Indu-Sol GmbH – Specialist in Industrial Networks

PROmesh B8
User Manual

Layer-2-Managed Industrial Ethernet-Switch

Indu-Sol GmbH

Blumenstraße 3

D-042626 Schmölln

Phone: +49 (0)34491 / 580 0

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

Email: info@indu-sol.com

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

Our **technical support** team is available at +49 (0)34491 / 58 18 14, weekdays between 7:30 – 16:30 (CET). You can also email us at: support@indu-sol.com

Is your plant standing still? You can reach our emergency service around the clock at: +49 (0)34491 / 580 0.

Revision overview

Date	Revision	Change(s)
10/01/2023	0	First version
03/02/2023	1	Power Supply
16/02/2023	2	Cover

W A R N I N G

Commissioning and operation of this device must only be performed by qualified personnel. Qualified personnel within the meaning of the safety notices in this manual are persons authorised to commission, ground, and mark devices, systems, and circuits in accordance with safety engineering standards.

Improper use or configuration of the *PROmesh B8* in the network may cause severe physical injury as well as property and material damage, also due to uncontrolled machine movements.

Table of content

1   General information

Please read this document thoroughly from start to finish before you begin installing the device and putting the device into operation.

1.1   Overview of the *PROmesh B8* – function scope

The *PROmesh B8* is an industrial Ethernet switch with management and PROFINET functions 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
- Anti-reverse supply 12-36V DC, redundant operation possible
- Port statistics (network load in ms, errors, discards)
- Alarm management
- 8 x 10/100 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 by 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
- 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
- Update, save, and backup the system configuration via web interface

1.2   Scope of supply

The scope of supply comprises the following individual parts:

- *PROmesh B8*
- 7-pin pluggable terminal block, 2.5 mm² (power supply and alarm contact)
- User quick start guide (hardcopy)

Check that the content of your delivery is complete before commissioning. In case of questions, contact our technical support team immediately before commissioning.

1.3   Safety notices

Check that it is in perfect condition externally before commissioning of the device. If any damage is suspected, return the PROmesh B8 to your supplier immediately and do not operate the device. Our technical support team will be happy to answer any questions you may have.

The *PROmesh B8* was developed for use in PROFINET applications in accordance with conformance class B. Also note the selection of the data lines used in accordance with the standard to fully support the PROFINET standards.

Always observe the technical specification of the device to ensure safe and optimum use. The device is designed for IP20 protected environments. Take appropriate measures in case of deviating operating environment to ensure proper operation of the device.

Do not open the housing under any circumstances. No parts that require servicing have been installed. Unauthorised opening of the housing will void any warranty claims.

2 Connections and status indicators on the device

Device connections

Status LEDs

X1 data ports

8x RJ45

X2 Power supply and alarm contact

FE connection

Potential-free
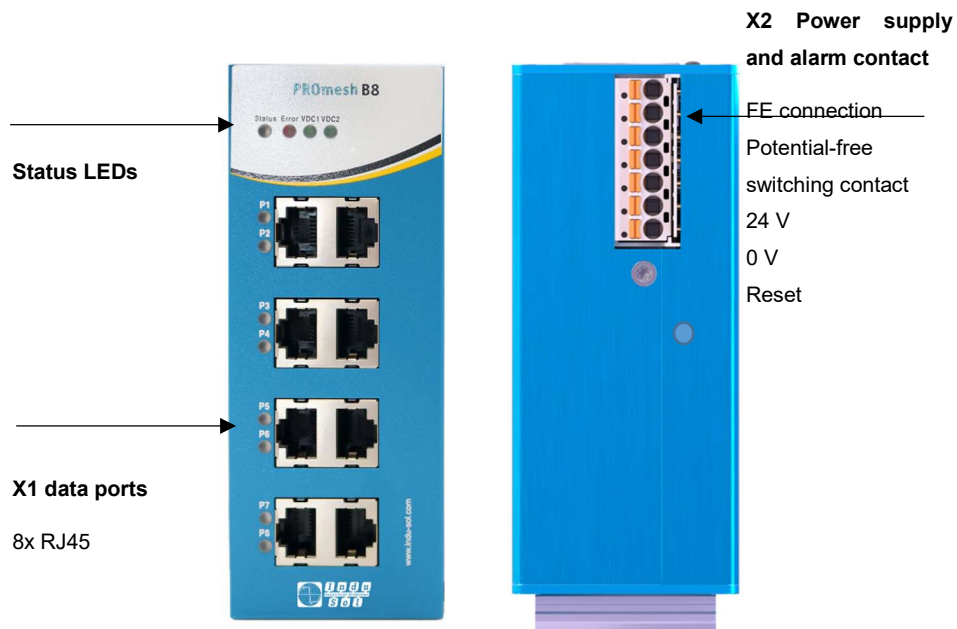
switching contact

24 V

0 V

Reset

Figure 1: Device connections

2.2 Installation

The PROmesh B8 is designed for individual use in control cabinets of various types and can be mounted on a standard 35 mm DIN top-hat rail.

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

2.3 Mounting

The *PROmesh B8* is mounted vertically in the control cabinet on a 35 mm DIN top-hat rail in accordance with DIN EN 60715.
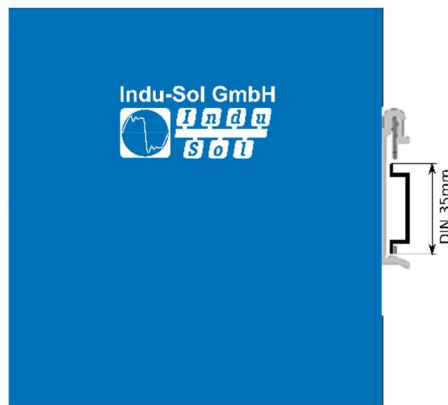

Figure 2: Side view with connection terminal on the right

The following distances to other assemblies must be observed for correct mounting:

- To the left and right: 20 mm
- Up and down: 50 mm

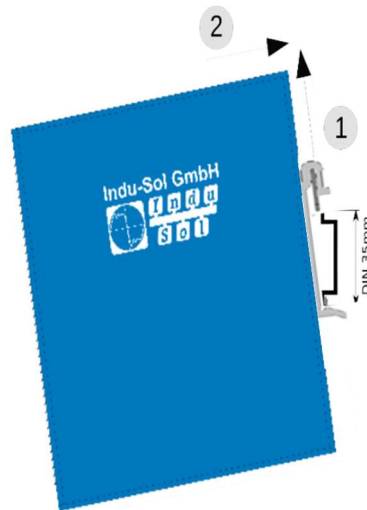Assembly and disassembly of the device are displayed in Figure 3.

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

Do not mount the *PROmesh B8* switches directly adjacent to any devices that generate strong electromagnetic interference fields, such as transformers, contactors, frequency converters, etc.

Do not mount the *PROmesh B8* switches directly adjacent to any heat-generating devices and protect the switch from direct sunlight to avoid unwanted heating. Protect the PROmesh B8 from any additional heat radiation and observe the permitted storage and operating temperature range.

2.4   Connection of power supply and error relay

Operate your *PROmesh B8* with a nominal voltage of DC 12 V to 48 V. Connect the redundant power supply VDC1 and VDC2 to the correspondingly marked connection terminals of the supplied 7-pin terminal block adapter (VDC1, GND as well as VDC2, GND) to ensure your system availability. The power supply shall comply with UL60950-1/UL62368-1, Class 2 (NEC), limited energy source (UL61010-1).

The 7-pin 2.5 mm² connector terminal block on the top of the device is assigned as follows:
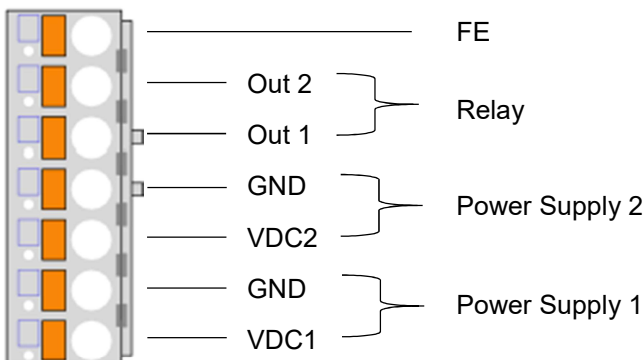
Figure 4:Connector terminal block assignment

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

There is a potential-free error relay contact (NC contact) at the OUT terminals inside the unit. The relay serves as an alarm receiver. It can be linked to various alarm triggers in the software. The relay contact then opens, for example, in case of a power outage or a change in the status of the port depending on the configuration.

