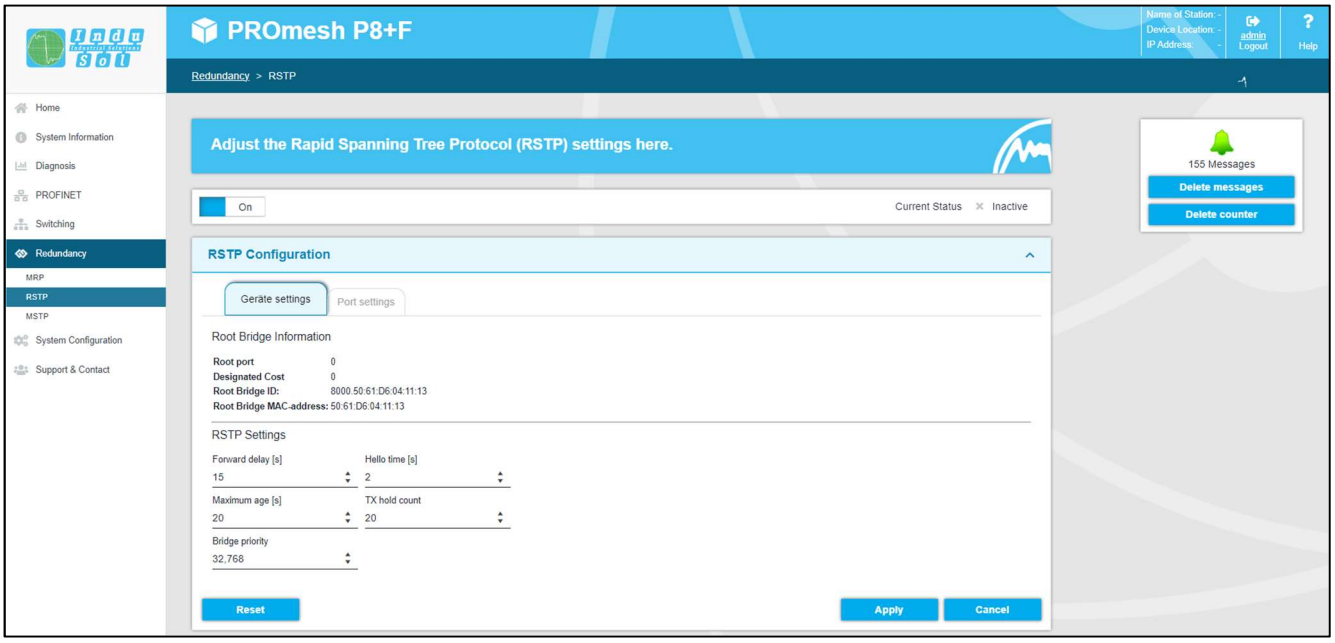

Figure 18: Device settings RSTP

Note: Follow the rule to configure Forward Delay, Maximum Age and Hello Time:

2 * (Forward Delay Time - 1) >= MaxAge >= 2 * (Hello Time + 1).

Recommended procedure: Select a value for the "Hello Time" and calculate with the formula 2 * (Hello Time + 1) according to the rule given above to obtain the lower limit of the Maximum Age. Select a value for the "Forward Delay Time" and calculate with the formula 2 * (Forward Delay Time - 1) of the rule given above to get the upper limit of the Maximum Age. Then select a Maximum Age between 6 and 40 seconds, which is between the previously calculated limits.

When you have set the parameters, click Apply to apply the changes. The root bridge information is now displayed at the top of the page.

