Indu-Sol GmbH – Specialist in Industrial Networks

PROmesh P10

User Manual

PROFINET/Ethernet Switch

Indu-Sol GmbH

Blumenstraße 3

042626 Schmölln

Tel.: +49 (0)34491 / 58 18 0

Fax: +49 (0)34491 / 5818-99

E-mail: info@indu-sol.com

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

Our **Technical Support** team can be contacted at +49 (0)34491 / 58 18 14, on workdays from 7:30 a.m.– 16:30 p.m. (CET). Or 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, under the following telephone number:
+49 (0)34491 / 58 18 0.

Revision overview

Date	Revision	Change(s)
01.10.2020	0	First version

We reserve the right to amend this document without notice. We continuously work on further developing our products. We reserve the right to make changes to the scope of supply in terms of form, features and technology. No claims can be derived from the specifications, illustrations or descriptions in this documentation. Any kind of reproduction, subsequent editing or translation of this document, as well as excerpts from it, requires the written consent of Indu-Sol GmbH. All rights under copyright law are expressly reserved for Indu-Sol GmbH.

WARNING

This device may only be put into operation and operated by qualified personnel. Qualified personnel, as referred to in the safety-related information of this manual, are persons who are authorised to put into operation, to earth and to label devices, systems and electrical circuits in accordance with the standards of safety engineering.

Improper use or configuration of the ***PROmesh P10*** in the network can lead to severe bodily injury as well as property damage due to uncontrolled machine movements.

Contents

1 General information

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

1.1 Overview of the *PROmesh P10* – functionality

The ***PROmesh P10*** is an industrial Ethernet switch with management and PROFINET functions that can be easily and conveniently configured via a web application. Thanks to its extensive functions with cut-through technology, it helps you to effectively set up all network topologies, such as bus, star and ring structure, in your system.

Features:

- Web application for configuration
- 12-36 V DC supply, protected against polarity reversal, redundant operation possible
- Cable diagnostics
- Leakage current monitoring
- Port statistics (Network Limit in ms, Errors, Discards)
- Alarm management
- 8 x 10/100/1000 mbps RJ45
- 2 x 100/1000/2500 mbps SFP
- Switch Technology: Cut-through
- 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 packages
- Port mirroring (Rx / Rx and Tx packages)
- Port-based VLAN with 4096 possible VLAN IDs
- Simple Network Time Protocol (SNTP)
- Simple Mail Transfer Protocol (SMTP)
- Internet Group Management Protocol - Snooping (IGMP-Snooping)
- Dynamical Host Configuration Protocol (DHCP) client function
- Simple Network Management Protocol (SNMP), v1, v2c
- Updating, saving and backing up the system configuration via web interface, TFTP and memory card

1.2 Scope of supply

The scope of supply comprises the following individual parts:

- ***PROmesh P10***
- 7-pin plug-in terminal block, 2.5 mm² (power supply and alarm contact)
- Quick-start user guide (hardcopy)
- USB stick with following files: Manual (PDF), user quick-start user guide (PDF), service tool (ZIP), switch explanation video (MP4)
- SD card, for backup and update

Please check that the contents of your delivery are complete prior to commissioning. If you have questions, promptly contact our technical support team prior to commissioning.

Prior to the first commissioning, insert the external memory card into the appropriate slot on the rear of the device (see Figure 1).

1.3 Safety information

Prior to commissioning the device, check that it is in perfect order on the outside. If you suspect that the PROmesh P10 has been damaged, send the device back to your supplier immediately and do not commission the device. Our technical support team will be happy to answer any questions you might have.

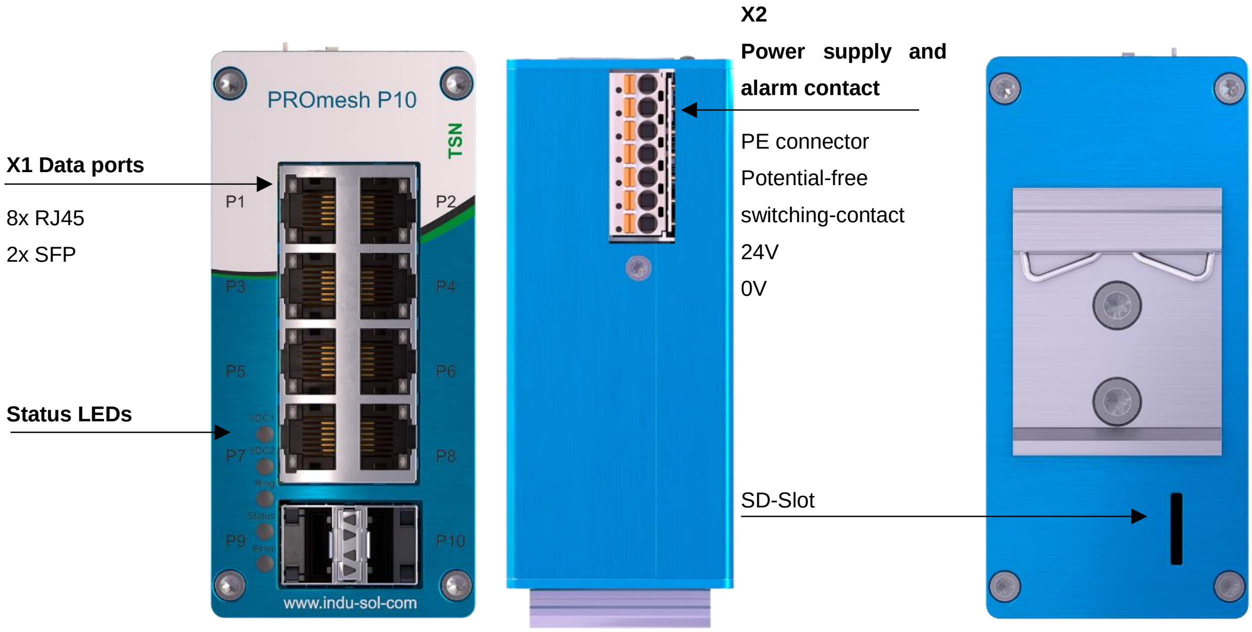
The ***PROmesh P10*** was developed for use in PROFINET applications in acc. with Conformance Class B. To achieve complete compliance with the PROFINET standard, also observe the standard's specifications regarding the selection of the data wiring used.

Also pay attention to the technical specification of the device, to ensure safe and optimal use. The device has been developed for IP30-compliant protective environments. If you use the device in a different environment, take suitable measures to ensure proper operation of the device.

Do not open the housing. No serviceable parts have been installed. Opening the housing without authorization voids all warranty claims.

2 Device ports and status indicators

Device ports



X1 Data ports

8x RJ45

2x SFP

Status LEDs

X2
Power supply and alarm contact

PE connector

Potential-free switching-contact

24V

0V

SD-Slot

Figure 1: Device ports

2.2 Installation

The PROmesh P10 has been designed for individual use in different kinds of control cabinets and can be mounted on a standard 35 mm DIN top-hat rail.

Use only the provided top-hat rail fasteners to mount the device, or, if necessary, purchase appropriate spare parts to guarantee adequate electrical contact and the withstanding of mechanical stress by the device.

2.3 Installation instructions

The ***PROmesh P10*** is installed horizontally inside the control cabinet on a 35 mm top-hat rail in accordance with DIN EN 60715.

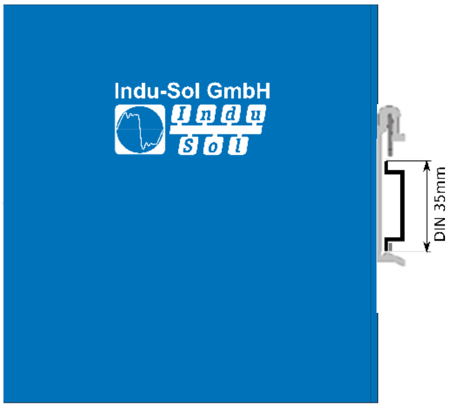


Figure 2: Side view, with connection terminal on the right

The following distances must be maintained from other modules for correct installation:

- From left and right: 50 mm
- From top and bottom: 50 mm

Installation and removal of the device is displayed in Fig. 4.

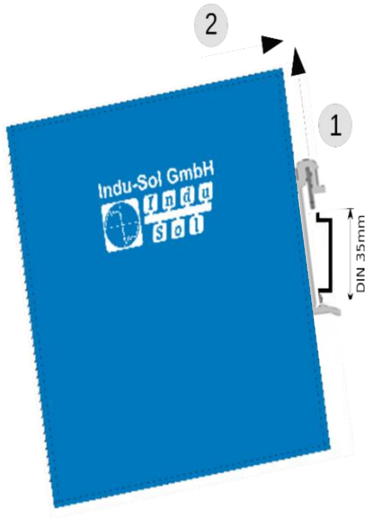


Figure 3: Installation on and removal from the top-hat rail

Do not mount the ***PROmesh P10*** switches directly next to devices that emit strong electromagnetic interference fields, such as transformers, contactors, frequency inverters, etc.

Do not mount the ***PROmesh P10*** switches directly next to devices that generate a lot of heat and protect the switch against direct sunlight to prevent undesirable warming up. Protect the PROmesh P10 against additional heat radiation and observe the approved temperature range for storage and operation.

2.4 Voltage supply connection and fault relay

Operate your ***PROmesh P10*** with a nominal voltage of DC 12 V to 36 V. To safeguard your system availability, connect the redundant voltage supply VDC1 and VDC2 with the appropriately marked terminals of the supplied 7-pin terminal block adapter (VDC1, GND, as well as VDC2, GND). The voltage needs to be an SELV/LPS-compliant voltage in acc. with IEC 60950-1 / EN60950-1 / VDE0805-1.

The 7-pin 2.5 mm² terminal block at the top of the device is assigned as follows:

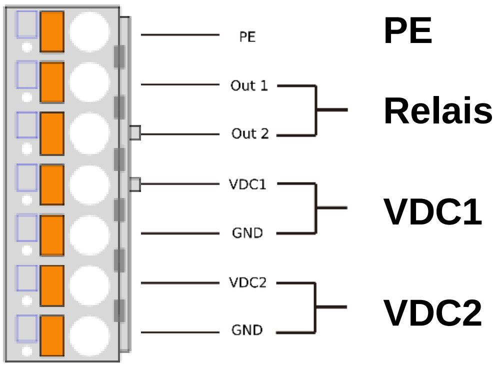


Illustration 4:Assignment of terminal block

The labelling shown is also present on the supplied terminal block.

There is a potential-free fault relay contact (opener) at the device-internal OUT terminal. The relay serves as an alarm receiver and can be linked in the software with various alarm triggers. Depending on the configuration, the relay contact then opens for example in case of a voltage drop or a status change of the port.

2.5 LED indicators

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

Additionally, each of the 10 data ports feature two status LEDs.

The LEDs show the most important diagnostic information regarding the device and connection status of the PROmesh P10 in your PROFINET network (see Table 1).

LED	Status	Meaning
VDC1	Green	Voltage at terminal is sufficient
	Off	Voltage at terminal is not sufficient
VDC2	Green	Voltage at terminal is sufficient
	Off	Voltage at terminal is not sufficient
Ring	Green	The switch is manager in the MRP ring
	Off	The switch is not a manager in the MRP ring
Status	Green	Active PROFINET connection to the controller
	Yellow	No PROFINET connection to the controller
Error	Red	Voltage failure, port fault or configurable alarm active
	Flashing	No voltage failure, no port fault and no configurable alarm active
LED 1 port 1-8	Off	No link
	Flashing	Link + data exchange (flashing speed indicates link speed)
	On	Link
LED 2 port 1-8	Off	Port speed 10 mbps
	Flashing	Port speed 100 mbps
	On	Port speed 1 Gbps
LED 1 port 9-10	Off	No link

	Flashing	Link + data exchange (flashing speed indicates link speed)
	On	Link
LED 2 port 9-10	Off	No link
	Flashing	Port speed 2.5 Gbps
	On	Port speed 100 mbps or 1 Gbps

Table 1: LED functions

2.6 Reset button

If the PROmesh P10 is out of reach due to unforeseen problems, the reset button can be used. With the help of the reset button, the PROmesh P10 can either be restarted or reset to its factory settings. For this, the following procedure is necessary:

- Restart device: Press reset button for 1 second
- Reset device to factory settings: Press reset button for at least 8 seconds

2.7 Network integration and commissioning

2.7.1 Data ports

The ***PROmesh P10*** is equipped with 10 data ports which enable data transmission at up to 2.5 Gbps in conformance with PROFINET Standard 2.4. The actual baud rate is negotiated by the device using auto-negotiation.

The two SFP slots are used to install SFP transceiver modules and thus make flexible integration with the media type that you need possible (copper, multi-mode fibreglass, single-mode fibreglass).

The proper functioning of the SFP ports can only be guaranteed with SFP modules from the manufacturer Indu-Sol.

2.7.2 Media selection and connection

In addition to the 8 data ports for connecting RJ45 copper lines, the PROmesh P10 is equipped with two additional data ports for connecting Mini GBIC transceiver modules in acc. with the SFP INF standard.

This makes it possible to flexibly integrate the PROmesh P10 into your automation network by using different media types, such as copper lines, single-mode fibreglass lines and multi-mode fibreglass lines in duplex mode.