2.5 LED displays

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

Each of the 8 data ports also has a status LED.

The LEDs display the most important diagnostic information about the device and connection status of the PROmesh B8 in your PROFINET network (see Table 1).

LED	Status	Meaning
VDC1	Green	Voltage at connection sufficient
	Off	Voltage at connection insufficient
VDC2	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 ports 1-8 (green)	Off	No link
	Flashing	Link + data exchange (flashing speed reflects link speed)
	On	Link

Table 1: LED functions

2.6 Reset button

The reset button can be used if the PROmesh B8 experiences any unexpected abnormalities that render it inaccessible. It can either restart the PROmesh B8 or reset to its factory settings. This requires the following procedure:

- Restarting the device: Push the reset button for 1 second

- Reset to factory settings: Push the reset button until all LEDs go out (approx. 10s)

2.7   Network integration & commissioning

2.7.1   Data ports

The *PROmesh B8* is equipped with 8 data ports that allow data transmission at up to 100 Mbit/s in compliance with PROFINET standard 2.4. The actual data rate is negotiated by the device using auto-negotiation.

2.7.2   Media selection & connection

The PROmesh B8 has nine data ports for connecting RJ-45 copper cables.

Observe the applicable standards and fixed connections in the connector application when designing, selecting, assigning, and assembling your data cable in order to ensure the longest possible cable length and cascading of network segments in accordance with your media type (copper, optical fibre, etc.).

2.7.3   Wiring

Connect your PROmesh B8 via the existing RJ-45 data ports using twisted pair cables of category 5 (Cat 5) or higher with a maximum cable length of up to 100 m. We recommend the PROFINET RJ45 connectors from Indu-Sol to improve the shielding.

2.8 Network topologies & redundancy

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

2.8.1 Network topologies

Classical Ethernet star structures (see Figure 5) can be linked to the *PROmesh B8* switches without additional configuration. The devices are ready for use immediately.
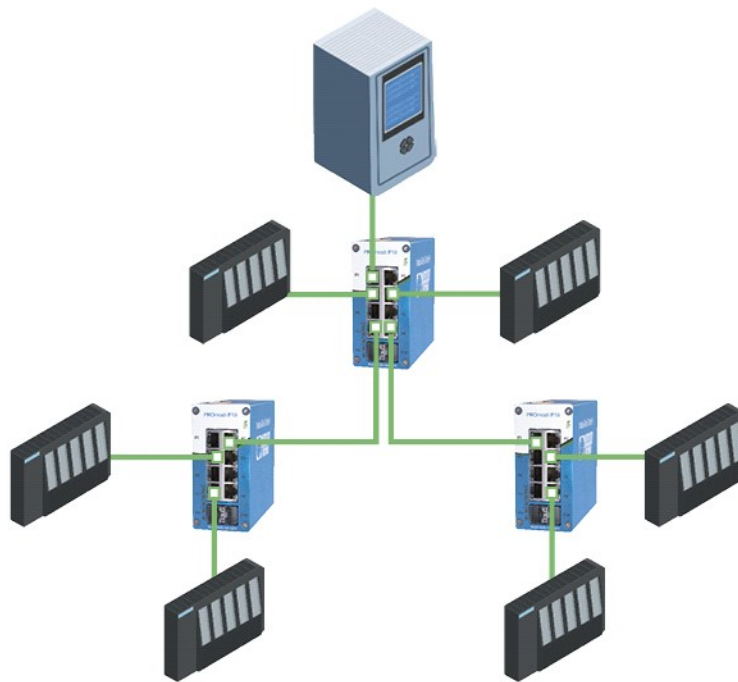

Figure 5: *PROmesh B8* in a star network

2.8.2 Ring structure

The *PROmesh B8* supports the IEC 62439 standard, thereby enabling deterministic reconfiguration of information forwarding in simple redundancy (ring topologies, see Figure 6). This enables reconfiguration times of up to 200 ms, depending on the size of your system.
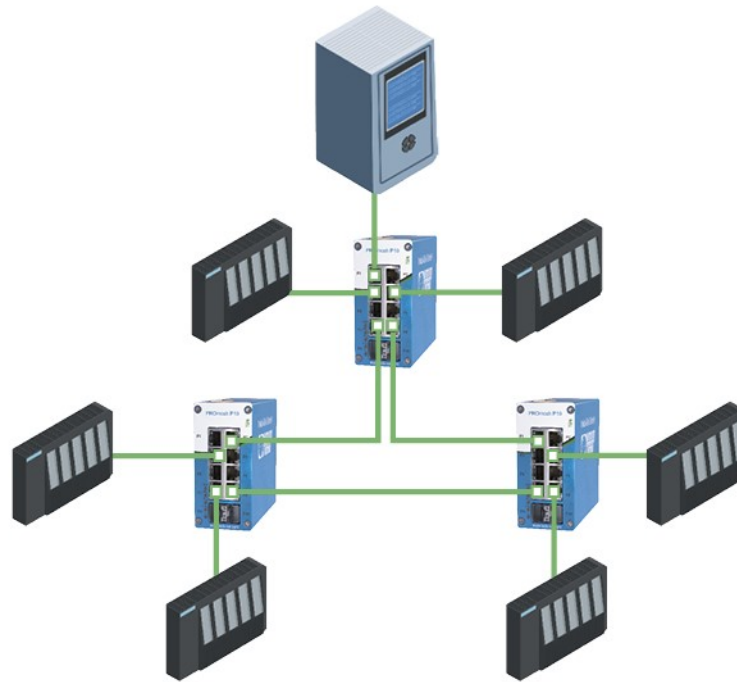
Figure 6: *PROmesh B8* in a ring-shaped network

3   Web application

The *PROmesh B8* switches are equipped with a modern web interface that may be configured comfortably from any web browser.

3.1   Preparations

Install the *PROmesh B8* switch on the network before using web management and ensure that the PC designated to configure the switches can access the switch through the web browser. The PROmesh B8 and the client PC to be connected must be in the same IP address range and IP subnet. You must assign an PROmesh B8 IP address at first use for this.

The following IP address, subnet mask, administrator username, and administrator password are set when the device is shipped from the factory:

- 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 part of the scope of delivery or can be downloaded for free via the following link:
https://sdx.indu-sol.com/s/CtYtsHNW73Z3KCa

Our software is updated regularly. Please ensure that you have the latest version.

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

The corresponding address settings are then made automatically this way if you include the switch in a PROFINET system in the hardware configuration of the controller.

A user access with lower authorizations and adapted menu navigation is available as an alternative to the administrator access. The user has no access to the Switching, PROFINET and redundancy functions or their sub-items. The submenus for system configuration are also restricted. The access data for this are:

- Username: **user**
- Password: **user**

3.2 System login

1. Launch a web browser on your computer.

2. Enter the IP address of the *PROmesh B8* switch you are using into the address line of the web browser and confirm your entry with the *Enter* key.