Port settings

Set the following port-related settings per port:

- Port: You can configure all ports individually.
- RSTP on: For each port, select whether the Rapid Spanning Tree Protocol should be activated on this port or not.
- Status: Shows the current status of the individual ports. A distinction is made between:
  - Blocking: Discards packets; does not learn addresses; receives and processes BPDUs
  - Listening: Discards packets; does not learn addresses; receives, processes and transmits BPDUs
  - Learning: Discards packets; learns addresses, receives; processes and transmits BPDUs
  - Forwarding: forwards packets; learns addresses; receives, processes and transmits BPDUs
  - Disabled: Discards packets; does not learn addresses; does not receive and process BPDUs
- Role: Each port can run in one of the following modes:
  - Root Port: A port in the forwarding state. Shortest path to the root bridge.
  - Designated port: A port in the forwarding state that enables communication to other bridges in the spanning tree.
  - Alternative port: An alternative path to the root bridge that exists in addition to the current root port.
  - Backup Port: A backup path provided through a designated port towards the branches of the tree structure. Backup ports can only exist where two ports are connected as a loopback by a point-to-point connection or a bridge with two or more connections to a common LAN segment.
  - Disabled Port: A port that has no operational function in the tree structure.
- Priority: You can assign higher priorities to certain ports to influence the structure of the tree. Enter a number between 0 and 240. The value must be a multiple of 16.
- Cost: The cost from the sending bridge at the respective port of another bridge. Enter a number between 1 and 200,000,000. With this parameter you can influence the structure of the tree.
  - defined: The costs of a connection to the root bridge can be specified.
  - designated: The designated costs are calculated by the RSTP and displayed here.
- Edge port: Refers to a port that is directly connected to an end device and not to another bridge (a switch). These ports cannot cause loops and therefore immediately switch to Forwarding mode. Changing the status of an edge port does not change the topology in any case. By setting edge ports fixed, they speed up the reconfiguration time of the redundancy protocol.
  - Force: The port is configured as an edge port by default.
  - Auto: Detection as an edge port is automatic.

After you have set the respective parameters, click Apply to apply the settings.

3.9.3 MSTP

Instance configuration

In this menu you can create multiple spanning tree instances. This allows you to create a separate spanning tree for each VLAN. The following settings are required for this:

- Instance ID: Select the Multiple Spanning Tree Instance ID here. This ID must be identical for all switches that are to belong to the same spanning tree.
- Priority: Each participant of an MST instance can be assigned a priority. The values can be assigned in steps of 4096 (starting with 4096). The lower the value, the higher the assigned priority. The participant with the lowest priority is declared the Spanning Tree Master.
- VLANs: Here you can specify a VLAN or a VLAN group for which the spanning tree is created.

Port setting

In this menu you can make the following settings:

- MTSP on: Activate the settings made in this menu
- BPDU Guard: The BPDU Guard is a security mechanism of the STP and should be activated on all access ports. If these ports receive a BPDU, they are deactivated. This can prevent the network from being disturbed by manipulated BPDUs.
- Edge port: Refers to a port that is directly connected to an end device and not to another bridge (a switch). These ports cannot cause loops and therefore immediately switch to Forwarding mode. Changing the status of an edge port does not change the topology in any case. By setting edge ports, they speed up the reconfiguration time of the redundancy protocol.
- Force: When enabled, the port is configured as an edge port by default.
- Auto: The port is not configured as an edge port by default.

3.10 System configuration

The System Configuration page displays the IP address settings, the time setting, access options to the unit and general unit information.

The purpose of the page is to enable you to get a compact view of the System Configuration menu in order to understand how the unit works and where action is required.

With the help of the edit buttons, you can go directly to the corresponding protocols and functions to make further settings there.