When laying out, selecting, assigning and assembling your data line, pay attention to the pertinent standards and make sure fixed connections are used for applying the connectors; this is necessary in order to ensure the max. possible cable lengths and cascading of network segments in acc. with your media type (copper, optical fibres, etc.).

2.7.3 Cabling

To connect your PROmesh P10 via the existing RJ45 data ports, use 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 connector from Indu-Sol to improve the shield contact.

2.8 Network topologies & Redundancy

By employing various protocols, the devices of the ***PROmesh*** product family can be implemented in star-shaped switched-Ethernet networks as well as in redundant networks such as intermeshed networks or rings.

2.8.1 Network topology

Typical Ethernet star structures (see Figure 5) can be networked with the ***PROmesh P10*** switches without further configuration. The devices are operable immediately.

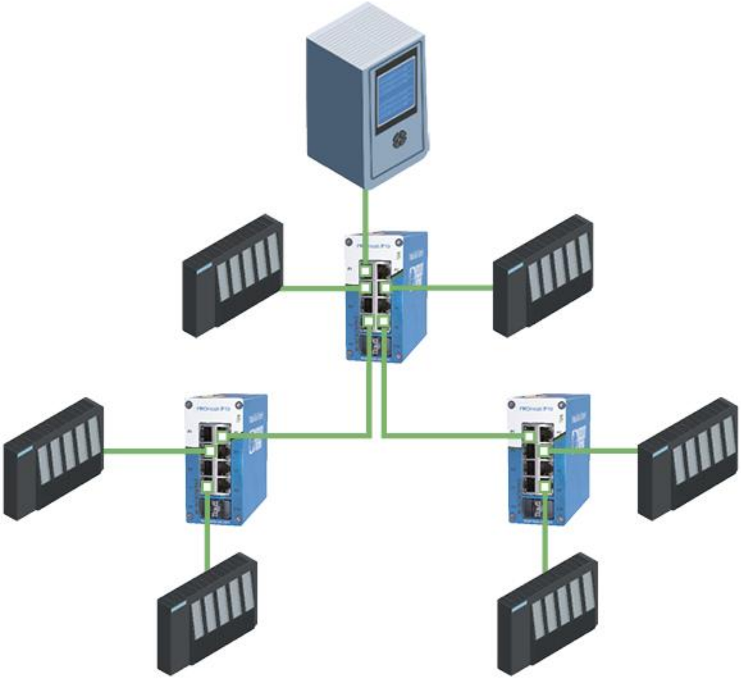


Figure 5: ***PROmesh P10*** in a star-shaped network

2.8.2 Ring structure

The ***PROmesh P10*** fully supports the IEC 62439 standard and enables deterministic convergence of the information forwarding with simple redundancy (ring topologies, see Figure 7). Depending on your system size, convergence times of max. 200 ms thus become possible.

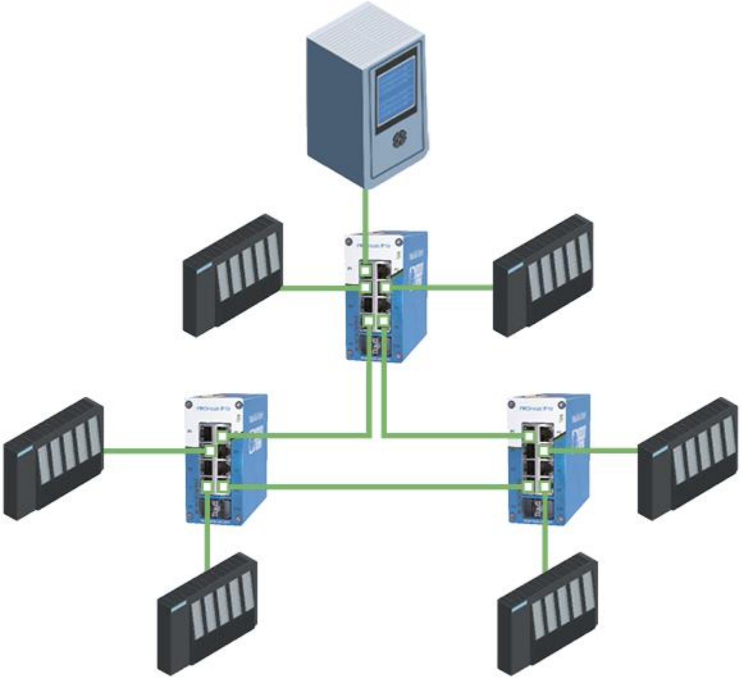


Figure 6: *PROmesh P10* in a ring-shaped network

3 Web application

The ***PROmesh P10*** switches are equipped with a modern web interface by which they can be conveniently configured from any web browser.

3.1 Preparations

Install the ***PROmesh P10*** switch in the network before you use the web management and make sure that the PC intended for the configuration of the switches can access the switch via the web browser. The PROmesh P10 and the client PC to be connected have to be in the same IP address range and IP subnetwork. To this end, you first have to assign an appropriate IP Address to your PROmesh P10.

In delivery status of the device, the following IP address, subnet masks, administrator user name and administrator password have been set:

• IP address:	**0.0.0.0**
• Subnet mask:	**0.0.0.0**
• Gateway:	**0.0.0.0**
• User name:	**admin**
• Password:	**admin**

It is mandatory to change the factory default password immediately after the first log-in. It is your responsibility to document this password and protect it against unauthorised access.

The setting of your intended user addresses can be conducted easily with the **Indu-Sol ServiceTool**. This is available for download, free-of-charge from the following link:
https://www.indu-sol.com/servicetool

Our software is updated regularly. Make sure that you have the current version.

After installing and opening the software, establish a network connection from your computer to one port of the switch and scan the system with the search setting *PROFINET device*. Afterwards, you can enter and save the corresponding entries in the input mask.

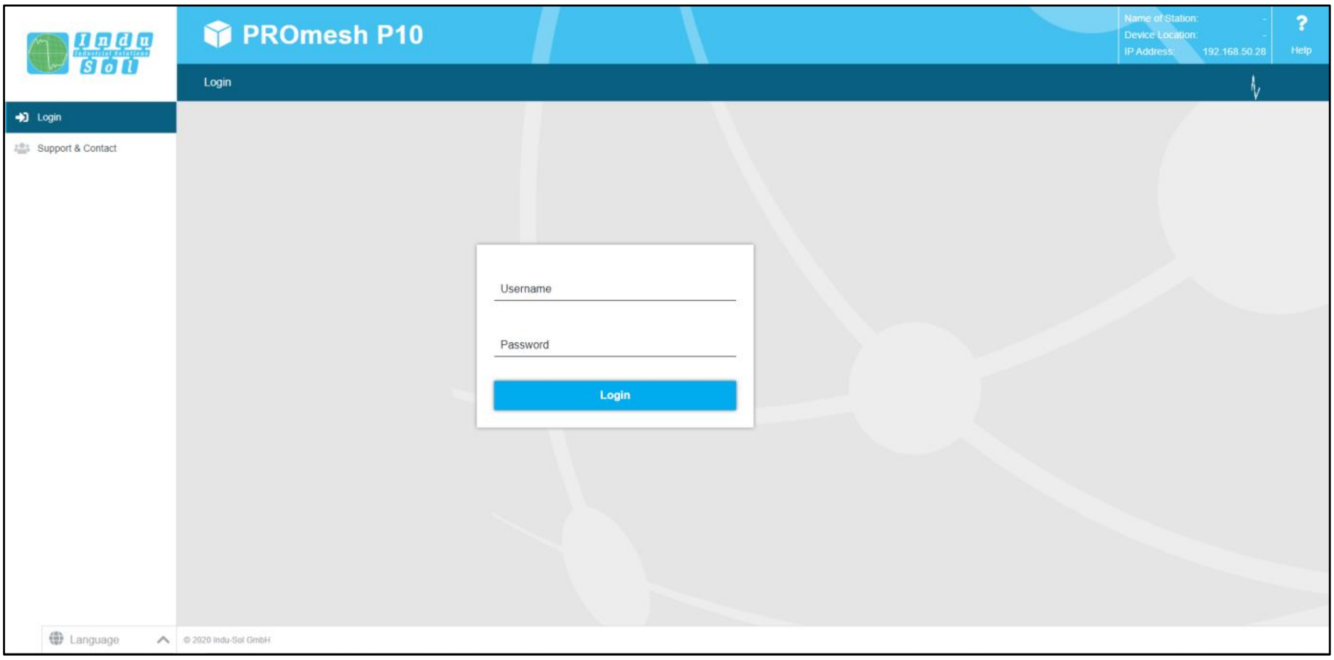
If, in a PROFINET system, you include the switch in the hardware configuration of the controller, the appropriate address settings are automatically carried out via the controller afterwards.

As an alternative to the administrator access, there is a user access available with reduced rights and adjusted menu. The user has no access to the switching and maintenance function as well as their sub-items. The access data for this is:

- User name:	**user**
- Password:	**user**

3.2 System login

1. Start a web browser on your computer.
2. In the address bar of the web browser, enter the IP address that you use for the ***PROmesh P10*** switch and confirm by pressing the *Enter* button.
3. The login mask of the device then appears on the screen.



Name of Station: -
Device Location: -
IP Address: 192.168.50.28

Figure 7: Login mask

4. Select the desired menu language (DE / EN). This can be changed at any time in every menu of the web interface.
5. Then enter the user name and password.
6. Press the *Enter* button or click on *Log in* to get to the web interface of the switch.

3.3 Web interface

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

✓ **No fault:** Communication is functioning without any problems.

! **Warning:** At least one communication fault (discard, error) has occurred at the corresponding port, which has not led to a failure yet. The sources of these events should be localised and resolved.

Fault: A critical fault has appeared at the corresponding port, and this fault leads to an interruption of communication. Urgent action is required to resolve the fault.

No communication is taking place at the respective port. Either there is no device connected (possibly also line interruption) or no telegram traffic can be detected (serious malfunction in the network) or the devices no longer communicate.

3.4 Start

After having logged in successfully, you arrive at the main overview with the information bar in which the device name, the installation site and the IP address can be viewed. The current user is displayed under the logout button on the right end of the bar. Press this button to log out. The Help button will show you information and explanations for the individual pages.

In the Port Statistics you will see an overview of the status of the available ports since the start or reset of the switch (history) and within the last minute (current). You can choose between two views. The overview shows:

- Current partner
- Transmission speed
- Diagnostic messages.

Besides the parameters of the overview, the Details view also shows:

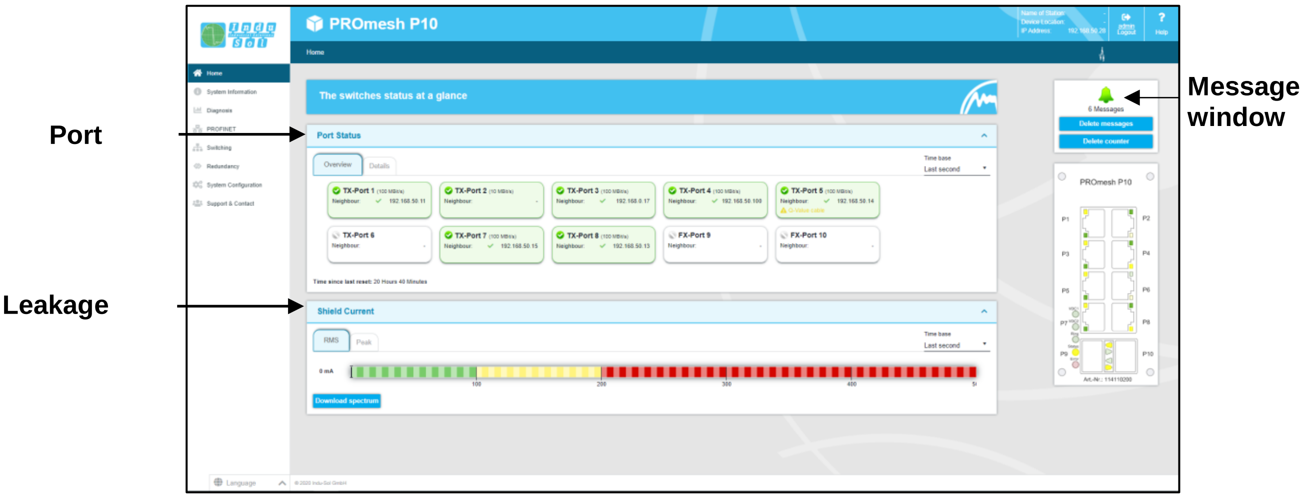
- Network Limit per s
- Network Limit per ms
- Discards
- Errors
- Cable quality value

The number of messages that occurred is displayed in the Messages window. The entries in the Message list are opened automatically with a mouse click on the alarm bell. The messages as well as the counter reading of the ports can be deleted by the respective buttons.

The overview of the leakage current presents the current current value between the RJ45 port and the top-hat rail of the device. For this, you can switch between the peak value (Peak) and the effective value (RMS). Interference currents, which can lead to direct communication problems, are made visible early on by this information.

To enable correct measurement of the leakage current, the top-hat rail has to be earthed correctly.