3. The login mask of the device now appears on the screen.
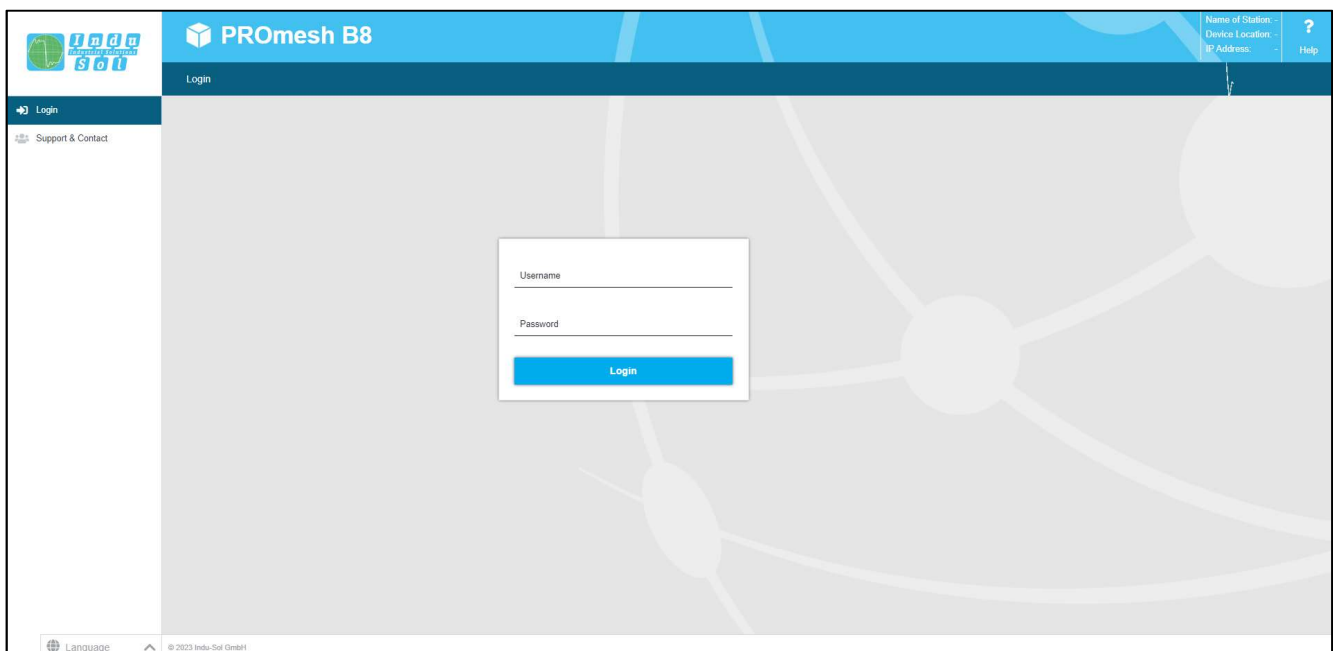
Figure 7: Login mask

4. Select the desired menu language (DE / EN). You can change this at any time, in any menu of the web interface.

5. Then enter the username and password.

6. Pressing the *Enter* key or clicking *Login* will take you to the switch web interface.

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 without any errors.

Warning: At least one communication fault (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 fault has occurred on the corresponding port, resulting in a communication interruption. Urgent action is needed to correct the disruption.

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

3.4 Start

Successful login will lead to the main overview with the information bar, where the device name, the installation location, and the IP address are displayed. The current user is displayed under the logout button at the right end of the bar. You can log out by pushing the button. The help button displays notes and explanations for the individual pages.

The port statistics provide an overall view of the state 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

are displayed. In the Details view, the parameters of the overview and:

- Netload per s
- Discards
- Errors

are displayed.

The number of messages that have occurred is displayed in the message window. Clicking on the alarm bell will automatically call up the entries in the message list. The messages as well as the counter status of the ports can be deleted with the corresponding buttons.

Selection in the menu bar allows you to call up the individual pages and make settings there. The displayed menu items are subdivided into further subitems.
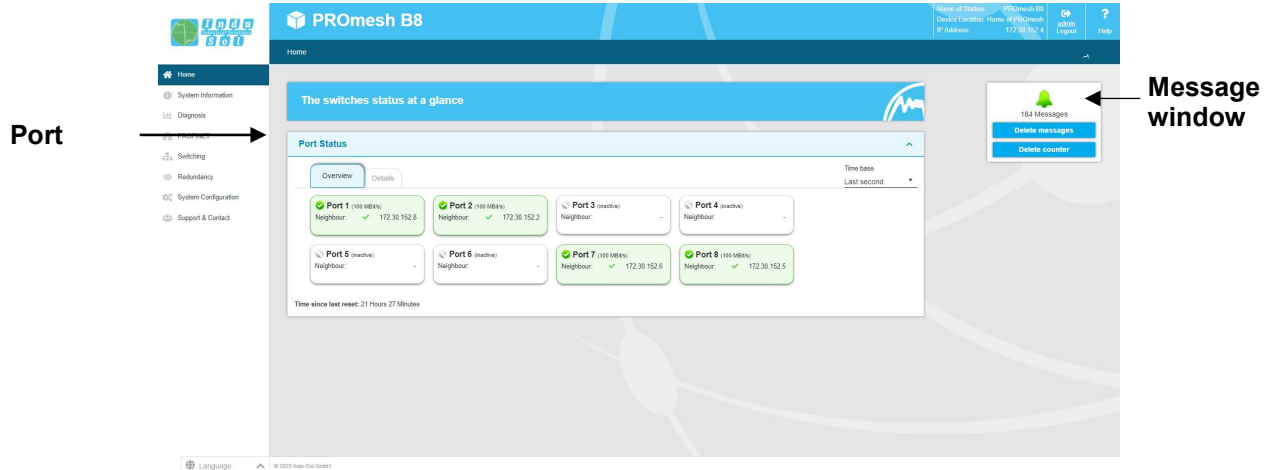
Port

Message window

Figure 8: Start

3.5 System information

An overview of the enabled or disabled protocols and functions is displayed under this menu item in addition to the device information. You can switch directly to the corresponding protocols and functions in order to make settings there by selecting the respective Edit button.
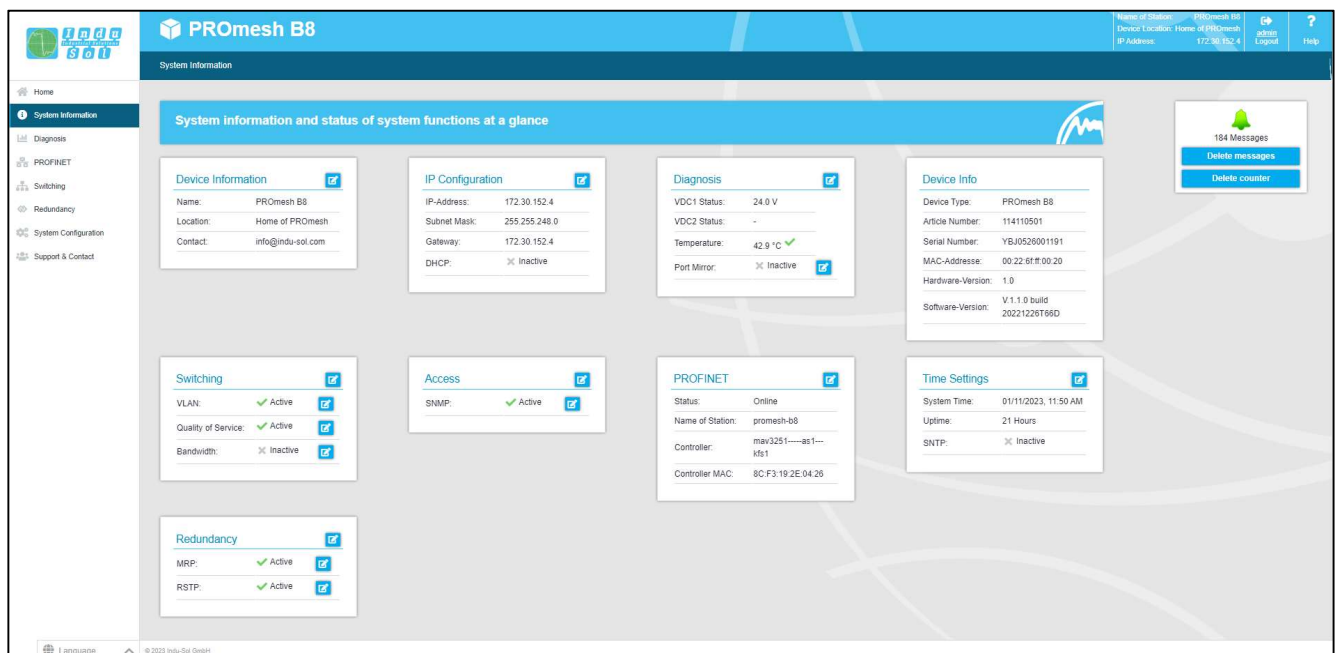

Figure 9: Status and diagnosis

3.6 Diagnosis

The diagnosis page provides an overview of the status of configured alarm triggers (alarm trigger configured or not) for the individual diagnostic data acquired by the PROmesh B8. The status for topology determination and port mirroring is also displayed.