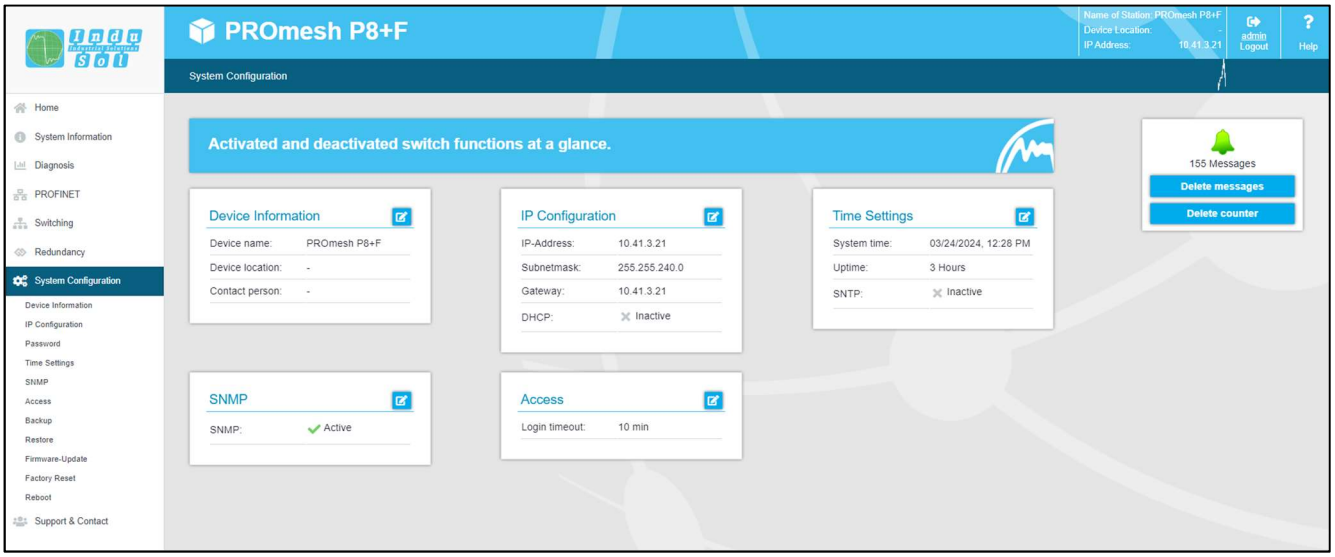

Figure 19: System configuration

3.10.1 Unit information

The Unit Information page allows you to assign a unique unit name, installation location and contact person to the unit.

- Device name: This name corresponds to the PROFINET name and is assigned by means of DCP.
- Installation location: Specify the installation location of the unit to facilitate localisation.
- Contact person: Enter a contact person for the unit.

The input fields are configured so that you may use up to 50 characters. The use of special characters is possible. The unit name and installation location are displayed in the information bar in the top right-hand corner and help you to keep track.

3.10.2 IP configuration

The IP configuration can be carried out either by the PROFINET controller, automatically using the Dynamic Host Configuration Protocol (DHCP) or manually. If the address is assigned automatically, the IP may change after a device restart depending on the settings of the DHCP server.

PROFINET

If the unit is configured in a PROFINET network, the unit receives its IP configuration from the PROFINET controller. With an existing PROFINET connection, the IP configuration cannot be done automatically or manually.

Automatic

To obtain a configuration of the IP address, the subnet mask and the standard gateway from a server operating in the network with corresponding functionality, select the checkbox "automatic (DHCP)".

After you have saved the settings by clicking on the Apply button, the unit sends a request to the server and adopts the configuration received from the DHCP server. Since the unit has now received a new IP address, it can no longer be reached via the default IP. Please contact your network administrator or use an appropriate tool (Indu-Sol ServiceTool) to obtain the new IP address.

Manual

If your network does not have a DHCP server or you want to make the settings manually, deactivate the "automatic (DHCP)" button and enter the following data:

- IP address: Please note that the IP address you set must be accessible from your PC so that you can connect to the unit again to make the other settings.
- Subnet mask: Enter the subnet mask of the IP address, this separates the IP address into a network part and a device part. This determines which IP addresses can be reached directly by the unit and which addresses must be addressed via a gateway.
- Gateway: Enter a standard gateway. The gateway is used to communicate with devices outside your subnet.

Please check exactly which settings you make so that there are no problems with duplicate IP addresses. The format of the IP address, the subnet mask and the gateway must be entered in decimal notation.

3.10.3 Password

On this page, the preset default password for the users Admin and User can be changed. The user names and rights of the administrator and the user are fixed and cannot be changed.

Form fields

- New password: Please enter the password you have set for the previously selected user in this field. Please also note the information on assigning passwords in the section below.
- Confirm password: To make sure you have entered your password correctly, repeat the entry in this field.
- Current password: Please enter the current password used so far to ensure that you are authorised to change the password.