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



Name of Station: -
Device Location: -
IP Address: 192.168.50.28

The switches status at a glance

Port Status

Time base: Last second

TX-Port 1 (100 MBit/s) Neighbour: ✓ 192.168.50.11
TX-Port 2 (10 MBit/s) Neighbour: -
TX-Port 3 (100 MBit/s) Neighbour: ✓ 192.168.0.17
TX-Port 4 (100 MBit/s) Neighbour: ✓ 192.168.50.100
TX-Port 5 (100 MBit/s) Neighbour: ✓ 192.168.50.14 ⚠ Q-Value cable
TX-Port 6 Neighbour: -
TX-Port 7 (100 MBit/s) Neighbour: ✓ 192.168.50.15
TX-Port 8 (100 MBit/s) Neighbour: ✓ 192.168.50.13
FX-Port 9 Neighbour: -
FX-Port 10 Neighbour: -

Time since last reset: 20 Hours 40 Minutes

Shield Current

Time base: Last second

0 mA

6 Messages

PROmesh P10

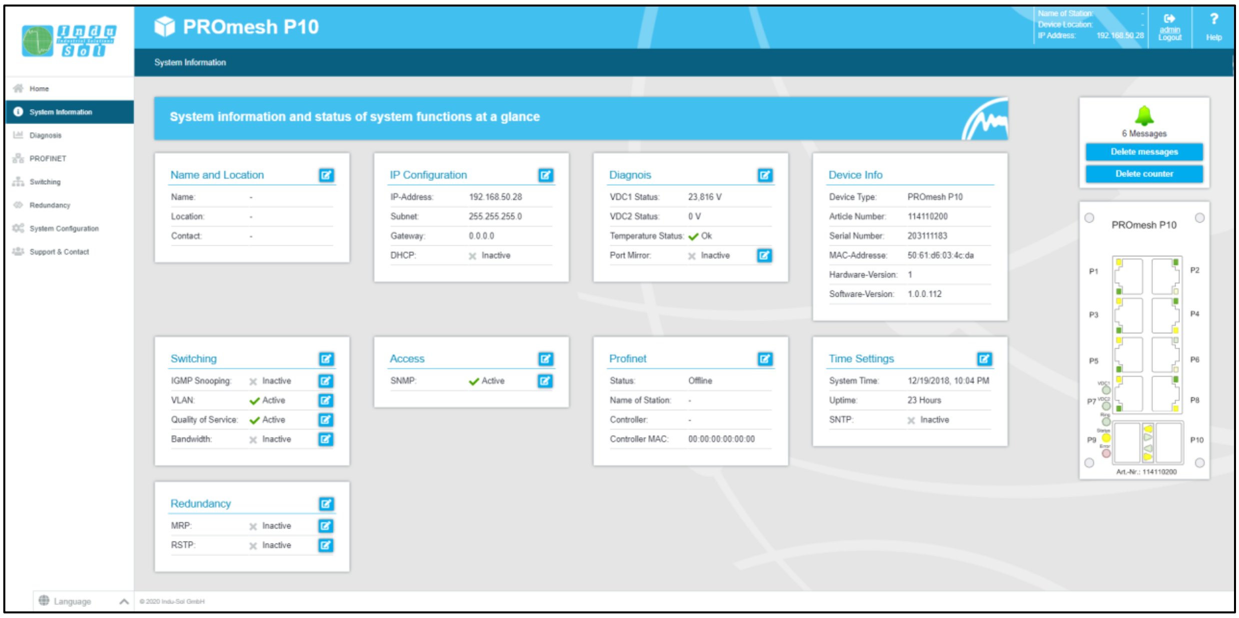
Art.-Nr.: 114110200

© 2020 Indu-Sol GmbH

Figure 8: Start

3.5 System information

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



Name of Station: -
Device Location: -
IP Address: 192.168.50.28

System information and status of system functions at a glance

6 Messages

Name and Location

Name:	-
Location:	-
Contact:	-

IP Configuration

IP-Address:	192.168.50.28
Subnet:	255.255.255.0
Gateway:	0.0.0.0
DHCP:	✗ Inactive

Diagnois

VDC1 Status:	23,816 V
VDC2 Status:	0 V
Temperature Status:	✓ Ok
Port Mirror:	✗ Inactive

Device Info

Device Type:	PROmesh P10
Article Number:	114110200
Serial Number:	203111183
MAC-Addresse:	50:61:d6:03:4c:da
Hardware-Version:	1
Software-Version:	1.0.0.112

Switching

IGMP Snooping:	✗ Inactive
VLAN:	✓ Active
Quality of Service:	✓ Active
Bandwidth:	✗ Inactive

Access

SNMP:	✓ Active

Profinet

Status:	Offline
Name of Station:	-
Controller:	-
Controller MAC:	00:00:00:00:00:00

Time Settings

System Time:	12/19/2018, 10:04 PM
Uptime:	23 Hours
SNTP:	✗ Inactive

Redundancy

MRP:	✗ Inactive
RSTP:	✗ Inactive

PROmesh P10

Art.-Nr.: 114110200

Figure 9: Status and diagnostics

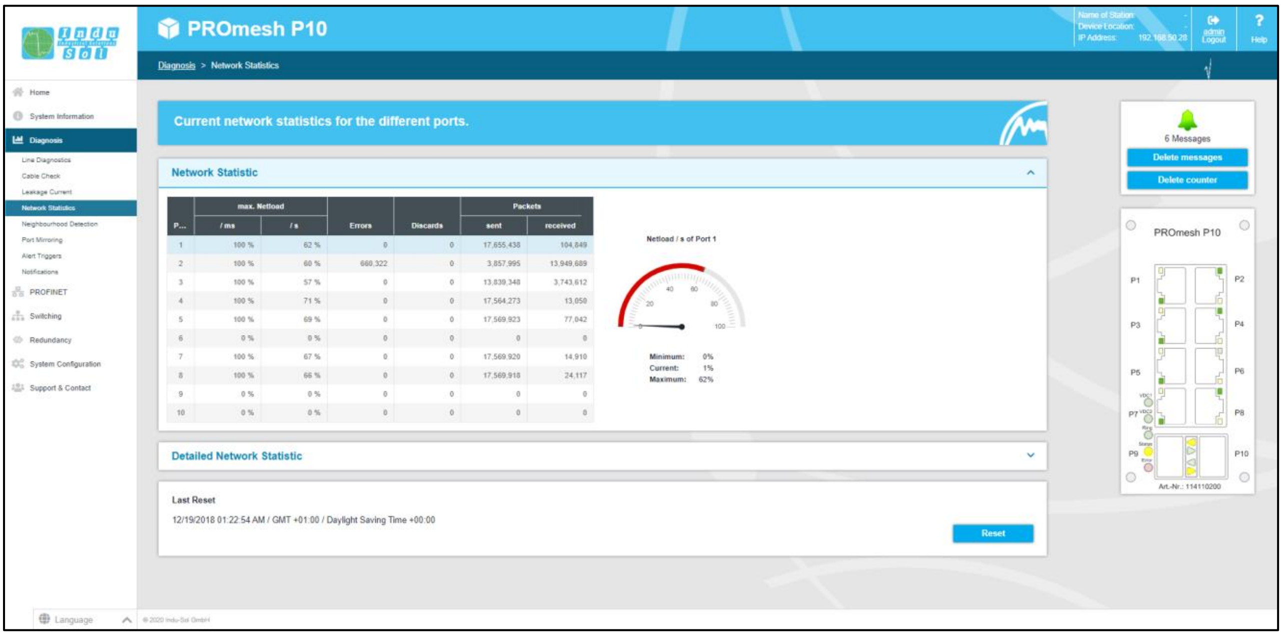
3.6 Diagnostics

The Diagnostics page provides an overview of the status of configured alarm triggers (alarm trigger configured or not) for the individual diagnostic data recorded by the PROmesh P10. Furthermore, the status for topology determination and port mirroring is displayed.

3.6.1 Port statistics

The Port Statistics page provides information on the data traffic of the individual ports. This information is useful for diagnostic purposes or when network problems occur.
In the main view of the port statistics, the following information is provided for each port:

- Received data packages
- Sent data packages
- Received Network Limit
- Sent Network Limit
- CRC error (defective telegrams)
- Discards (discarded telegrams because of too high data volumes)



Current network statistics for the different ports.

Network Statistic

P...	max. Netload		Errors	Discards	Packets	
	/ ms	/ s			sent	received
1	100 %	62 %	0	0	17,655,438	104,849
2	100 %	60 %	660,322	0	3,857,995	13,949,689
3	100 %	57 %	0	0	13,839,348	3,743,612
4	100 %	71 %	0	0	17,564,273	13,050
5	100 %	69 %	0	0	17,569,923	77,042
6	0 %	0 %	0	0	0	0
7	100 %	67 %	0	0	17,569,920	14,910
8	100 %	66 %	0	0	17,569,918	24,117
9	0 %	0 %	0	0	0	0
10	0 %	0 %	0	0	0	0

Netload / s of Port 1

Minimum: 0%
Current: 1%
Maximum: 62%

Detailed Network Statistic

Last Reset

12/19/2018 01:22:54 AM / GMT +01:00 / Daylight Saving Time +00:00

Figure 10: Port Statistics

Resetting the values

Below the table, there is a status bar. Here the counters of all ports can be reset. This restarts the evaluation.

In the graphical display for the port load, the current incoming or outgoing Network Limit, as well as the minimum, average and maximum values for the selected port are displayed.

Detailed port statistics

In the statistical details, the size of the individual packages is recorded statistically up to various limit values. (Up to 64, 127, 255, 511, 1023, or 1518 Byte.)

Amongst the sent packages, a difference is made between:

- Number of Unicast packages (packages to one receiver)
- Number of non-unicast packages

Amongst the received packages, a differentiation is made between:

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

The *Packages up to bytes* line provides information about the number of packages in various sizes. Here the number of received packages is recorded, for the package sizes up to 63, 127, 255, 511, 1023, or 1518 byte.

Package collisions are also recorded and divided according to:

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

Such collisions and associated data losses always occur when several devices want to transmit simultaneously on one medium.

3.6.2 Cable diagnostics

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

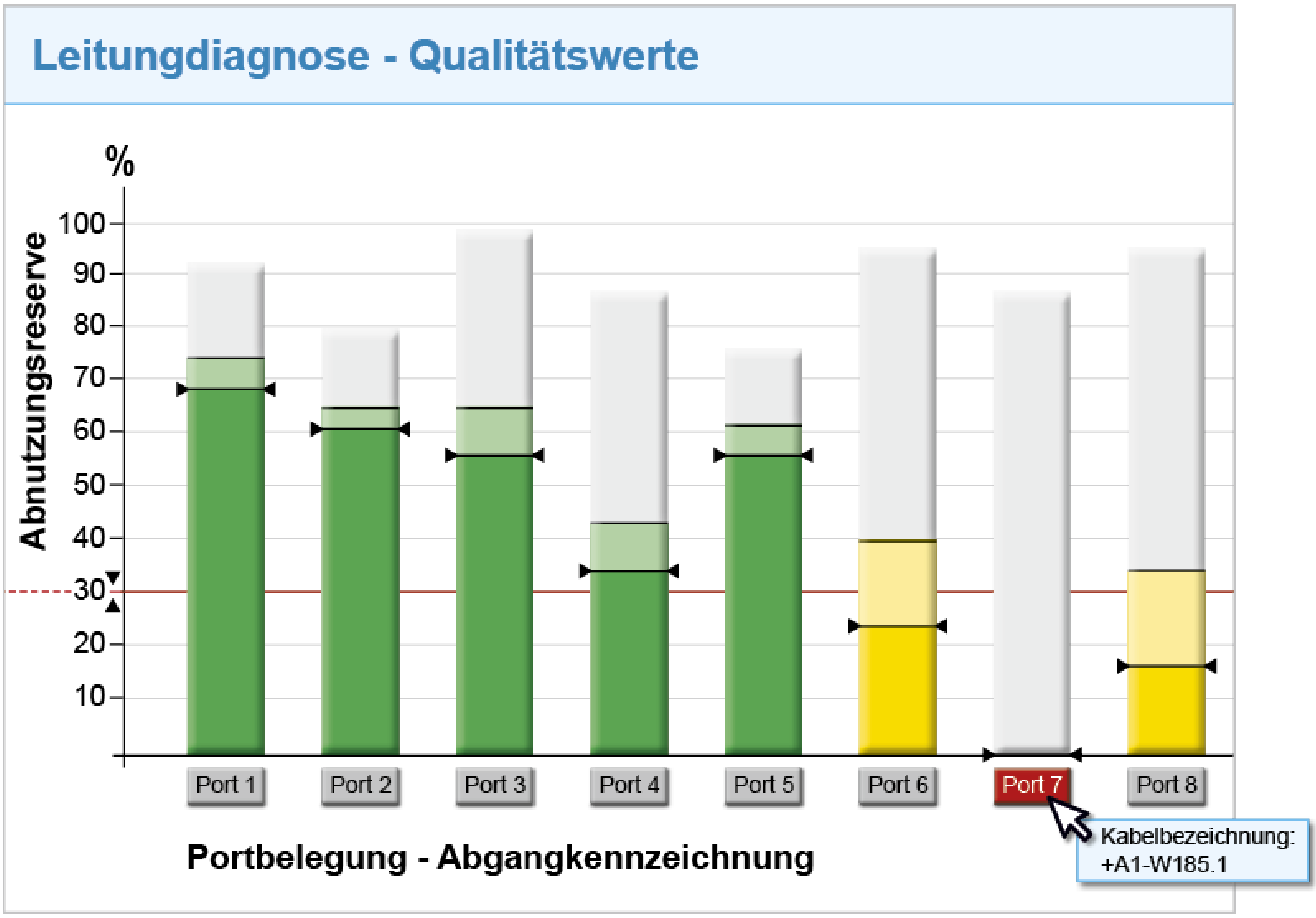


Figure 11: Quality value

Bar diagram with information

3 values are shown per bar.