3.6.1 Network statistics

The port statistics page provides information about the traffic on each port. 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)
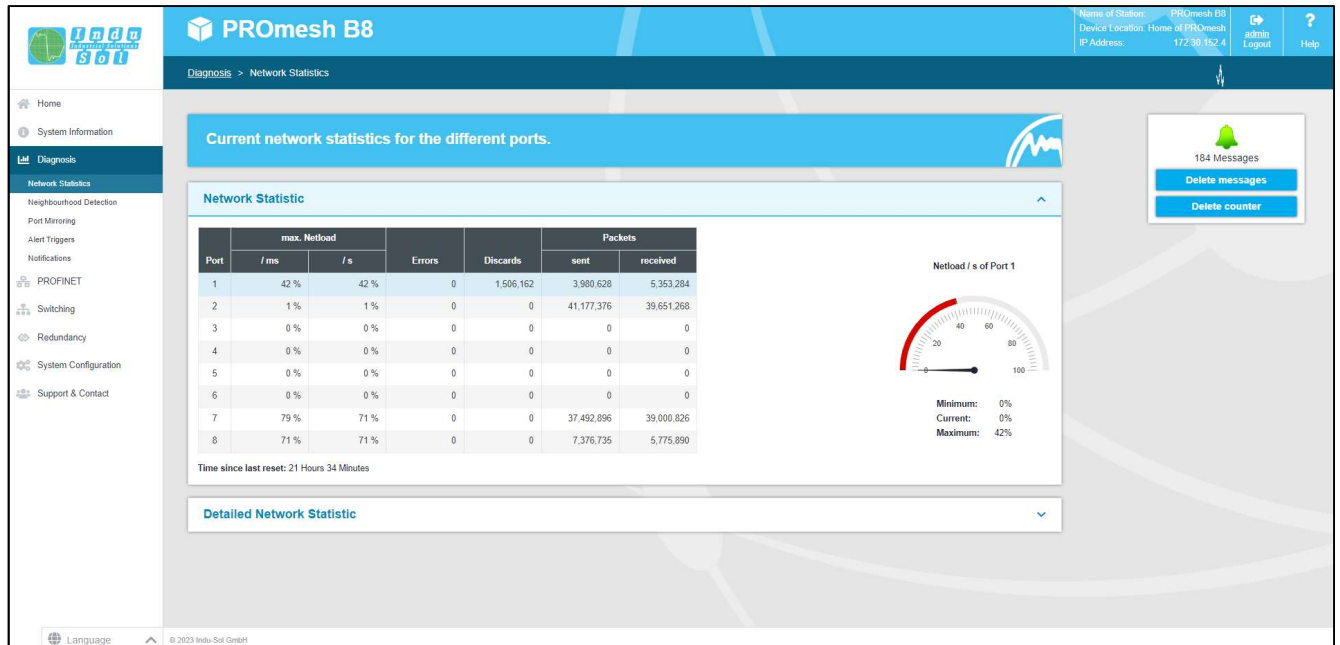- Discards (telegrams discarded due to too much data)

Figure 10: Port statistics

Resetting the values

The upper right part of the web interface contains the "Delete counter" button. The values of the table can be reset with this button.

Detailed port statistics

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

The packets sent are distinguished as follows:

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

The received packets are distinguished between:

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

The line *Packets up to bytes* gives information about the number of packets in different sizes. This records the number of packets received up to 63, 127, 255, 511, 1023, or 1518 bytes in size.

In addition, packet collisions are detected and distinguished by:

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

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

3.6.2 Neighbourhood detection (LLDP)

The Link Layer Discovery Protocol (LLDP) is a vendor-independent layer-2 protocol that provides the ability to exchange information (addresses, names, and descriptions) between neighbouring devices. An LLDP agent operates on every device that supports LLDP. This sends information about its own state at periodic intervals and receives information from neighbouring devices.

Since this is done independently, LLDP is also referred to as 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) where the device-specific LLDP telegram is sent to the neighbouring devices. The default setting is 5 seconds.

3.6.3 Port mirroring

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

Monitoring of the source ports takes place without affecting the traffic of this port. The resulting mirror port can be connected to a LAN analyser or used for diagnosis and debugging.

- 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 enabled, select a port on which to mirror the data. The mirrored packets can be forwarded to exactly one destination port.
- Source port: You can select which ports to monitor and forward their packets to the destination port here. It is possible to route only sent packets (TX for transmit) to the destination port or to monitor both directions, i.e., sent (TX for transmit) and received (RX for receive) packets. You can select a maximum of eight source ports on the switch. Check the respective checkbox to select a port.

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

3.6.4 Alarm trigger

The menu item Alarms 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 power supply voltage
- MRP protocol event
- Exceeding the network load on a port
- Incorrect connected neighbour (can only be configured via the configuration software)
- 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
- PROFINET (only configurable via configuration software)

If one of the alarms set up is detected and triggered, the software will forward the event to the corresponding alarm receiver and document the event as a syslog message.
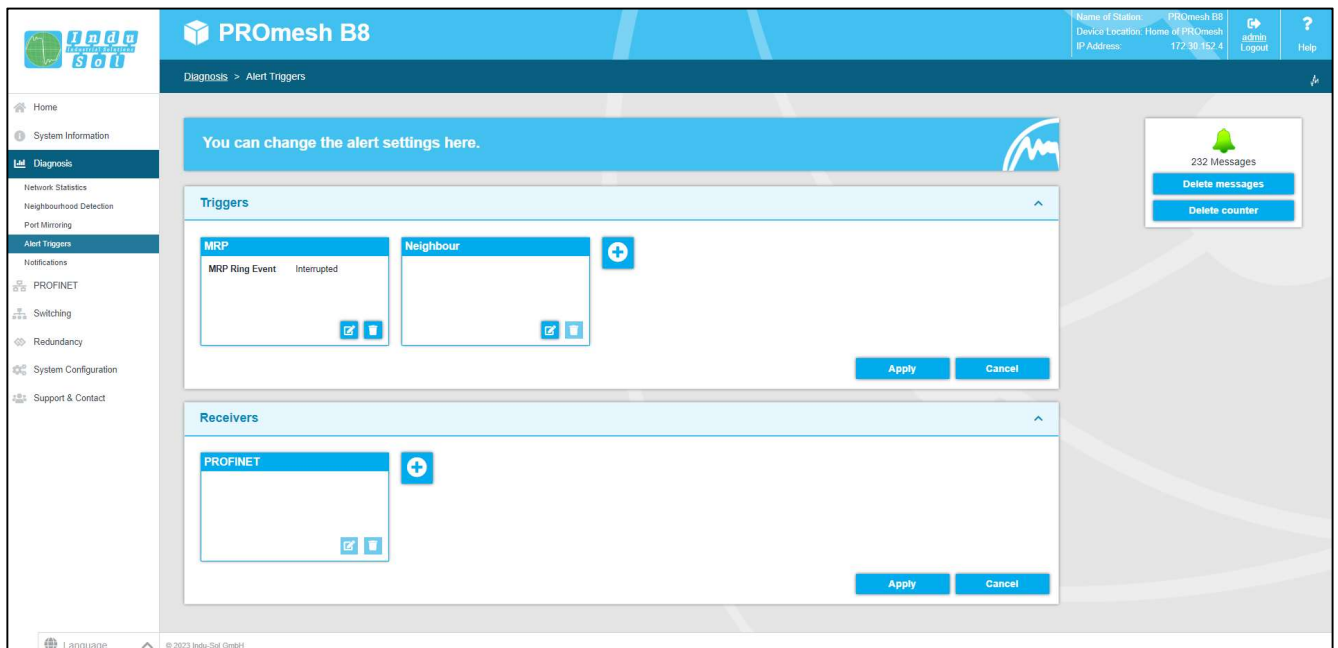
Figure 11: Alarm trigger

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

- Alarm triggers with assigned receivers
- Alarm receivers with associated triggers

Add and edit alarm triggers

New alarms and messages can be added by clicking on the button with the "+" symbol. If alarms are already present, the user has the option of editing or deleting them using a button. In the upper part of the "Alarm trigger" pop-up, the user can select the different alarms. The associated recipients can be selected in the lower part of the pop-up and linked to the alarm trigger in this way when the alarms are set up and edited, provided that the alarm recipients have already been defined.

Adding and editing alarm recipients

New alarm recipients can be added by clicking on the button with the "+" symbol. The relay is already present as an alarm receiver and cannot be deleted, only linked to alarm triggers. The recipient email, SNMP, and PROFINET can be selected as well. The associated alarm triggers can be linked to the current recipient in the lower part of the pop-up.

- Error notifications are generated by the device and sent to a management station without being requested with Simple Network Management Protocol (SNMP). The device cannot determine whether the manager received the information since the packets are not acknowledged.

- The user can specify an email address and an SMTP (Simple Mail Transfer Protocol) server when using the email function. The device sends an email to the user if there is an alarm. Authentication can be enabled as an option. The required access data must be entered for this purpose.

- Once the switch has been integrated and parametrised 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 enabled in the hardware configuration of the controller. If a trigger occurs, the switch sends an alarm message to the controller. This information can then be processed programme-technically within the PLC.

3.6.5 Messages

The messages help the user 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 device, they are no longer available after a device restart or a power interruption. It is possible to use an external syslog server to archive the messages permanently.