Notes on passwords

The security of your system is essentially related to the security of your passwords. It is therefore generally recommended for passwords:

- not to use dictionary entries
- Use passwords that are as complex as possible
- Use combinations of letters, numbers and special characters
- use small and capital letters
- use a password of at least eight characters
- Not to write down passwords

3.10.4 Time setting

In this menu you can store the device time of the switch. For this purpose you have the options the time:

- Automatic (SNTP)
- Manual

to store the time. Furthermore, the PROmesh P8+F can be used as a time server to provide other devices with the current system time.

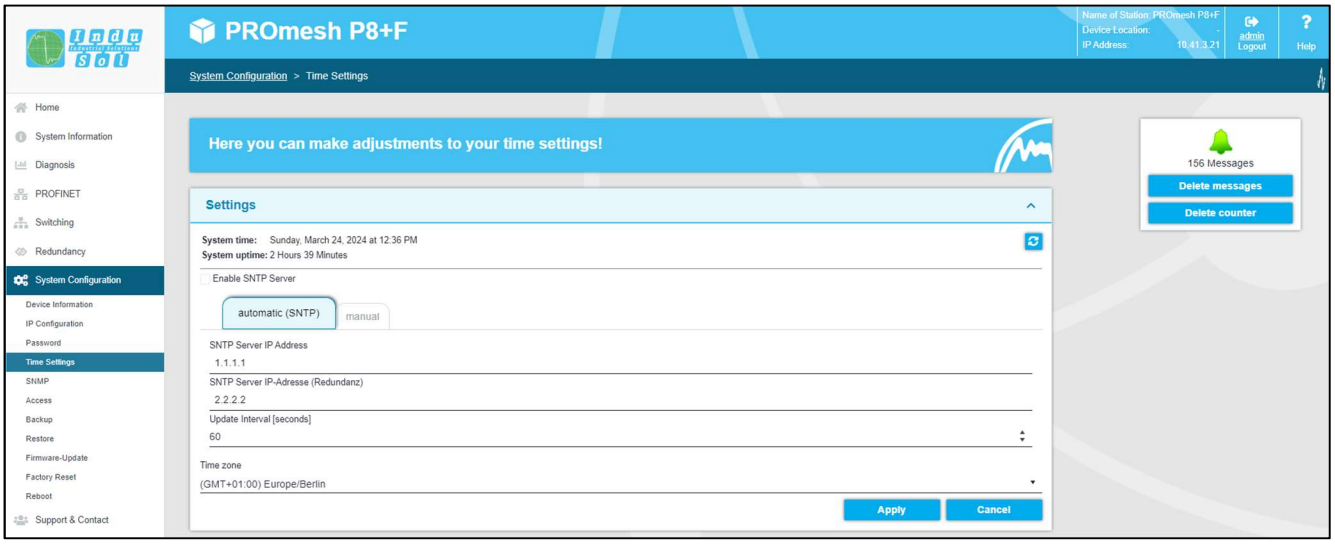

Figure 20: Time server

Automatic (SNTP)

- SNTP Server: Store the IP address of the time server. It is possible to store a second time server as redundancy.
- Update interval: Here you can determine the cycle in which the device time is synchronised with the time server.
- Time zone: Then select your valid time zone

Manual

In this setting you have the option of manually entering the current date and time by clicking on the calendar icon.

Furthermore, you can select your valid time zone under "Time zone".

3.10.5 SNMP

The Simple Network Management Protocol (SNMP) regulates the communication between the monitored devices and the monitoring station. It enables the reading and writing of system variables.

Current SNMP accesses

The overview table shows you the currently defined community strings and access permissions.

- Active: Shows which community strings are currently activated and which are not.
- Community String: The accesses are defined by unique names that you can customise.
- Read only: The community string allows read-only access.
- Read and write: The community string allows read and write access.

- Remove: You can mark the community strings to be deleted and then remove them with the "Delete" button.