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

- Green: The cable quality is OK. No measures are required.
- Yellow. The defined threshold value of 30% has been fallen below. The cable quality is insufficient. The connection should be checked in the next maintenance interval.
- Red: No data exchange can occur any longer. Change to the cable test menu to start an error analysis.

A cable designation can be stored for each port in the Port Configuration menu. This can be displayed by moving the mouse pointer over the port.

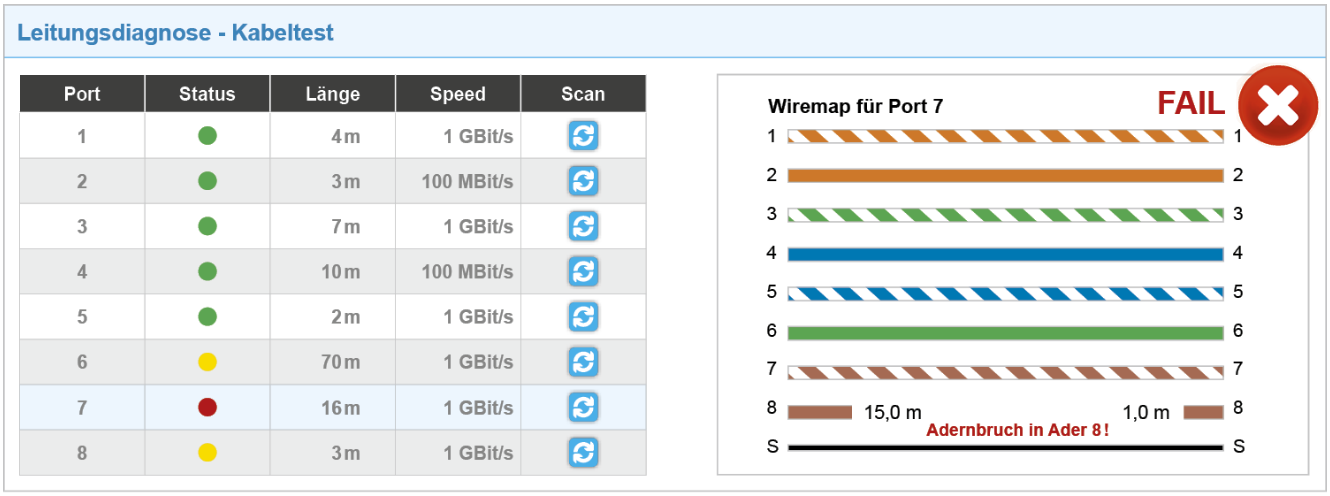
Other

The threshold value, which colours the bar yellow and recommends that the connection should be checked, can be adjusted by the user. We do not recommend setting the threshold value under 30%. In the Alarms menu, alarms can be defined for the cable quality value, which send messages via relay, SNMP, PROFINET or e-mail when the cable quality falls below a threshold value.

3.6.3 Cable test

The cable test makes it possible to check the wiremap of the cables connected to the ports. This shows if there are broken cores or short circuits between cores. In addition to the condition of the cores, the length of the cable is determined.

The cable test is performed every time the port status changes. Furthermore a cable test can be initiated manually. This is only possible if the cable is connected to the PROmesh P10 and the other end of the cable is not installed at any remote station. (open end)



Leitungsdiagnose - Kabeltest

Port	Status	Länge	Speed	Scan
1	🟢	4 m	1 GBit/s	↻
2	🟢	3 m	100 MBit/s	↻
3	🟢	7 m	1 GBit/s	↻
4	🟢	10 m	100 MBit/s	↻
5	🟢	2 m	1 GBit/s	↻
6	🟡	70 m	1 GBit/s	↻
7	🔴	16 m	1 GBit/s	↻
8	🟡	3 m	1 GBit/s	↻

Wiremap für Port 7

FAIL

15,0 m

1,0 m

Adernbruch in Ader 8 !

Figure 12: Cable test

Information table

- Port: The cable test is available for ports 1-8. By selecting a port, the wiremap of the connected connection is displayed.

- Status: The status is derived from the determined quality values of the cable diagnostics.
  - Green: The cable quality is OK. No measures are required.
  - Yellow. The cable quality is insufficient. The connection should be checked in the next maintenance interval.
  - Red: No data exchange can occur any longer. Select the port in question to view the current wiremap and thus obtain initial information on the cause of the error.
- Length: Displays the determined length of the cable.
- Speed: Displays the used transmission speed of the port. The transmission speeds can be 10 mbps, 100 mbps or 1 Gbps.
- Scan: Enables the manual determination of the wiremap.

Displayable errors with wiremap

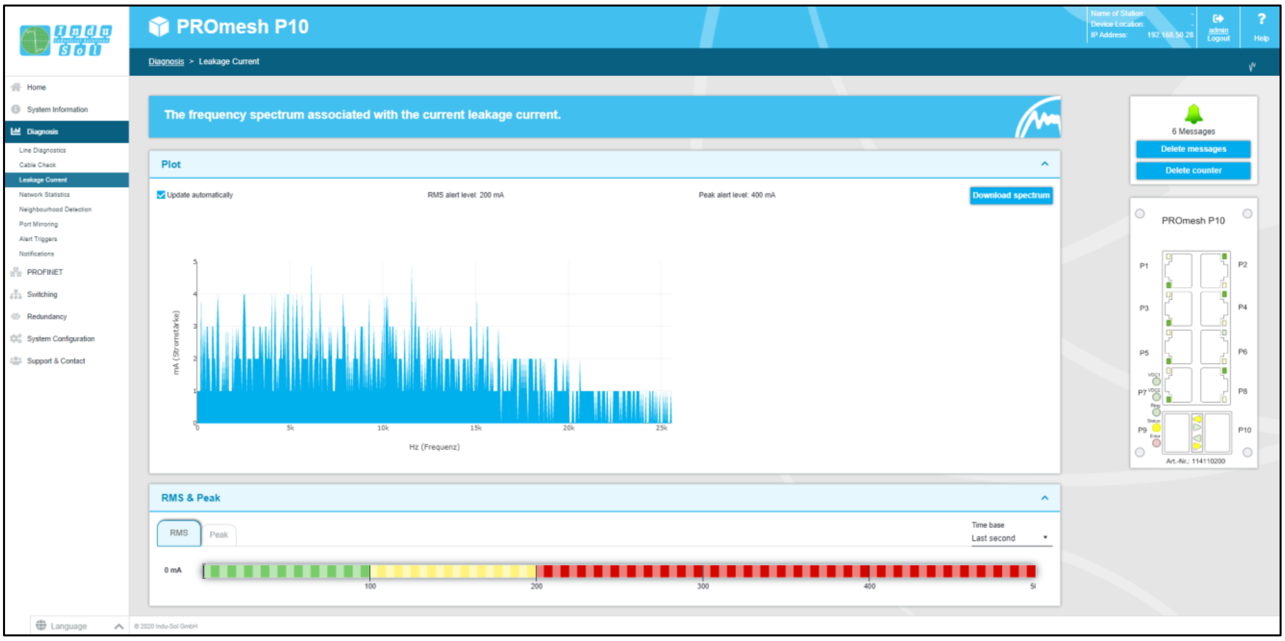
- Wire breaks
- Short circuit to another wire

3.6.4 Leakage current

The leakage current monitoring (Figure 13) makes it possible to permanently record and evaluate the sum of all shield currents of the PROFINET lines that are dissipated via the device into the equipotential bonding system. The corresponding spectrum with the respective frequency components is specified for this in addition to the current value. Using this function, the PROmesh series also offers mechanisms for detecting EMC interference or couplings.

Other functions:

- Downloading the frequency spectrum after a threshold value was exceeded
- Switching the axes between a decimal and a logarithmic scaling



The frequency spectrum associated with the current leakage current.

☑ Update automatically

RMS alert level: 200 mA

Peak alert level: 400 mA

Time base: Last second

Figure 13: Leakage Current

3.6.5 Topology

The Link Layer Discovery Protocol (LLDP) is a manufacturer-independent Layer-2 protocol which provides the possibility to exchange information (addresses, names and descriptions) between neighbouring devices. An LLDP agent is running on every device that supports LLDP. This sends information about the individual status in periodic intervals and receives information from the neighbouring devices.

Since this takes place independently from one another, the LLDP is also termed a one-way protocol.

The following information is compiled and sent by the LLDP:

- System name and description
- Port name and description
- VLAN name

- IP address

LLDP interval

The LLDP interval parameter can be used to specify in what intervals (in seconds) the device's own LLDP telegram is sent to the neighbouring devices. Standard setting is 5 seconds.

Forwarding Database

The Forwarding Database gives information on which MAC address is connected to which port of the switch.

3.6.6 Port mirroring

Port mirroring is a method in networks to route the traffic of one port (source) simultaneously to a second port (destination) and to check that in this way. This means that the received and sent packages of the source port to the port to be monitored are duplicated.

The monitoring of the source ports takes place without influencing the data traffic of the port. The mirror port thus created can be connected to a LAN analyser or be used for diagnosis and debugging purposes.

- Port and Port name: All ports are displayed here so that one destination and one or more source ports can be selected.
- Destination: If port mirroring is activated, select one port on which the data should be mirrored. The mirrored packages can be forwarded to precisely one destination.
- Source Port: Select here which ports should be monitored and forward their packages to the destination port. The option is available to forward only transmitted packages (TX for transmit) to the destination or to monitor both directions, that is transmitted (TX for transmit) and received (RX for receive) packages. You can select up to eight source ports in the switch. Mark the respective checkbox to select a port.

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

3.6.7 Alarms / Notifications

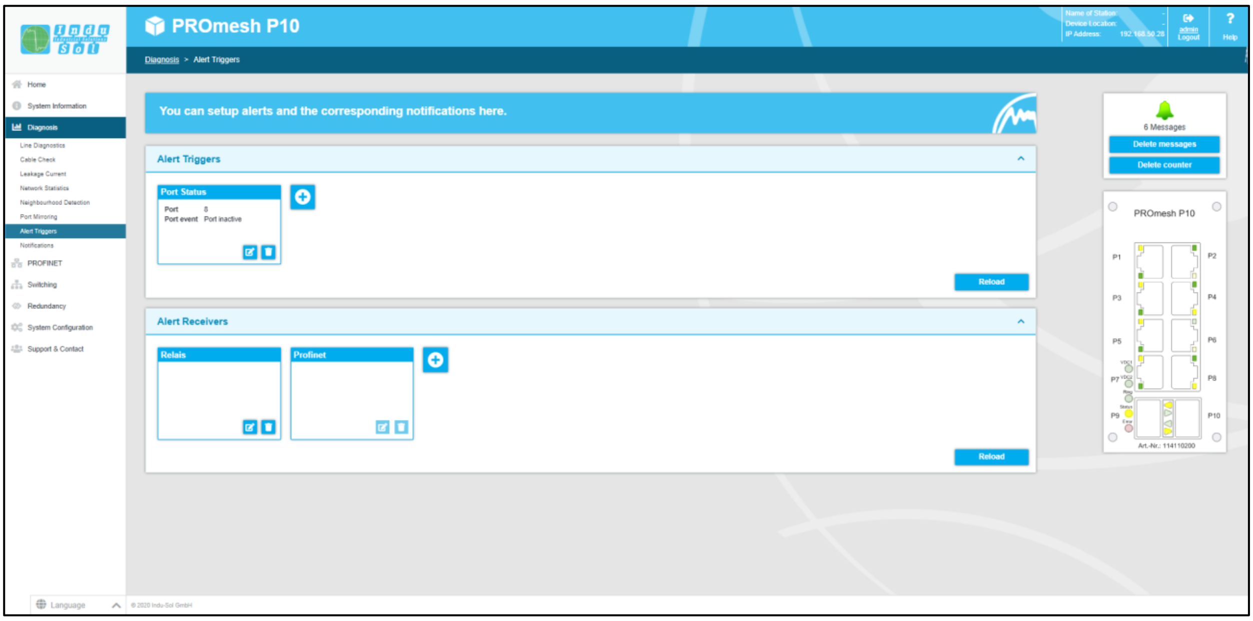
The Alarms / Notifications menu item is used for the configuration of alarm triggers and alarm receivers. Alarms can be specified for the following events:

- Status change of a port
- Too high or too low temperature
- Failure of a supply voltage
- MRP protocol event
- Exceeding a leakage current
- Exceeding the network utilisation at a port
- Incorrectly connected neighbour
- Exceeding the cable quality value
- Too high or too low voltage value of the 24 V voltage supply

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

- Fault relay
- SNMP traps
- E-mail addresses
- PROFINET

If one of the specified alarms is detected and triggered, then the software forwards the event to the corresponding alarm receiver and documents this event additionally as a syslog message.



PROmesh P10

Name of Station: -
Device Location: -
IP Address: 192.168.50.28

Diagnosis > Alert Triggers

You can setup alerts and the corresponding notifications here.