Statistics

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

Settings

- Syslog server: Enable this function to save the messages on a syslog server. Enter the syslog server IP address in decimal point notation, select "File" from media type, and save the settings using the Apply button. Check if the server is reachable and saves the messages in a file.

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

3.7 PROFINET

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

The device is developed as a Profinet IO device for connection of decentralised peripherals to a Profinet controller. The device supports conformance Class B. This page offers the option of making port settings for DCP and downloading the configuration file.

DCP settings:

- You can specify for each port whether it supports the discovery and configuration protocol (DCP). DCP is used to distribute addresses and names to the individual subscribers in a Profinet IO system.

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.
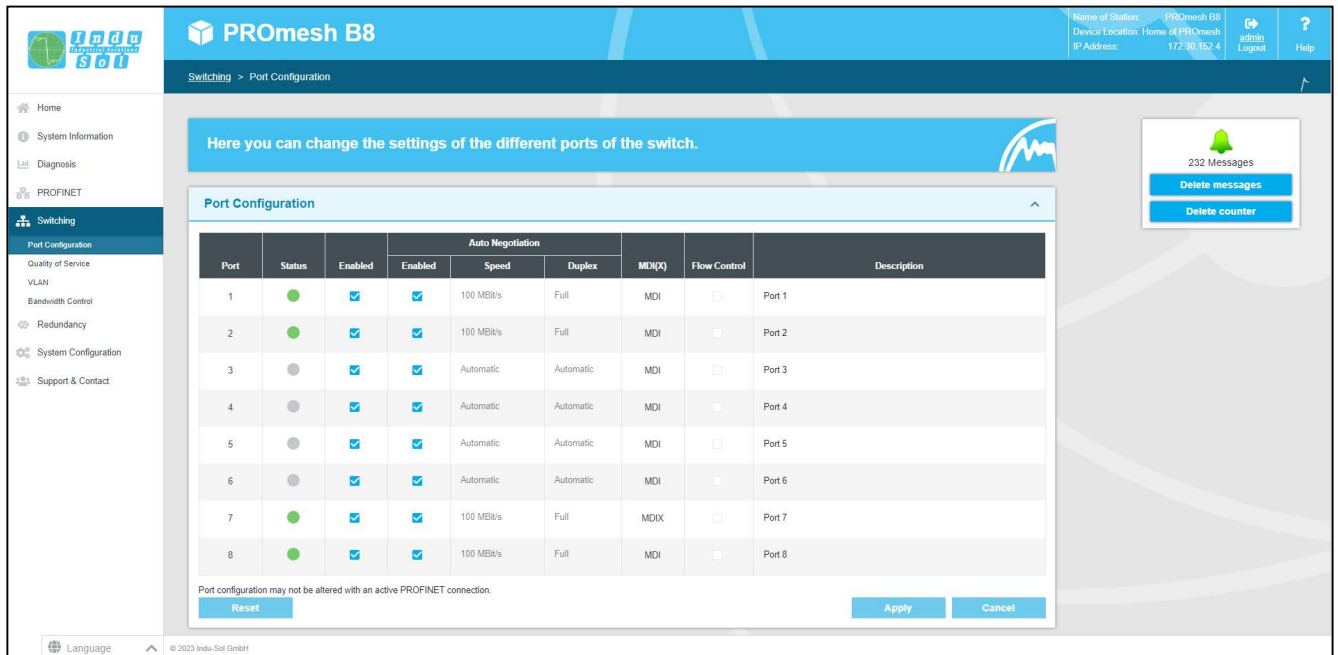
Furthermore, the current state of the device in PROFINET, the PROFINET name assigned as well as its controller (if available) is displayed.

3.8 Switching

This page provides an overview of the enabled and disabled functions in the Switching area. You can see which functions are currently enabled right away. Clicking the Edit button takes you directly to the various pages to 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 can also be edited. The page is regularly refreshed and reloaded.
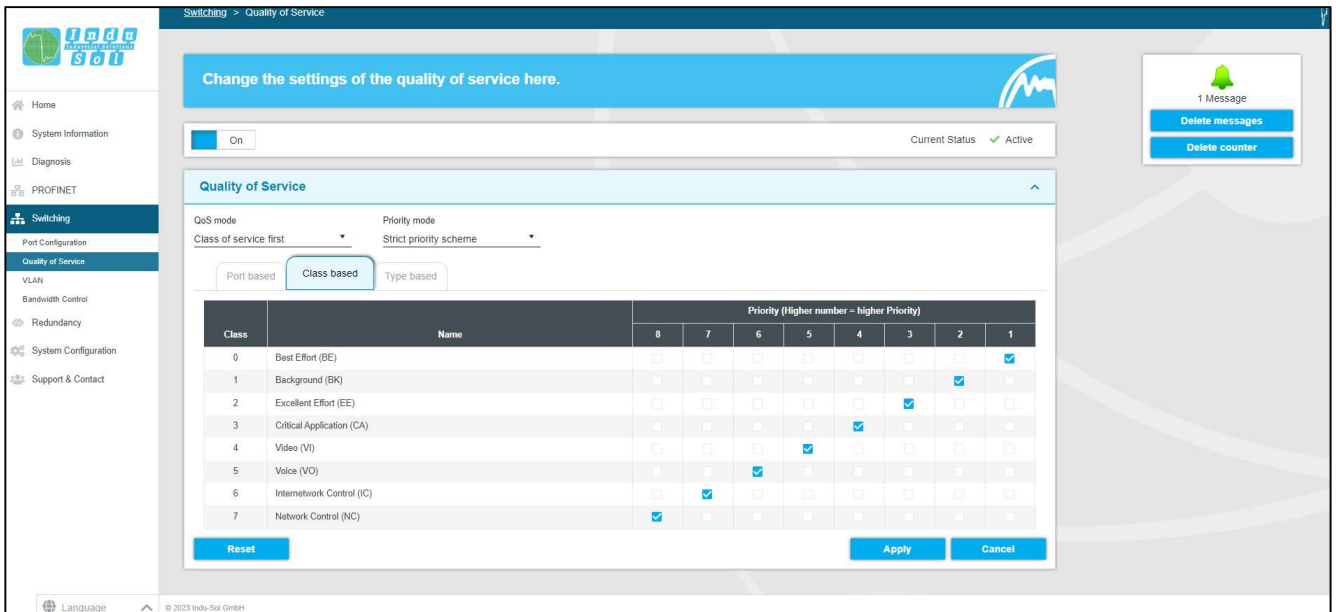
Figure 12: Port configuration

Details on the columns:

- Port: Specifies the port number, also marked on the housing.
- Enabled: The individual ports can be enabled or disabled. This specifies whether a port can be used or not.
- Status: Status signals the current state of the ports:
    o green: The port is enabled and there is a connection.
    o grey: The port is inactive or disabled.
- Autonegotiation: If this function is enabled, the transmission speed and duplex mode are configured automatically. The device and the connected remote party negotiate the settings automatically. If autonegotiation is disabled, the settings can be firmly set manually:
    o Speed: The data rate of the ports can be firmly set. A data rate of 10 Mbps or 100 Mbps can be set.
    o Duplex: Duplex mode can be switched between half and full duplex. This setting is thus set firmly for a connection.
- MDI(X): The device can perform autocrossover detection by default. This means that the switch automatically detects whether the subscriber is connected via a crossed or non-crossed 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: You can give the ports names in this column. The names are displayed throughout the configuration and facilitate the selection of the correct settings as well as diagnosis in the event of a fault. Click the port name to edit the name in the line.

3.8.2 **Quality of service**

Quality of service (QoS) includes all procedures that influence the data flow in the device. With the assignment to queues with different priorities, certain user data can be treated preferentially. For example, real-time data, control data, audio or video data may be preferred over file transfers.

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 13: 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 that port in accordance with your priority.
- Classes based (COS): COS uses a data field present in the VLAN tag with priority information. Eight different priority values from best effort (BE,0-low) to network Control (NC,7-high) are specified. Assign the COS priorities to the switch's four queues as needed in your application.
- Type based (TOS): TOS uses a differentiated services code point (DSCP) data field in the IP header of packets that can have up to 64 different priorities. As with COS, you can use these priorities to prioritize real-time control data, Voice over IP (VoIP), or audio data over normal data transfer, for example. Adjust the settings to your requirements.
- QoS mode:
  - Port-based only: Priorities are based only on the priority of the ports.
  - Class of service only: Priorities are based solely on the class of service data field of the packets.