Create SNMP access

To create a new community string, click on the "Add" button. The following parameters are required:

- Community String: Enter a unique name for the new SNMP access. A maximum of 32 characters is allowed.
- Access: Specify whether read-only or read and write access is allowed.

Save the settings by clicking on the "Create" button.

The unit supports SNMP versions V1, V2C and V3. Select the desired version.

The following additional settings are required for SNMP V3:

- Username: Enter a user name here.
- Verification: Enter the authentication type here. You can choose between MD5 and SHA. Enter the corresponding password.
- Encryption: Select the encryption mechanism. You can choose between AES, DES or no encryption.
- Access: Select whether only read or read and write permissions are assigned by the configured access.

3.10.6 Access time

Settings

The time until automatic logout defines how long a session in web management remains without activity before an automatic logout takes place. You can set a time between 3 and 30 minutes. The default setting is 10 minutes.

Use the "Apply" button to save the settings.

Furthermore, you can here:

- Enable SSH and Telnet
- Enable web access via HTTP, HTTPS or through HTTP and HTTPS

3.10.7 Backup

This menu item allows you to save the current configuration of the unit in a file. The backup can be saved as a download, on the SD card or via TFTP.

The unit creates and saves a backup file with all settings that can be loaded at a later time using the Restore function.

- Download: The backup file is stored in the browser's download directory or the user can specify a path where the file is then saved.
- SD card: An SD card can be inserted into the SD card slot on the back of the unit. The backup file is then saved to this SD card with this option.

3.10.8 Restoration

This menu item is used to import a previously saved backup file. The menu item Backup is used to create the backup file. The backup can be loaded via TFTP, as an upload or via SD card.

- Upload: The backup file is located on the computer currently in use and is transferred from there to the unit.
- SD card: The backup file is on an SD card and is restored from there.

3.10.9 Firmware update

Here you can update the firmware of the device. Please only use firmware versions that you have received from Indu-Sol and that have been developed for the PROmesh switches.

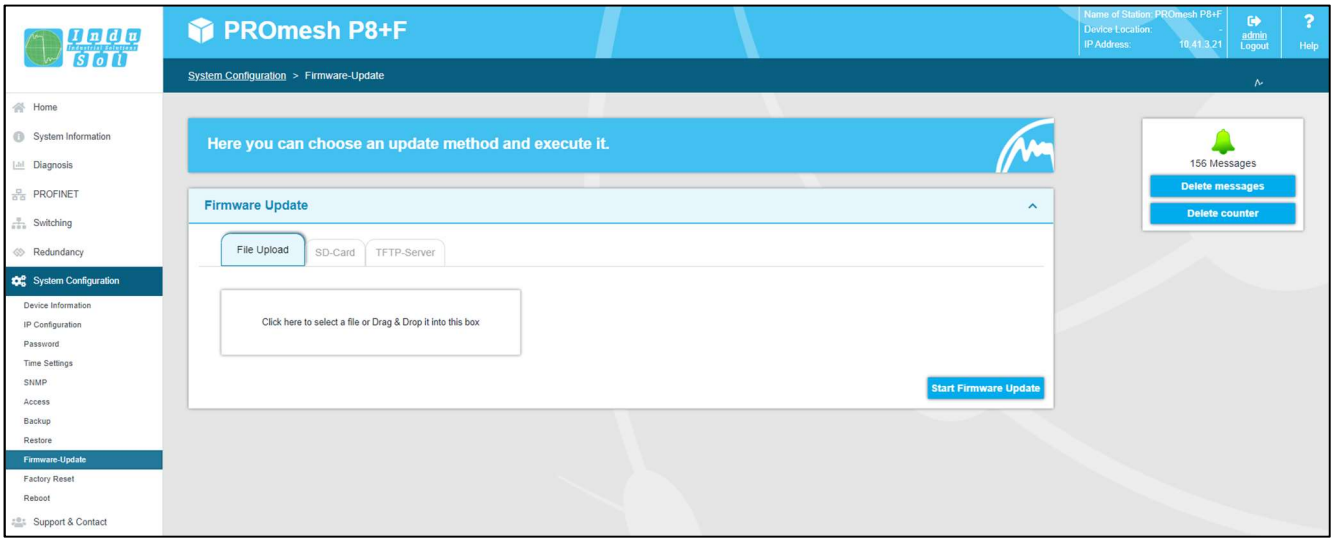

Figure 21: Fimware update

The firmware file is either provided by a TFTP server or loaded onto the unit via upload or SD card. Before updating, check that you have selected the correct firmware image.