Alert Triggers

Port Status
Port 8
Port event Port inactive

Alert Receivers

Relais

Profinet

6 Messages

Art.-Nr.: 114110200

© 2020 Indu-Sol GmbH

Figure 14: Alarm trigger

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

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

Adding and editing alarm triggers

Click the button with the "+" symbol to add new alarms and messages. If alarms are already available, then the user has the option to edit or delete them by the click of a button. The user can select the different alarms in the top part of the "alarm trigger" pop-up. During the creation and editing of the alarms, the corresponding receivers can be selected in the lower part of the pop-up, and thus linked to the alarm trigger once the alarm receiver has already been defined.

Adding and editing alarm receivers

Click the button with the "+" symbol to add new alarm receivers. The relay already exists as alarm receiver and cannot be deleted but only linked to alarm triggers. Besides this, the receiver e-mail, SNMP and PROFINET can be selected. The corresponding alarm triggers can be linked in the lower part of the pop-up to the current receiver.

- In the Simple Network Management Protocol (SNMP), error messages are generated by the device and sent to a management station without request. Since the packages are not confirmed, the device 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 server (Simple Mail Transfer Protocol). In case of an alarm, the device sends an e-mail to the user. Optionally, the authentication can be activated. For this, the necessary access data must be entered.
- The alarm receiver “Profinet” is permanently system-internally set in a Profinet network after integration and parametrising of the switch and cannot be changed in the device. The alarm triggers of the individual events are activated in the hardware configuration of the controller. If a trigger is triggered, there is an alarm message of the switch at the controller. This information can then be processed further by programs in the PLC.

3.6.8 Messages

The messages help the user to receive status and error messages of the various functions. The messages are displayed in the overview with date and time as well as a code, a description and a reference. Since the log entries are not stored in the device, they are no longer available after a device restart or voltage interruption. To archive the messages permanently, an option is provided to use an external syslog server or the SD card.

Statistics

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

Securing the messages

- Syslog server: To save the messages on a syslog server, activate this function. Enter the IP address of the syslog server with decimal points, select "File" under media type and save the settings with the Apply button. Please check if the server can be reached and saves the messages in a file.
- Syslog on SD card: To save the messages on the SD card, make sure that an SD card has been inserted and activate this function. Then select "SD Card" under media type and save the settings using the Apply button. Please check whether there is enough free memory available on the SD card and whether the messages are saved in a file.

Resetting the entries

- The reset button removes all entries from the table. The time of deleting the entries is then possible at 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 stands for the open Industrial Ethernet Standard for automation.

The device has been developed as a Profinet IO device for connecting distributed periphery to a Profinet controller. The device supports Conformance Class B. You can configure the port settings for DCP on this page and download the configuration file.

DCP settings:

- For every port, you can specify whether it supports the Discovery and Configuration Protocol (DCP). By means of the DCP, the addresses and names are distributed in a Profinet IO system to the individual devices.

Additional information

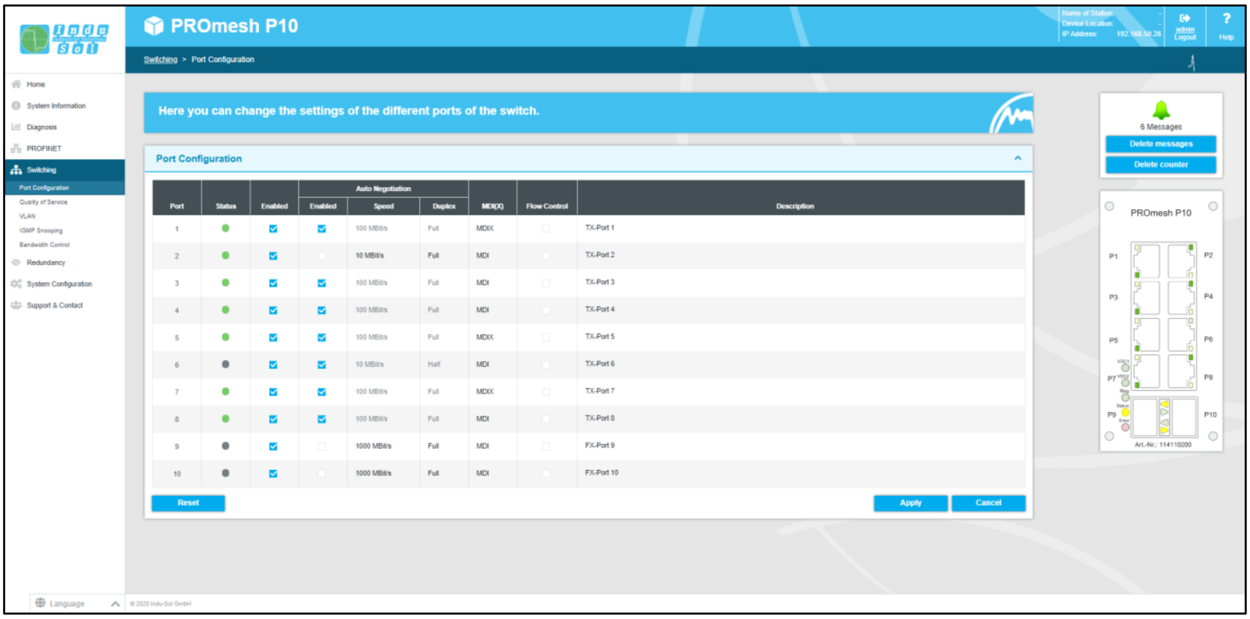
The configuration file saved on this page describes the Profinet field devices. The file is written in General Station Description Markup Language (GSDML). The file serves as a basis for planning the configuration of a Profinet IO system.
Furthermore, the current status of the device is shown in PROFINET and in its controller (if present).

3.8 Switching

This page provides an overview of the activated and deactivated functions in the switching area. You can see at a glance which functions are currently activated. By clicking the Edit button, you switch directly to the various pages and can make further settings there.

3.8.1 Port configuration

The table enables an overview of the current configuration of the individual ports. The columns Enabled, Auto Negotiation, Flow Control and Description, can also be edited. The page is regularly updated and reloaded.



Here you can change the settings of the different ports of the switch.

Port Configuration

Port	Status	Enabled	Auto Negotiation			MDI(X)	Flow Control	Description
			Enabled	Speed	Duplex			
1	●	☑	☑	100 MBit/s	Full	MDIX	□	TX-Port 1
2	●	☑	□	10 MBit/s	Full	MDI	□	TX-Port 2
3	●	☑	☑	100 MBit/s	Full	MDI	□	TX-Port 3
4	●	☑	☑	100 MBit/s	Full	MDI	□	TX-Port 4
5	●	☑	☑	100 MBit/s	Full	MDIX	□	TX-Port 5
6	●	☑	☑	10 MBit/s	Half	MDI	□	TX-Port 6
7	●	☑	☑	100 MBit/s	Full	MDIX	□	TX-Port 7
8	●	☑	☑	100 MBit/s	Full	MDI	□	TX-Port 8
9	●	☑	□	1000 MBit/s	Full	MDI	□	FX-Port 9
10	●	☑	□	1000 MBit/s	Full	MDI	□	FX-Port 10

Figure 15: Port configuration

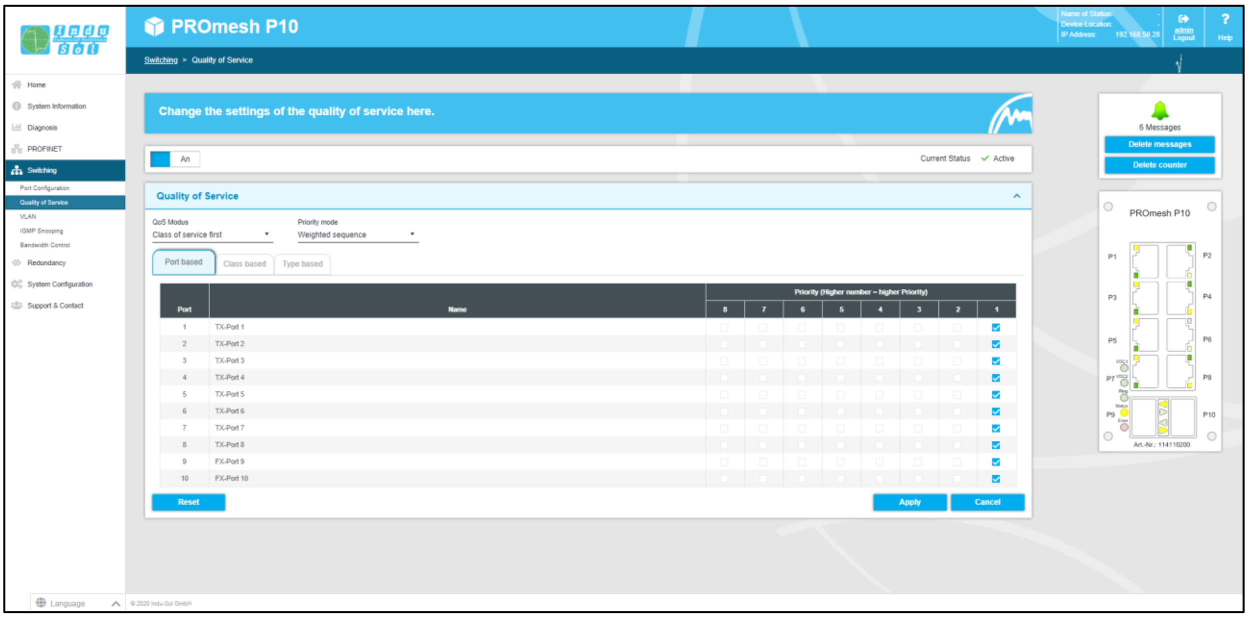
The individual columns:

- Port: Displays the port number that is also marked on the housing.
- Enabled: The individual ports can be activated or deactivated. With that, you specify whether or not a port can be used.
- Status: Status signals the current status of the port:
    - Green: The port is activated and a connection has been established.
    - Grey: The port is inactive or deactivated.
- Auto Negotiation: If this function is activated, an automatic configuration of transfer rate and duplex mode is done. The device and the connected receiver coordinate the settings automatically with each other. If auto negotiation is deactivated, you can make the settings permanently by hand:
    - Speed: The baud rate of the ports can be permanently specified. The option is provided to set a baud rate of 10 mbps or 100 mbps.
    - Duplex: The duplex mode can be switched between semi- and full-duplex. This setting is thus permanently specified for one connection.
- MDI(X): The device can execute autocrossover detection by default. This means that the switch can independently detect whether the device is connected by a crossed or a non-crossed cable.
- Flow control: The flow control makes sure that the received data packages are ignored if a port is overloaded, and the connected device gets a signal that it will stop sending.
- Description: You can name the ports individually in this column. The names are displayed during the entire configuration and make the section of the correct settings easier as well as the diagnostics in case of malfunction. Click directly on the port description and edit the name in the row.

3.8.2 Quality of Service

All processes are combined under Quality of Service (QoS) that influence the data flow in the device. Certain payload data can be treated with priority by being assigned to various priority queues. For example, real-time data, control data, audio or video data can have priority over file transfers.

The switch supports four different queues that are processed with various priorities. The option exists to apply only one of the classification methods below or to combine several ones.



Change the settings of the quality of service here.

An

Current Status ✓ Active

Quality of Service

QoS Modus: Class of service first

Priority mode: Weighted sequence

Port based | Class based | Type based

Port	Name	Priority (Higher number – higher Priority)							
		8	7	6	5	4	3	2	1
1	TX-Port 1	□	□	□	□	□	□	□	☑
2	TX-Port 2	□	□	□	□	□	□	□	☑
3	TX-Port 3	□	□	□	□	□	□	□	☑
4	TX-Port 4	□	□	□	□	□	□	□	☑
5	TX-Port 5	□	□	□	□	□	□	□	☑
6	TX-Port 6	□	□	□	□	□	□	□	☑
7	TX-Port 7	□	□	□	□	□	□	□	☑
8	TX-Port 8	□	□	□	□	□	□	□	☑
9	FX-Port 9	□	□	□	□	□	□	□	☑
10	FX-Port 10	□	□	□	□	□	□	□	☑

Reset | Apply | Cancel

Figure 16: Quality of Service

QoS mode and priority scheme

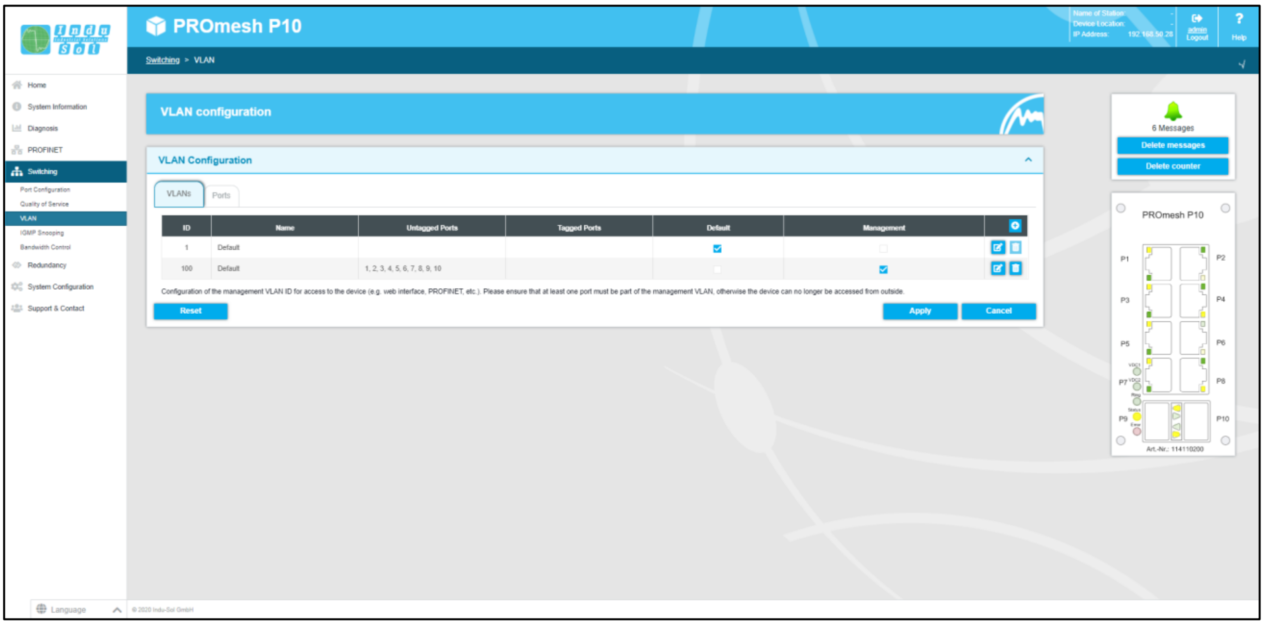
With QoS mode, a differentiation is made between the following settings:

- Port based: You can set a data transfer priority for each port and the switch will forward the data packages of the respective port according to your priority.
- Class of Service (COS): The COS uses a data field with priority information existing in the VLAN Tag. Eight different priority values are specified here, from Best Effort (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 of Service (TOS): TOS uses a data field Differentiated Services Code Point (DSCP) in the IP header of the packages, which can have up to 64 different priorities. As with COS, these priorities can be used to prioritise real-time control data, Voice over IP (VoIP) or audio data over normal data transmission. Adapt the settings according to your requirements.
- QoS mode:
  - Only port-based: The prioritisation is done exclusively based on the priority of the ports.
  - Only Class of Service: A prioritisation is done exclusively based on the Class of Service data field of the packages.
  - Only Type of Service: A prioritisation is done exclusively based on the Type of Service data field of the packages.
  - Class of Service first: In this variant, the prioritisation is first decided based on COS, then (if necessary) according to TOS and finally according to port.
  - Type of Service first: Here, the prioritisation is decided based on TOS, then (if necessary) based on COS and finally based on the port.

- Priority scheme:
  - Strict priority scheme: In the strict priority scheme, all packages leave a port until the corresponding priority queue is empty. Only then are packages sent from the queues with lesser priority. If packages are permanently arriving in the queue with the highest priority, it may be that packages of the lowest queue are never sent. This mode is recommended if there are really strong real-time requirements.
  - Weighted sequence: This approach prevents that low-priority packages are never sent if high-priority packages are to be permanently sent. This leads to only minor increased latency for the high-priority packages. The switch primarily sends high-priority packages but also processes all low-priority queues in one send cycle.

3.8.3 VLAN

A virtual LAN (VLAN) is a logical group of network devices. A VLAN permits the isolation of a part of the network. All data traffic of network devices of a VLAN group is transferred only within the VLAN group.



ID	Name	Untagged Ports	Tagged Ports	Default	Management
1	Default			☑	□
100	Default	1, 2, 3, 4, 5, 6, 7, 8, 9, 10		□	☑

Configuration of the management VLAN ID for access to the device (e.g. web interface, PROFINET, etc.). Please ensure that at least one port must be part of the management VLAN, otherwise the device can no longer be accessed from outside.

Figure 17: VLAN

You can make settings for a VLAN based on 802.1Q (Tagged VLAN) here. For tag-based VLAN, the VLAN control information from the package header are needed. The tags include a VLAN identifier here that denotes the association of the package to the corresponding VLAN. This makes it possible to set up a VLAN spanning the network.

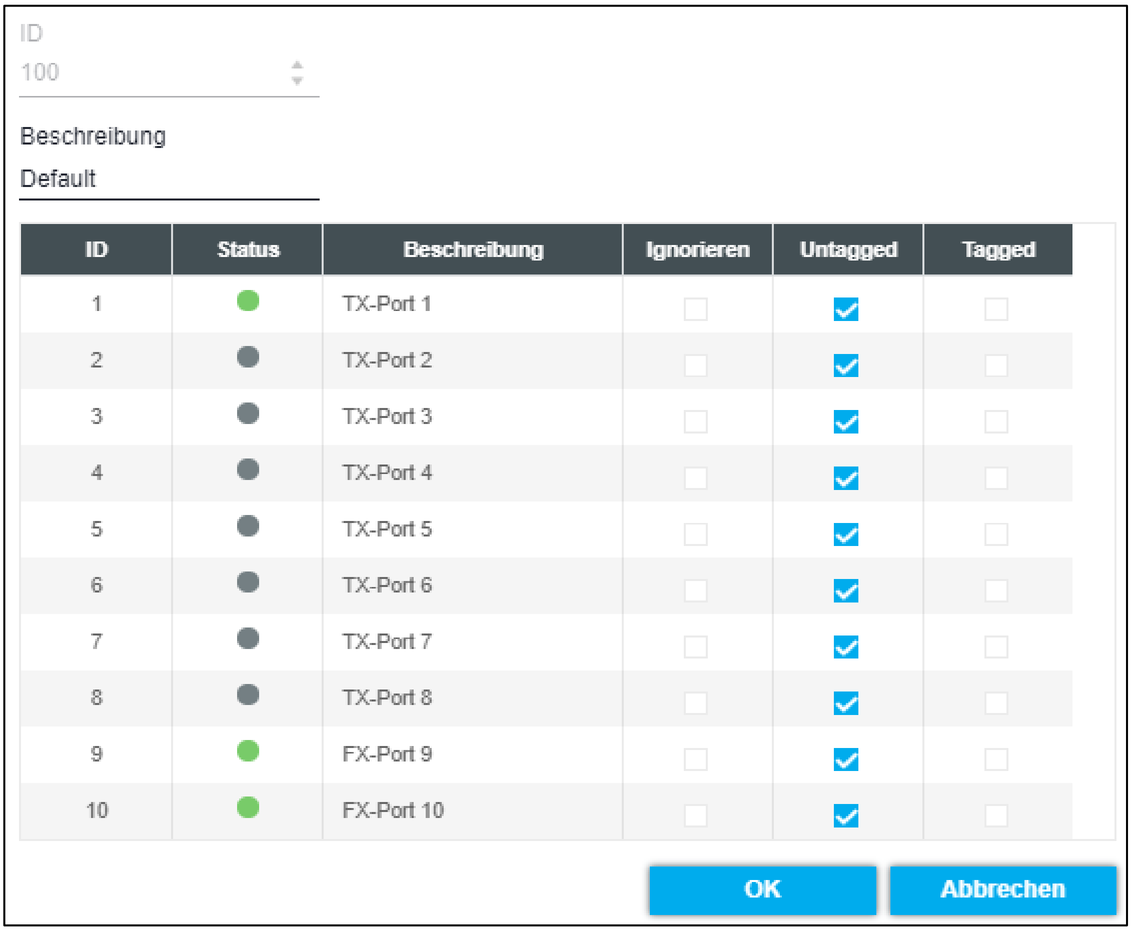
If the VLAN 802.1Q function is activated, you can add a new Tagged-VLAN using the Add button. Additionally you have the option to select an existing VLAN in the list and to edit or to delete it using a button.

You can choose between two views. The overview according to VLANs displays the IDs and names of all virtual LANs and shows the tagged and untagged ports based on the port number. You can also determine here which VLAN is treated as management and which VLAN is treated as default. The overview according to ports displays the port number and name of a port and lists all VLANs with IDs that include port tagged or untagged.

Add new VLAN

Use the "+" button to create a new VLAN and define the following settings.

- VLAN ID: This identification number is uniquely assigned to a VLAN. VLAN IDs are possible between 1 and 4094. Make sure that IDs in your network are not used by another VLAN.
- VLAN description: Enter the name here for the new VLAN. Maximum permitted length of the VLAN name is 50 characters
- Port ID: Select how a port should behave in the newly created VLAN.
- Status: Is a device connected to the respective port or not.
- Description: A more detailed explanation of the port is possible here.
- Ignore: The port ignores the ID of the current VLAN and cannot communicate with this VLAN.
- Untagged: All output data packages of this port feature a VLAN identification. Communication with this VLAN ID is possible.
- Tagged: All output data packages of this port feature a VLAN identification of the corresponding ID.
- Port Name: The port name that you issued in the Port Configuration menu is displayed here.



ID

100

Beschreibung

Default

ID	Status	Beschreibung	Ignorieren	Untagged	Tagged
1	🟢	TX-Port 1	□	☑	□
2	●	TX-Port 2	□	☑	□
3	●	TX-Port 3	□	☑	□
4	●	TX-Port 4	□	☑	□
5	●	TX-Port 5	□	☑	□
6	●	TX-Port 6	□	☑	□
7	●	TX-Port 7	□	☑	□
8	●	TX-Port 8	□	☑	□
9	🟢	FX-Port 9	□	☑	□
10	🟢	FX-Port 10	□	☑	□

Figure 18: Add new VLAN

Note: When you add ports to your VLAN, the untagged output data traffic of these ports are tagged with the VLAN ID of your VLAN. Thus the package is uniquely associated with your VLAN.

Default and management VLAN

The default VLAN as relevance when no VLAN is activated. In this case all ports are in the default VLAN. If the VLAN function is activated, ports can also be assigned to other VLANs. There is no functional difference between the default and other VLANs except that the default VLAN cannot be deleted. It is different in the Management VLAN. The PROmesh P10 can only be reached via the Management VLAN. Therefore, it is absolutely necessary for at least one port to be saved in the Default VLAN. Otherwise, the switch can no longer be reached. During network management, make sure that the network management system can access the Management VLAN. Otherwise, no data can be retrieved from the PROmesh P10.

3.8.4 IGMP snooping

The Internet Group Management Protocol (IGMP) is a protocol of the Internet protocol family. IGMP Snooping regulates the multicast traffic between switches, routers and hosts that support IGMP. Activating IGMP snooping makes it possible to make IGMP queries to the ports and send reports. IGMP features three basic types of messages:

- IGMP Queries: Are queries from IGMP router or switch that require an answer from all hosts of a multicast group.
- IGMP Reports: Are queries from hosts to become member of a report group or messages that they already belong to the group.
- IGMP Leave Group: Is a message from a host that wants to leave a specific multicast group.

Settings per stream

- VLAN ID: IGMP snooping operates on VLAN basis and can by activated for the individual VLAN IDs.
- Snooping: Activate or deactivate IGMP-Snooping for the VLAN.
- Fast leaver: Permits the software to remove a group if a Leave Report is received without sending a Query Message. Specify whether the Fast Leaver should be activated for the VLAN.
- Known ports: Shows to which ports Multicast receivers are connected, and to which ports the Multicast streams are forwarded.
- Static ports: Specify which ports should always receive Multicast streams, independent of IGMP messages, by permanently entering the ports. Click into the column for that and select the port from the pulldown menu.
- VLAN Name: The precise name of the VLAN is displayed.

General settings

- Activate querier: In case there is no Multicast router in the VLAN and that send queries, an IGMP snooping querier needs to be configured that generates the queries. The querier function can be activated here.
- Suppress report: In case two hosts exist in the same subset that receive the Multicast data of one group, then the host that receives a report from the other one will no longer send reports.

3.8.5 Bandwidth control

The bandwidth control permits you to force bandwidth limitations at a port. You can specify various sending and receipt rates for every port for this (incoming/outgoing package) and apply them to certain package types.

The tabular overview provides the following settings:

- ID: Displays the port number that is also marked on the housing.
- Package type: Select a package type according to which you want to filter.
    - All: The specified limits are observed for all packages transported via the port.
    - Broadcasts: The set limits are valid for all broadcast packages (at all devices in the network).
    - Broadcast & multicasts: The set limits are valid for all broadcast and multicast packages (at all or several devices in the network).
    - Broadcast, multicast & unknown unicasts: The limits apply for all broadcast, multicast, and unknown unicast packages (at one device).
- Limit ingress rate: Select the effective ingress rate of the port. Possible are 128 kbps, 256 kbps, 512 kbps, 1 mbps, 2 mbps, 4 mbps and 8 mbps. The standard value is defined as "No limit".
- Limit egress rate: The baud rates for outgoing packages refer to all package types. Select the effective egress rate of the port. Possible are 128 kbps, 256 kbps, 512 kbps, 1 mbps, 2 mbps, 4 mbps and 8 mbps. The standard value is defined as "No limit".

Once you have carried out the desired settings, click on "Apply" to save them.

3.9 Redundancy

This page provides an overview of the available redundancy protocols and their statuses. It is not possible that several redundancy protocols run at the same time. That is why only one can be activated. Press the Edit buttons to go to the protocols where the configuration can be carried out.

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.

Usage of the redundancy protocols guarantees your network an increased reliability and availability in case of a malfunction. The failure of a component is absorbed and devices 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 that are switched off during normal operation. The devices connected in the network operate in a line topology even though it physically is a ring topology. In case of a fault, communication is possible again across the previously deactivated path after a very brief re-establishment time.

MRP uses a redundancy manager that uses specific test packages to test the continuity of the ring and reconfigures the network in case of an error and also informs all devices about this. The guaranteed convergence time at up to 50 devices in the ring is 200 ms. In a typical application, the convergence time is normally less than 50 ms.