- o Type of service only: Priorities are based solely on the type of service data field of the packets.
- o Class of service first: In this variant, priorities are determined first by COS, then (if necessary) by TOS, and finally by port.
- o Type of service first: Here, priorities are determined first by TOS, then (if necessary) by COS, and finally by port.
- Priority scheme:
  - o Strict priority scheme: In 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 in the lowest priority queue may never be sent. This mode is recommended when there are very high real-time requirements.
  - o 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 subscribers. It allows the isolation of a network part. Any traffic from network subscribers of a VLAN group is transferred only within the VLAN group.

In the VLAN menu, VLAN settings can be made for each individual port. You can define port-specific in which VLAN a port should have its PVID and for which VLANs the port should be untagged or tagged.

- Tagged : Ports that are configured as tagged in a VLAN provide packets with a VLAN tag. Usually switch - switch connections are configured as tagged. A port can be configured as a tagged port in multiple VLANs. This means that VLANs are not restricted to individual switches, but can also be operated across multiple switches.
- Untagged: Ports that are stored as untagged in a VLAN can receive and forward packets of this VLAN ID. A port can be stored as an untagged port in multiple VLANs if the devices connected to this port shall communicate with multiple VLANs.
- PVID: Only one PVID can be assigned to 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.

Global you can define:

- The management VLAN: The switch itself can be reached via the management VLAN. If the switch is parameterized in a PROFINET controller, an EtherNet/IP scanner or another management software,

then it must be ensured that the management VLAN is located in the same VLAN as the scanner/controller/software.

- VLAN can be deactivated/activated: By default, VLAN is disabled. This causes the switch to operate in the Transparent mode. If VLAN is activated then the switch works in the Bridge mode.

Figure 16: VLAN Configuration

3.8.4 Bandwidth control

Bandwidth control makes it possible 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 the following settings:

- ID: Specifies the port number, also marked on the housing.
- Packet type: Select a packet type to filter by.
  - o All: The specified limits are observed for all packets transported via the port.
  - o Broadcasts: The set limits apply to all broadcast packets (to all devices in the network).
  - o Broadcast & multicasts: The set limits apply to all broadcast and multicast packets (to all or multiple devices on the network).

               o   Broadcast, multicast & unknown unicasts: The limits apply to all broadcast, multicast, and unknown unicast packets (to one subscriber).

- Limit of 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 bBit/s, 4 Mbit/s, and 8 Mbit/s. "No limit" is defined as the default value.

- Outgoing packet limit: 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 "Apply" to save them.

3.9   Redundancy

This page provides an overview of the available redundancy protocols and their status. It is not possible to have multiple redundancy protocols running at the same time, so only one can be enabled. 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.

The use of redundancy protocols guarantees your network increased reliability and availability in the event of a fault. The failure of a component is absorbed, and the subscribers 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 set to shutdown state during normal operation. The subscribers connected in the network operate in a line topology, although it is physically a ring. In the event of a fault, communication can take place via the previously disabled path after a very short recovery time.

MRP uses a redundancy manager that tests the continuity of the ring by means of special test packets and reconfigures the network in the event of a fault and informs the subscribers accordingly. The guaranteed reconfiguration time, with up to 50 devices in the ring, is 200 ms. The reconfiguration time usually is less than 50 ms in a typical application.

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 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 primary ring port.
- Second ring port: Specify a second port to operate as a secondary ring port. Please note that the secondary ring port and the primary ring port must be different.
- This device operates as: Please specify whether the device should 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 for managing mixed structures, including a ring, on the network. It prevents network loops that can result from redundant transmission paths and includes a mechanism for automatic reconfiguration after a device or link failure.

Enable the RSTP function globally before configuring the corresponding parameters.

Root bridge information

The following parameters are displayed in this field:

- Root port: Indicates which port is working as the root port. This port is the shortest path to the root bridge
- Root bridge ID: Identification number of the current root bridge negotiated between the devices.
- 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 the RSTP learning and listening state to the forwarding state. Enter a value between 4 and 30 seconds.
- Maximum age: The amount of time a bridge waits before attempting to reconfigure 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 allowed.
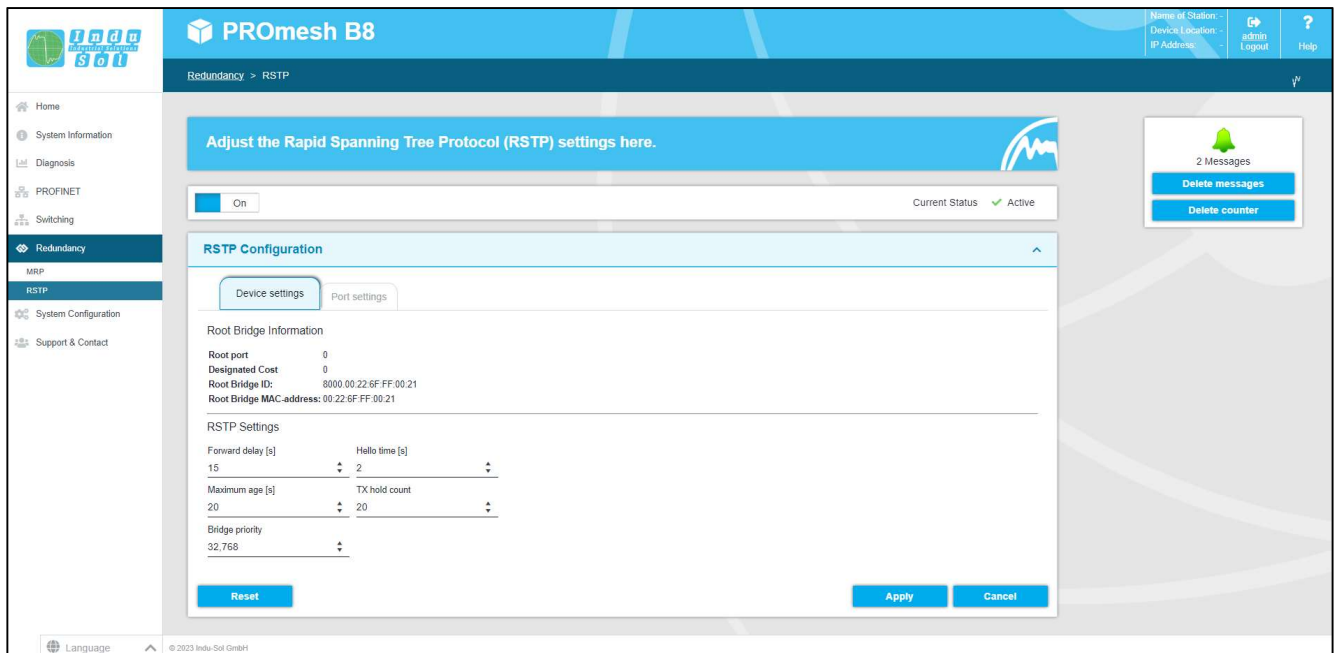
Figure 14: Device settings RSTP