- Upload: The firmware update is located on the computer currently in use and is transferred from there to the unit.
- SD card: The firmware update is on the SD card and is imported from there.
- TFTP server: The firmware update is downloaded from a TFTP server present in the network.

Preparation:

It is not recommended to perform the update when the MRP protocol is activated. Please open the MRP ring first by pulling out one of the cables and then deactivate the Media Redundancy Protocol. Now perform the firmware update.

Settings

- TFTP server IP address: Enter the IP address of the TFTP server available on the network in decimal dot notation.
- File name: Enter the name of the new firmware file to be installed here. Please enter the name relative to the root directory of the server.

Use the button "Start firmware update" to execute the action and confirm this in the window that opens. Please ensure that the firmware update can be carried out completely.

Important:

Refrain from the following actions while the firmware update is being carried out.

- Do not disconnect the unit from the supply voltage under any circumstances.
- Do not unplug or reconnect any network plugs.

A message appears as soon as the update is completed. The unit will then restart automatically.

3.10.10 Factory settings

This menu item is used to reset the unit to its factory settings.

Click on the button "Set factory settings" to carry out the action and confirm this in the window that opens. The unit must then be restarted.

3.10.11 Restart

Here you can reboot the switch to perform a software reset. By pressing the restart button, the software of the switch is terminated and the device reboots.

Alternatively, you can switch the two supply voltages of the switch off and on again and thus perform a hardware reset.

3.11 Support

In the Support section you will find all relevant contact information for Indu-Sol

Licence information

The linked license.txt file contains information regarding the "open source software" used.

3.12 Troubleshooting tips

- Check that the power supply is correct. At least one of the VDC LEDs must light up green.
- Check the link/act LEDs of the wired RJ45 sockets. When the connection is established, the link LEDs must light up or flash when data is being transmitted.
- If in doubt, disconnect redundant network structures and reset the ***PROmesh P8+F switch*** to factory settings. If the communication works afterwards, make your settings again bit by bit, observing at which point the error occurs.

4 Technical specification en

Network connections	8 x up to 1 Gbit/s RJ45
Power supply	12 V ... 48 V DC power supply
Power consumption	Maximum 8 W
Dimensions (HxWxD)	130 mm x 150 mm x 60 mm
Weight	0,9 kg
Housing	Aluminium, anodised
Storage temperature	-40 °C ... 75 °C
Operating temperature	-40 °C ... 75 °C
Humidity	Humidity 5 % ... 95 % RHD non-condensing
Protection class	IP20 (not evaluated by UL)
Assembly	35 mm DIN rail
EMC	2014/30/EU EN 61000-6-2 / EN 55032
LED display	Status LEDs / Port LEDs / Power supply
Management	SNMP management Web interface management
Switching technology	Store & Forward
MAC address table	16 K MAC address table
Ring	MRP Spanning Tree
VLAN	Port based VLAN Tagged VLAN IEEE 802.1Q
Class of Service	IEEE802.1p Class of Service with eight priority queues per port
Port Mirror	RX packages only or TX and RX packages
Firmware update	SD card, TFTP server, from local PC
Bandwidth contr.	Incoming and outgoing
DHCP Client	DHCP client function to obtain an IP address from the DHCP server

Indu-Sol GmbH
Blumenstraße 3
04626 Schmölln

Telefon: +49 (0) 34491 580-0
Telefax: +49 (0) 34491 580-499

info@indu-sol.com
www.indu-sol.com

Wir sind zertifiziert nach DIN EN ISO 9001:2015