Ring configuration

Please note that the ring may only be physically closed when MRP has been configured completely. One device must be configured as manager per ring. The other devices must be configured as client. The following settings are necessary for MRP:

- First ring port: Please select a port that should work as primary ring port.
- Second ring port: Specify a second port that should work as secondary ring port. Please note that the secondary ring port and the primary ring port have to be different.
- This device works as: Please specify whether the device should act as manager or as client. Please keep in mind 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, in the network. It prevents network loops that can be created by redundant transmission paths and contain a mechanism for automatic convergence following a device or connection failure.

Activate the RSTP function global before configuring the corresponding parameters.

Root bridge information

The following parameters are displayed in this field:

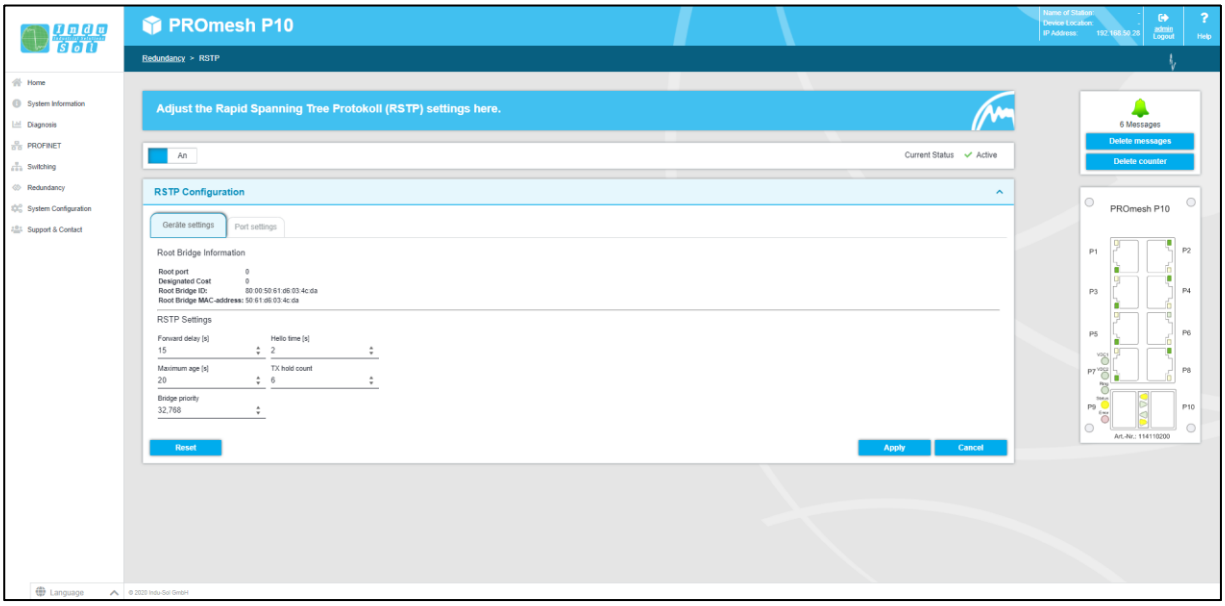
- Root Port: Displays which port is operating as root port. The shortest path to the root bridge runs through this port.

- Root Bridge ID: Identification number of the current root bridge, which was coordinated between the devices.
- Designated cost: Path costs 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 case:

- Forward delay: The time that a port waits before it switches from RSTP Learning and Listening status in den Forwarding status. Enter a value between 4 and 30 seconds.
- Maximum age: The time that a bridge waits before trying a new configuration without receiving messages from the Spanning Tree configuration protocol. Enter a value between 6 and 40 seconds.
- Bridge priority: This value is used for the negotiation of the root bridge. The bridge with the lowest value has highest priority and is selected as root bridge. The value has to lie between 0 and 61440 and be a multiple of 4096.
- Hello time: The time interval in which the switch sends BPDU packages (Bridge Protocol Data Unit) to check the current status of the RSTP. Enter a value between 1 and 10 seconds.
- TX hold count: Specifies the maximum number of transmitted hello packages within an interval. Permitted are a minimum of 1 and a maximum of 10 packages.



Adjust the Rapid Spanning Tree Protokoll (RSTP) settings here.

An

Current Status ✓ Active

RSTP Configuration

Geräte settings | Port settings

Root Bridge Information

Root port 0
Designated Cost 0
Root Bridge ID: 80:00:50:61:d6:03:4c:da
Root Bridge MAC-address: 50:61:d6:03:4c:da

RSTP Settings

Forward delay [s]: 15
Hello time [s]: 2
Maximum age [s]: 20
TX hold count: 6
Bridge priority: 32,768

Reset | Apply | Cancel

Figure 19: Device settings RSTP

Note: Observe the rule to configure Forward delay, Maximum age and Hello time:

2*(ForwardDelayTime-1) >= MaxAge >= 2*(HelloTime+1).

Recommended procedure: Select a value for the "Hello time" and calculate using formula 2 * (Hello Time + 1) according to the rule provided above to find the lower limit of the Maximum age. Select a value for the "Forward delay time" and calculate using formula 2* (Forward Delay Time - 1) of the rule provided above to receive the upper limit of the Maximum age. Then select a Maximum age between 6 and 40 seconds that lies between the previously calculated limits.

Once you have set the parameters, click on Apply to save the changes. The Root bridge information is now displayed in the upper area of the page.

Port settings

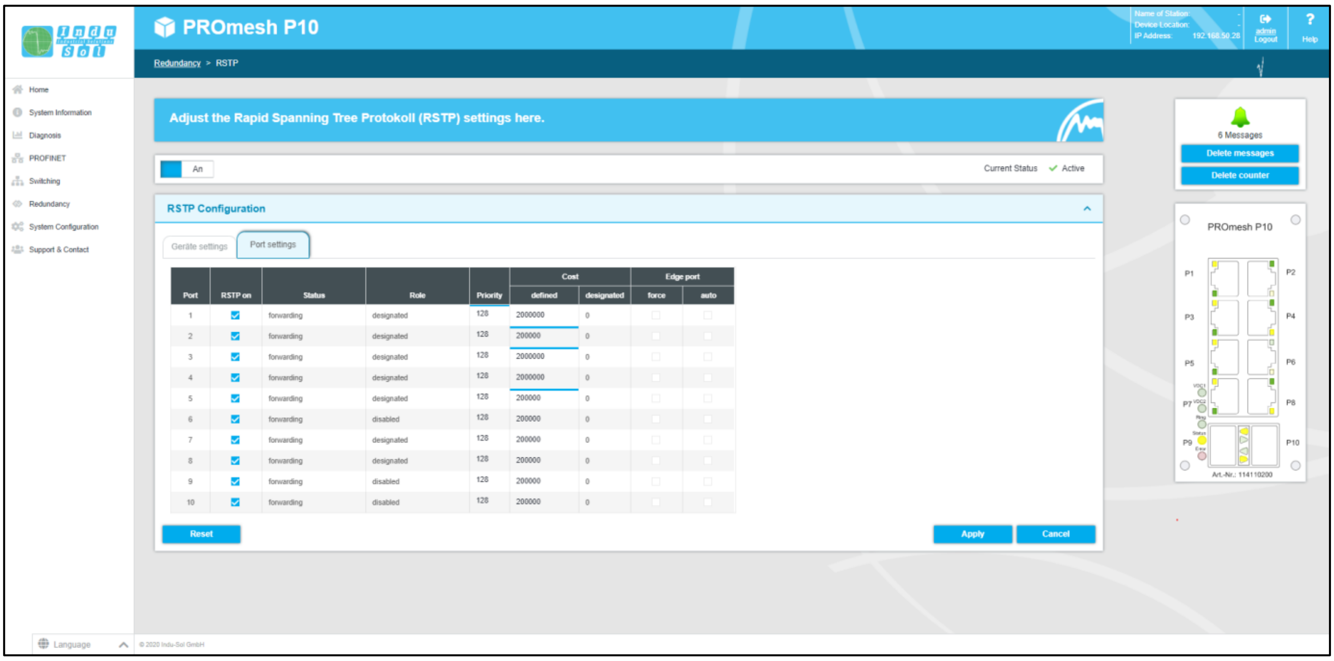
Set the following port-related settings per port:

- Port: You can configure all ports individually.
- RSTP on: Specify for every port whether or not the Rapid Spanning Tree Protocol should be activated for this port.
- Status: Displays the current status of the individual ports. A difference is made here between:
    - Blocking: rejects packages; learns no addresses; receives and processes BPDUs
    - Listening: rejects packages; learns no addresses; receives, processes and transmits BPDUs
    - Learning: rejects packages; learns addresses; receives, processes and transmits BPDUs
    - Forwarding: forwards packages; learns addresses; receives, processes and transmits BPDUs
    - Disabled: rejects packages; learns no addresses; receives and processes no BPDUs
- Role: Every port can run in one of the following modes:
    - Root port: A port in forwarding status. shortest path to the root bridge.
    - Designated port: A port in forwarding status that enables communication to other bridges in the spanning tree.
    - Alternative port: An alternative path to the root bridge, which is additional to the current root port.
    - Backup port: A backup port that is available via a designated port in the direction of the branching of the tree structure. Backup ports can exist only there where two ports are

connected as loopback via a point-to-point connection or a bridge with two or more connections to a common LAN segment.

    - Deactivated port: A port that has no operational function in the tree structure.

- Priority: You can assign higher priorities to certain port to influence the design of the tree structure. Enter a number between 0 and 240. The value has to be a multiple of 16.
- Costs: The costs of the transmit bridge at the respective port to another bridge. Enter a number between 1 and 200.000.000. With this parameter, you can influence the design of the tree structure.
    - 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: Term for a port that is connected directly with an end device and not with a further bridge (a switch). These ports cannot cause any loops and therefore switch immediately into forwarding mode. The status change of an edge port never leads to a change of the topology. Due to the permanent setting of edge ports, they accelerate convergence time of the redundancy protocol.
    - Force: The port is configured by standard as edge port.
    - Auto: The detection as edge port is done automatically.



Redundancy > RSTP

Adjust the Rapid Spanning Tree Protokoll (RSTP) settings here.

An

Current Status ✓ Active

RSTP Configuration

Geräte settings | Port settings

Port	RSTP on	Status	Role	Priority	Cost		Edge port	
					defined	designated	force	auto
1	☑	forwarding	designated	128	2000000	0	□	□
2	☑	forwarding	designated	128	200000	0	□	□
3	☑	forwarding	designated	128	2000000	0	□	□
4	☑	forwarding	designated	128	2000000	0	□	□
5	☑	forwarding	designated	128	200000	0	□	□
6	☑	forwarding	disabled	128	200000	0	□	□
7	☑	forwarding	designated	128	200000	0	□	□
8	☑	forwarding	designated	128	200000	0	□	□
9	☑	forwarding	disabled	128	200000	0	□	□
10	☑	forwarding	disabled	128	200000	0	□	□

Reset | Apply | Cancel

Figure 20: Port settings

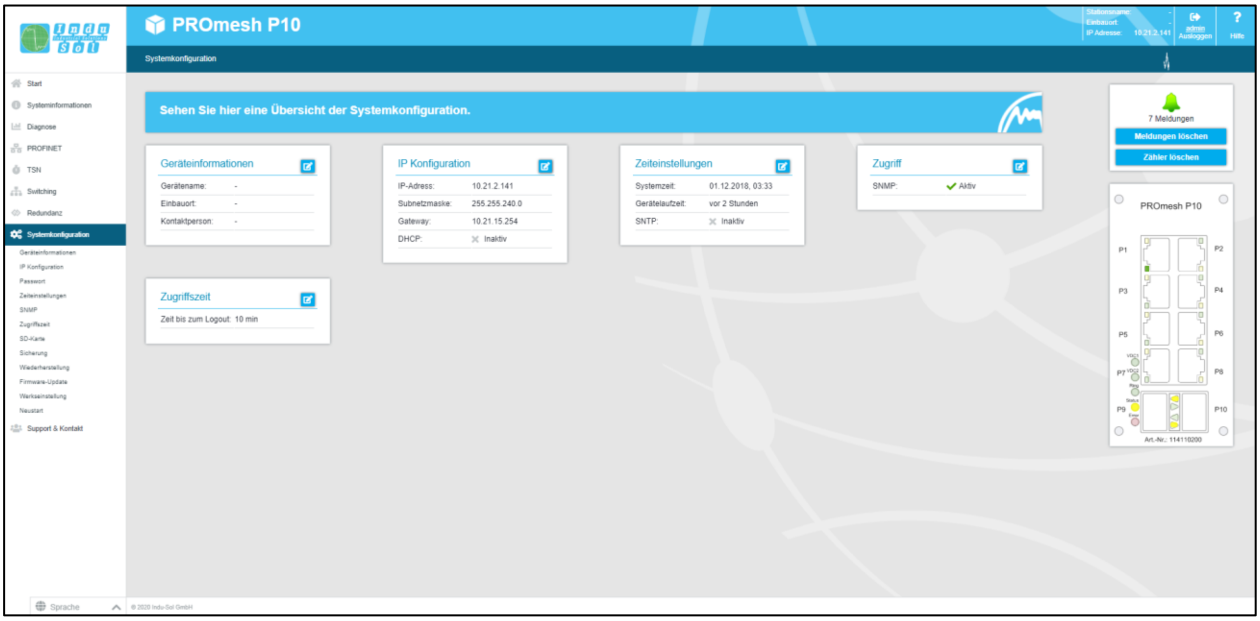
Once you have set the respective parameters, click on Apply to save the settings.