Notice: 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 "Hello Time" and calculate with the formula 2 * (Hello Time + 1) in accordance with the rule given above to get the lower limit of the Maximum Age. Select a value for "Forward Delay Time" and use the formula 2 * (Forward Delay Time – 1) of the above rule to calculate the upper limit of the Maximum Age. Then select a Maximum Age between 6 and 40 seconds, which lies 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 each ports individually.
- RSTP on: For each port, select whether or not to enable the Rapid Spanning Tree Protocol on that port.
- Status: Displays the current status of each port. The following are distinguished:
  - 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 way to the root bridge.
  - Designated port: A port in the forwarding state that allows communication to other bridges in the spanning tree.
  - Alternate port: An alternate path to the root bridge, 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 without any operational function in the tree structure.
- Priority: This allows the assignment of higher priorities to certain ports to influence the tree structure. Enter a number from 0 to 240. The value must be a multiple of 16.
- Costs: The cost from the sending bridge on the respective port of another bridge. Enter a number from 1 to 200,000,000. You can use this parameter to influence the structure of the tree.
  - defined: The cost of a connection to the root bridge can be specified.
  - designated: The designated costs are calculated by the RSTP and displayed here.
- Edge port: Specifies a port 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. They speed up the reconfiguration time of the redundancy protocol by setting edge ports fixed.
  - Force: The port is configured as an edge port by default.
  - Auto: Edge ports are detected is automatically.
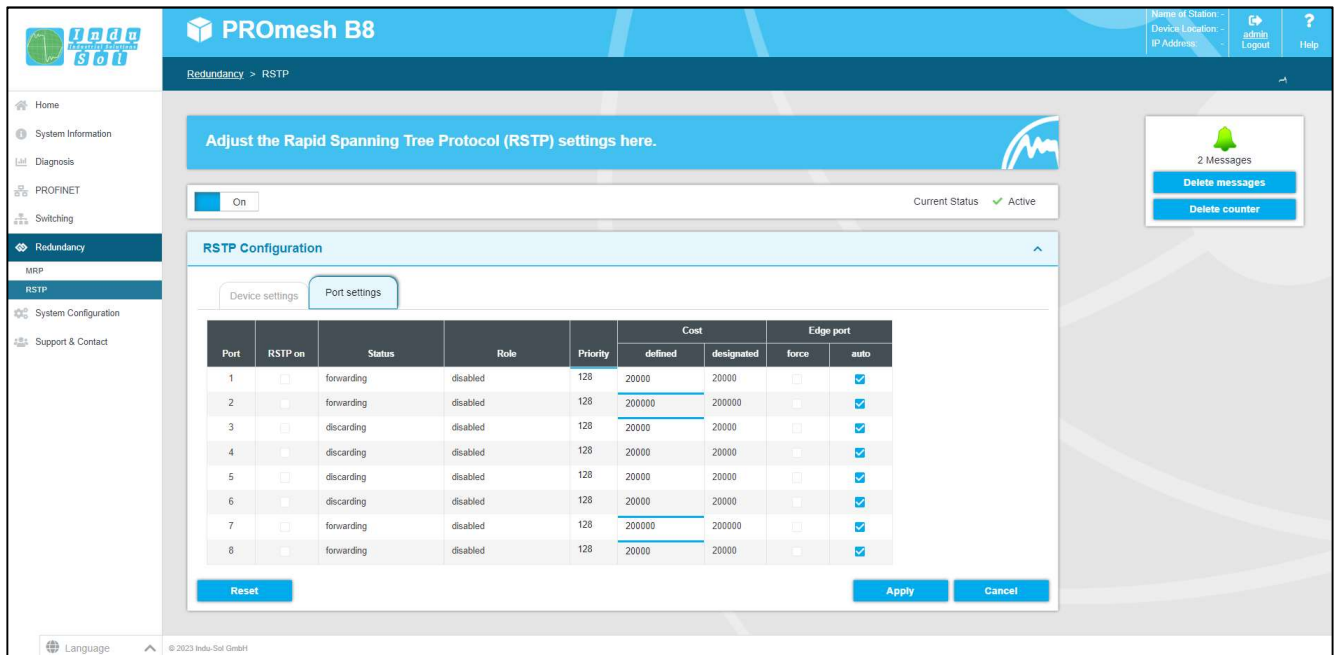
Figure 15: Port settings

Click Apply to apply the settings after you have set the respective parameters.

3.10 System configuration

The system configuration page displays IP address settings, time settings, access options to the device, and general device information.

This page is to provide a concise view of the system configuration menu to help you understand how the device works and where action is needed.

You can switch directly to the corresponding protocols and functions in order to make the other settings there with the respective Edit button.
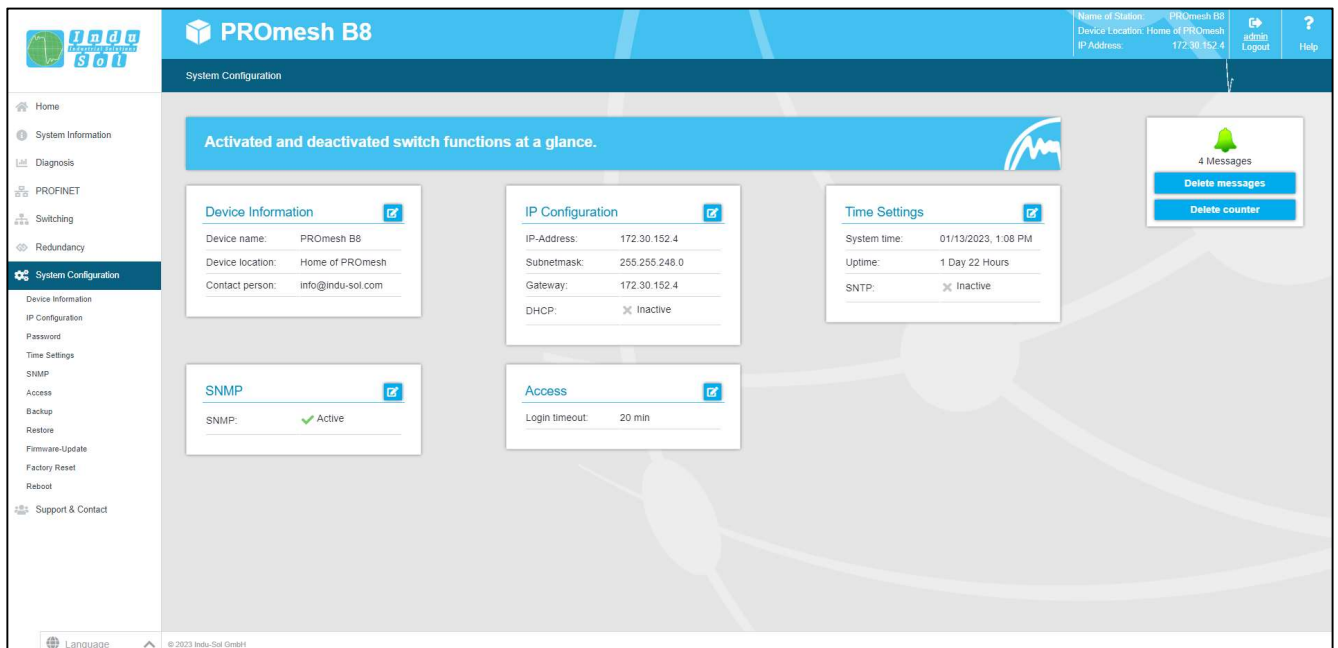
Figure 16: System configuration

3.10.1   Device information

The device information page allows you to assign a unique device name, installation location, and contact person to the device.

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

The input fields are configured so that you may use up to 50 characters. Special characters may be used. The device name and installation location are displayed in the information bar at the top right and help you to keep track of the device.

3.10.2   IP configuration

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

PROFINET

If the device is configured in a PROFINET network, the device receives its IP configuration from the PROFINET controller. The IP configuration cannot be performed automatically or manually with an existing PROFINET connection.

Automatic

Select the checkbox "automatic (DHCP)" to get a configuration of the IP address, the subnet mask, and the default gateway from a server working in the network with corresponding function.

The device sends a request to the server and adopts the configuration received from the DHCP server after you have saved the settings by clicking on the Apply button. The device can no longer be reached via the default IP because now has a new IP address. 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, disable 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 device 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 defines which IP addresses can be reached directly by the device and which addresses must be addressed via a gateway.
- Gateway: Enter a default gateway. The gateway is used to communicate with devices outside your subnet.

Please check the settings carefully to avoid 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 default password for the users Admin and User can be changed. The usernames and rights of the administrator and the user are fixed and cannot be changed.

Form fields

- New password: Enter the password set for the previously selected user in this field. Please also note the information on assigning passwords in the section below.

- Confirm password: Repeat the password in this field to make sure that you have entered your password correctly.