3.10 System configuration

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

The page provides you with a compact view via the System Configuration menu, so that you can understand how the device works, and identify where action is needed.

Using the edit button, you can switch directly to the corresponding protocols and functions to make further settings there.



Stationsname: -
Einbauort: -
IP Adresse: 10.21.2.141

Sehen Sie hier eine Übersicht der Systemkonfiguration.

7 Meldungen

Geräteinformationen

Gerätename:	-
Einbauort:	-
Kontaktperson:	-

IP Konfiguration

IP-Adress:	10.21.2.141
Subnetzmaske:	255.255.240.0
Gateway:	10.21.15.254
DHCP:	✗ Inaktiv

Zeiteinstellungen

Systemzeit:	01.12.2018, 03:33
Gerätelaufzeit:	vor 2 Stunden
SNTP:	✗ Inaktiv

Zugriff

SNMP:	✓ Aktiv

Zugriffszeit

Zeit bis zum Logout: 10 min

Figure 21: System configuration

3.10.1 Device information

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

- Device name: This name corresponds to the PROFINET name and is assigned via DCP.
- Location: Enter the device's location of installation to make localisation easier.
- Contact person: Enter someone as a contact partner for the device.

The input boxes are configured in such a way that you can enter up to 50 characters. Using special symbols is permitted. The device name and installation location are displayed in the information bar in the upper right. This helps give you an overview.

3.10.2 IP configuration

The IP configuration can be done either by the PROFINET controller, automatically using the Dynamic Host Configuration Protocol (DHCP) or through manual settings. Depending on the settings of the DHCP server, the IP address can change with the automatic address assignment after a device restart.

PROFINET

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

Automatic

Select the "automatic (DHCP)" check-box to receive a configuration of the IP address, the subnet mask and the standard gateway from a server operating in the network with appropriate functionality.
Once you have saved the settings by clicking on the Apply button, the device will send a query to the server and accept the configuration received from the DHCP server. Since the device has now received a new IP address, it can no longer be reached via the standard IP. Please contact your network administrator or use an appropriate tool (Indu-Sol ServiceTool) to get a new IP address.

Manual

If your network does not have a DHCP server, or if you wish to make the settings by hand, disable the "Automatic (DHCP)" button and enter the following data:

- IP address: Please note that the IP address set by you has to be reached from your PC so that you can connect with the device again so that further settings can be made.
- Subnet mask: Enter the subnet mask of the IP address; this divides the IP address into a network section and a device section. This specifies which IP address of the device can be reached directly and which addresses need to be addressed via a gateway.
- Gateway: Enter a standard gateway. The gateway is used to communicate with devices outside of your subnetwork.

Please check carefully which settings you make so that there are no problems with double IP addresses. The format of the IP address, the subnet mask and the gateway has to be entered with decimal points.

3.10.3 Password

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

Form boxes

- New Password: Please enter in this box the password specified by you for the previously selected user. Please also observe the instructions in the lower section about assigning passwords.
- Confirm Password: To make sure that you have entered your password correctly, repeat the input in this box.
- Current Password: Please enter the currently used password to ensure that you are authorized to change the password.

Notes on the passwords

The security of your system depends significantly on the security of your passwords. It is therefore generally recommended for passwords:

- Do not use any dictionary entries
- Use complex passwords
- Create combinations of letters, numerals and special characters
- Use lower- and upper-case letters
- Use a password with at least eight characters
- Do not write down passwords

3.10.4 Time setting

3.10.5 SNMP

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

Current SNMP accesses

The overview table displays the currently defined Community Strings and access permissions.

- Active: Shows which Community Strings are currently activated and which not.
- Community String: The accesses are defined by unique names that you can adjust.
- Read only: The Community String permits only reading access.
- Reading and writing: The Community String permits reading and writing accesses.

- Remove: You can mark the Community Strings to be deleted and then remove them by pressing the "Delete" button.

Creating SNMP access

Click the "Add" button in order to create a new Create String. The following parameters are required:

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

Save the settings by clicking the "Create" button.

The device supports SNMP of the versions V1 and V2C. Please select the desired version.

3.10.6 Access time

Settings

The time until automatic logout specifies how long a session in the web management system may run without activity before an automatic logout takes place. You can specify a duration between 3 and 30 minutes. Standard setting is 10 minutes.

Use the "Use" button to save the settings.

3.10.7 SD card

Configure whether you want to load the configuration directly from an inserted SD card when starting the device, or if the configuration on the external card should be ignored

If you want to rewrite the contents of the SD card, you have the possibility to format the SD card.

3.10.8 Backup

This menu item provides you with the option to backup the current device configuration in a file. The backup can be saved as a download on the SD card or by TFTP.

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

- Download: The backup file is saved in the download directory of the browser or the user can specify a path at which the file can be saved then.
- SD card: An SD card can be plugged into the SD card slot on the back of the device. The backup file is saved then by this option on this SD card.
- TFTP: The backup file is saved in a TFTP server accessible in the network. The TFTP server uses the Trivial File Transfer Protocol, a very simple file transfer system. The input of the IP address of the server and the file name is necessary for this.

Note:

When entering the file name, be sure of a unique assignment to the respective device so that the file can be assigned reliably after a longer time.

Once the parameters have been entered properly, click "Start backup" to save the backup file. Acknowledge the settings in the information window.

3.10.9 Restore

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

- Upload: The backup file is located on the currently used computer and is transferred from there to the device.
- SD card: The backup file is saved on an SD card and is uploaded from there.
- TFTP: The backup file is downloaded from a TFTP server existing in the network. It uses the Trivial File Transfer Protocol, a very simple file transfer system.

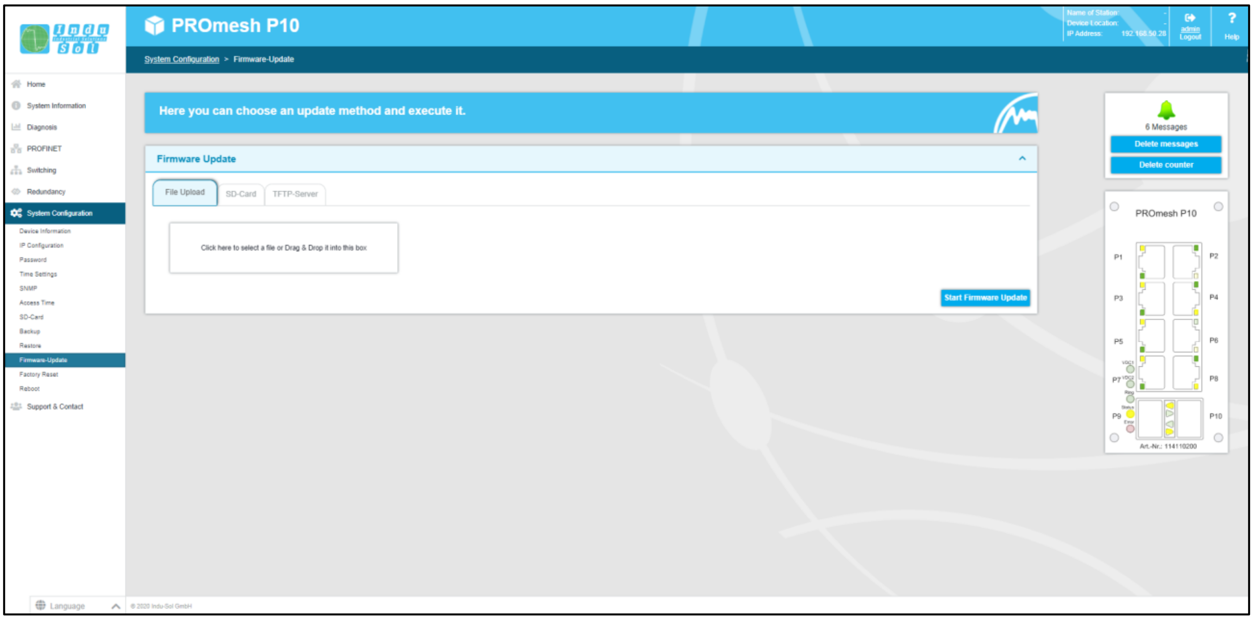
Settings

- TFTP server IP address: Enter the IP address with decimal points of the TFTP server available in the network.
- File name: The file name of the switch configuration file that should be loaded. Please enter the name relative to the root directory of the server.
- Password: Choose whether the current passwords should be maintained following a recovery or the password of the backup file should be used.
- IP Configuration: Enter whether the IP address, subnet mask and the gateway should be maintained after the recovery or the configuration of the backup file should be used.

Press the "Start recovery" button to execute the action and confirm this in the window that opens. Afterwards, the device will reboot.

3.10.10 Firmware update

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


PROmesh P10

System Configuration > Firmware-Update

Name of Station: -
Device Location: -
IP Address: 192.168.50.28

Here you can choose an update method and execute it.

Firmware Update

Click here to select a file or Drag & Drop it into this box

6 Messages

Figure 22: Firmware update

The firmware file is provided either from a TFTP server or is loaded via upload or SD card onto the device. Before updating, make sure that the correct firmware image has been selected.

- Upload: The firmware update is located on the currently used computer and is transferred from there to the device.
- SD card: The firmware update is on the SD card and is downloaded from there.
- TFTP Server: The firmware update is downloaded from a TFTP server existing in the network. It uses the Trivial File Transfer Protocol, a very simple file transfer system.

Preparation:

We do not recommend carrying out 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 carry out the firmware update.

Settings

- TFTP server IP address: Enter the IP address with decimal points of the TFTP server available in the network.
- File name: Enter the name of the new firmware file that should be installed. Please enter the name relative to the root directory of the server.

Press the "Start firmware update" button to execute the action and confirm this in the window that opens. Make sure that the firmware update can be executed completely.

Important:

Observe the following while the firmware update is running.

- Under no circumstance, disconnect the device from the voltage supply.
- Do not pull out any network connectors or replug them.

A message appears once the update has been completed. The device reboots automatically afterwards.

3.10.11 Default Settings

This menu item serves to reset the device to its default settings.

Settings

- Password: Choose whether the current passwords should be maintained following a recovery or be reset to the standard values.
- IP Configuration: Enter whether the IP address, subnet mask and the gateway should be maintained after the recovery or reset to the standard settings. In the standard setting, the device does not have an IP address. This needs to be set afterwards, for example using the Indu-Sol ServiceTool.

Click the "Set default settings" button to execute the action and confirm this in the window that opens. Afterwards, the device needs to be rebooted.

3.10.12 Restart

A restart of the switch can be performed here to carry out a software reset. By pressing the Restart button, the software of the switch is ended and the device reboots.

As an alternative, you can switch the two supply voltages of the switch off and back on and carry out a hardware reset this way.

3.11 Support

In the Support area you will find all the relevant files for the installed firmware version of the PROmesh P10:

- Manual
- MIB
- GSDML file

If these documents are not sufficient for your needs, or if you are still unclear about the product, then you will find the Indu-Sol contact information here.

Manufacturer

Please contact Indu-Sol as manufacturer of the device if you have serious problems with the configuration of the switch or questions arise that are not answered in the data sheet or in the operating instructions.

Manual

Click on this link to download or view the operating instructions of the device in Portable Document Format (*.pdf). A PDF Viewer is needed to display the file which can be downloaded for free in the Internet. Use, for example, the Acrobat Reader from Adobe.

SNMP - Management Information Base

To configure the device via SNMP, the parameters of the switch need to be defined. The description of the parameters is done in a file termed Management Information Base.

Profinet GSDML file

The GSDML file serves to describe the functionality of the switch for integration into a Profinet environment. The GSDML file (Generic Station Description Markup Language) is language-independent XML file.

License information

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

4 Notes on troubleshooting

- Check for proper voltage supply. At least one of the VDC LEDs needs to light up green.
- Check the Link/Act-LEDs of the RJ45 sockets with cables. If the connection is established, the Link LEDs have to be lit or flash when data is transmitted.
- If in doubt, disconnect redundant network structures and reset the ***PROmesh P10*** switch to default settings. If the communication functions again afterwards, carry out your setting again step-by-step and observe at what point the fault occurs.

5 Technical specifications

Network ports	8 x up to 1Gbps RJ45 2x up to 2.5 Gbps SFP
Power supply	12V .. 36V DC redundant voltage supply
Power consumption	Maximum 8 W
Dimensions (H x W x D)	105 mm x 49 mm x 112 mm
Weight	0.85 kg
Housing	Aluminium, anodised
Storage temperature	-40°C .. 85°C
Operating temperature	-40°C .. 60°C
Humidity	Humidity 5 % ... 95 %, RHD non-condensing
Protection class	IP20
Assembly	35 mm DIN top-hat rail
EMC	2014/30/EU EN 61000-6-2 / EN 55032
LED indicator	Status LEDs / Port LEDs / voltage supply
Management	SNMP management Web interface management
Switching technology	Cut-through
MAC Address table	16K 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	Only RX packages or TX and RX packages
Firmware update	SD card, TFTP server, from local PC
Bandwidth Control	Incoming and outgoing
DHCP Client	DHCP Client function to receive 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