- Current password: Please enter your current password here 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. Therefore, passwords generally should:

- not to use dictionary entries
- be as complex as possible
- use combinations of letters, numbers, and special characters
- use lower- and upper-case letters
- have at least eight characters
- never be written down

3.10.4 Time setting

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

- Automatically (SNTP)

- Manually

. Furthermore, the PROmesh B8 can be used as a time server to provide other devices with the current system time.
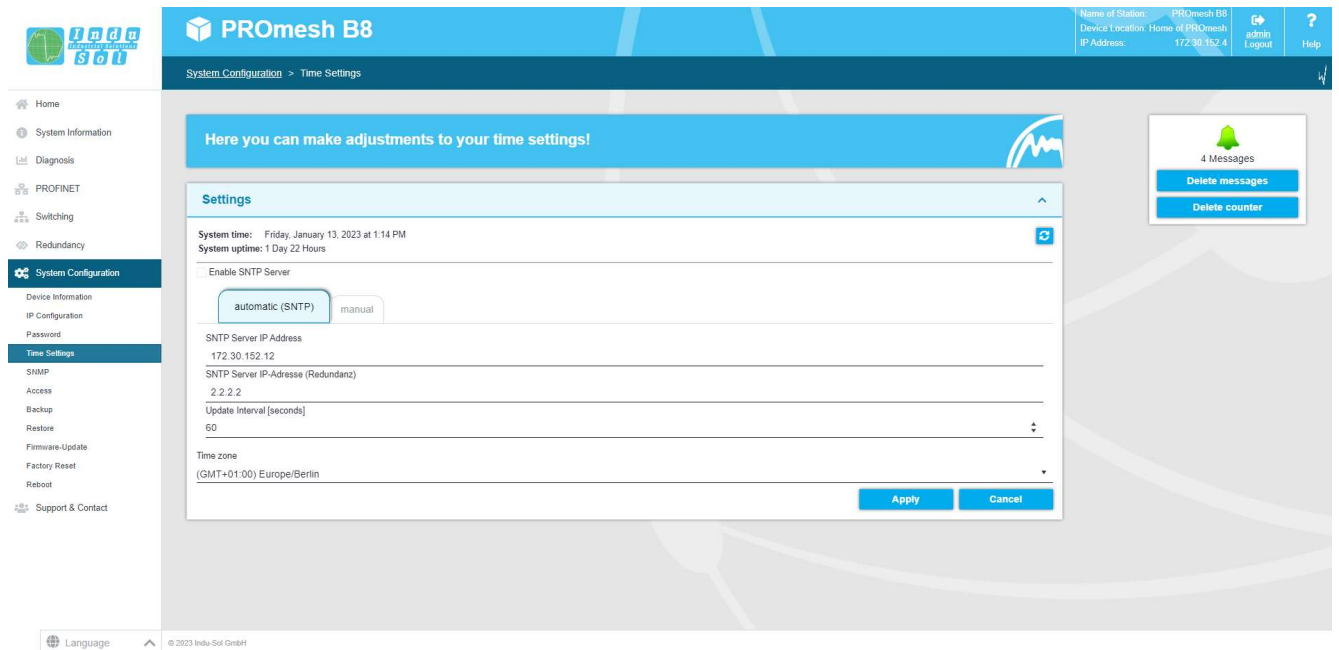
Figure 17: Time server

Automatically (SNTP)

- SNTP Server: Store the IP address of the time server. It is possible to store a second time server as redundancy.

- Update interval: You can determine the cycle in which the device time is synchronised with the time server here.

- Time zone: Then select your valid time zone

Manual

This setting lets you manually enter the current date and time by clicking the calendar icon.

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

3.10.5 **SNMP**

The Simple Network Management Protocol (SNMP) controls 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: Indicates which community strings are currently enable and which are not.
- Community string: The accesses are defined by unique names that you can change.
- Read only: The community string allows read-only access.

- Read and write: The community string allows read and write access.

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

Creating SNMP access

Click the "Add" button to create a new community string. 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 device supports SNMP versions V1, V2C, and V3. Select the desired version.

The following additional settings are required for SNMP V3:

- Username: Assign a username here.

- Examination: 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 granted by the configured access.

3.10.6   Access time

Settings

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

Save your settings with the "Apply" button.

Furthermore, you can:

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

3.10.7 **Backup**

This menu item allows you to back the current configuration of the device up in a file. The backup can be saved as a download.

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

- Download: The backup file will be stored in the browser's download directory, or the user can specify a path where the file is then saved.

3.10.8 **Recovery**

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 as an upload.

- Upload: The backup file is located on the computer currently in use and is transferred from there to the device.

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.
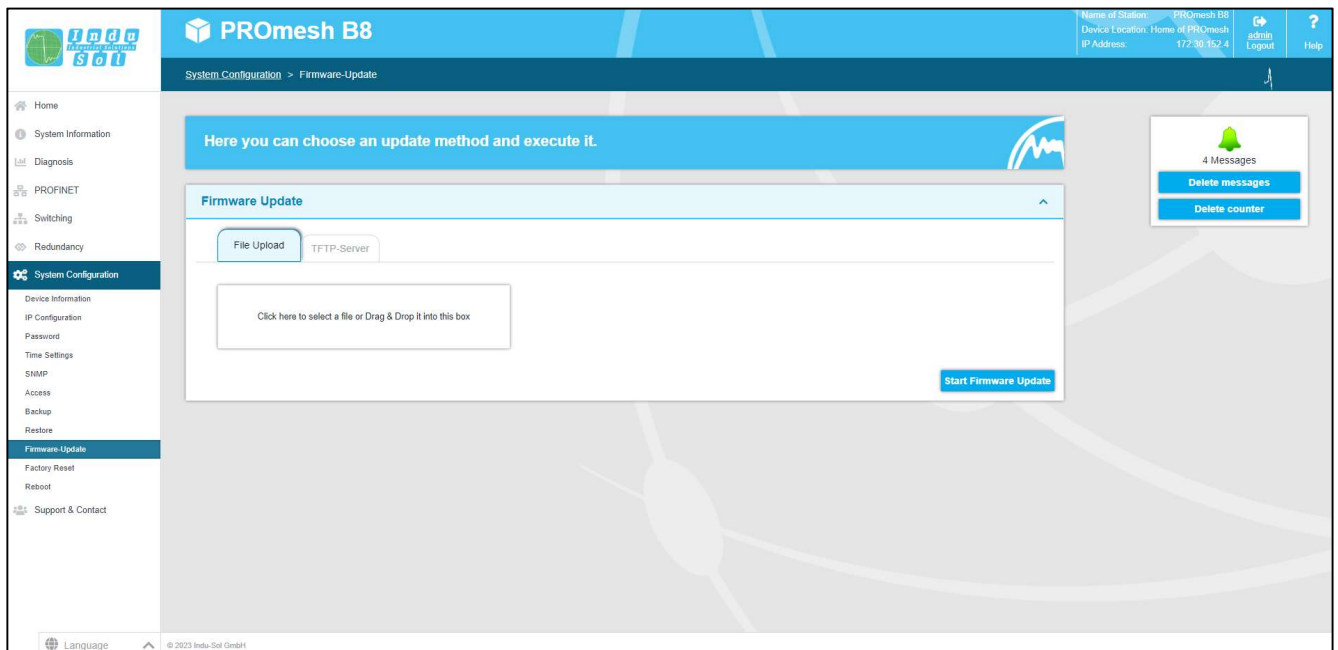
Figure 18: Firmware update

The firmware file is either provided by a TFTP server or uploaded to the device. 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 device.
- TFTP server: The firmware update is downloaded from a TFTP server on the network.

Preparation:

It is not recommended to perform the update if the MRP protocol is enabled. Please open the MRP ring first by pulling out one of the cables and then disable the media redundancy protocol. Now perform the firmware update.

Settings

- TFTP server IP address: Specify 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 specify the name relative to the root directory of the server.

Use the button "Start firmware update" to execute the action and confirm it in the window that opens. Please make sure that the firmware update can be executed completely.

Important:

Do not perform the following actions while the firmware update is in progress.

- Do not disconnect the device from the power supply voltage under any circumstances.
- Do not pull or change any network connectors.

A message will tell you when the update is complete. The device will restart automatically at that point.

3.10.10 Factory settings

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

Click the "Reset to default" button for this and confirm it in the window that opens. The device must then be rebooted.

3.10.11 Reboot

You can restart the switch to perform a software reset here. Pressing the reboot button will exit the switch software and reboot the device.

You can also turn both power supply voltages of the switch off and on again to perform a hardware reset.

3.11 Support

The support section contains all relevant contact information for Indu-Sol

License information

The linked license.txt file contains information regarding the "Open Source Software" used.

3.12 Troubleshooting advice

- 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. The link LEDs must light up when a connection is established and flash when data is being transmitted.
- If in doubt, disconnect redundant network structures and reset the *PROmesh B8* switch to factory settings. Make your settings again bit by bit and observe where the error occurs if the communication works afterwards.

4 Technical specifications

Network connections	8 x up to 100 Mbit/s RJ45
Power supply	12 V ... 36 V DC redundant power supply
Power consumption	Maximum 11,5 W
Dimensions (HxWxD)	138 mm x 53 mm x 110 mm
Weight	0.7 kg
Housing	Metal, painted
Storage temperature	-10 °C ... 60 °C
Operating temperature	-10 °C ... 60 °C
Humidity	Humidity 5% ... 95% RHD non-condensing
Protection class	IP20 (not evaluated by UL)
Assembly	35 mm DIN top-hat 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 packets only or TX and RX packets
Firmware update	TFTP server, from local PC
Bandwidth contr.	Incoming and outgoing
DHCP client	DHCP client function to obtain an IP address from the DHCP server