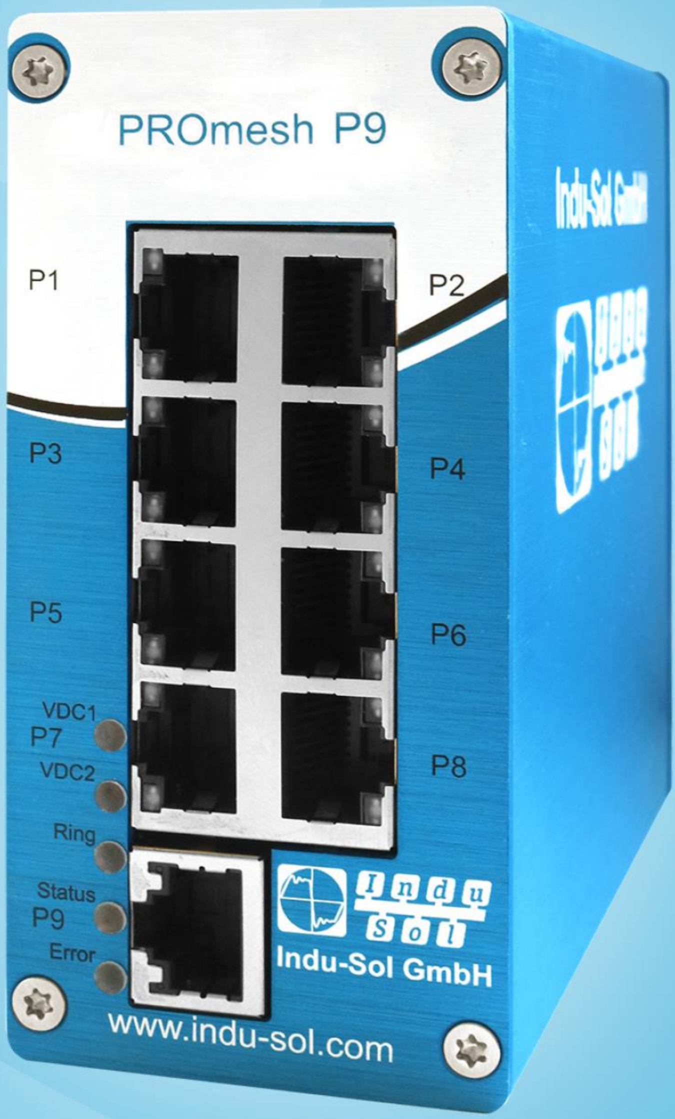
Indu-Sol GmbH – Specialist in Industrial Networks

PROmesh P9

User Manual



Diagnostic and service tools for PROFINET / Ethernet

Revision overview

Date	Revision	Change(s)
15.11.2017	0	First version
27.12.2018	1	Release version
26.08.2019	2	New function: time base and netload per second (5.3 Web interface), Management VLAN (5.10.2 VLAN 802.1Q)

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.

Caution!

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.

Contents

Revision overview 3

Contents 4

1 General information 6

1.1 Overview of the *PROmesh P9* - Functionality 6

1.2 Scope of supply 7

1.3 Safety information 7

2 Device ports and status indicators 8

2.1 Device ports 8

3 Installation 9

3.1 Installation instructions 9

3.2 Connection voltage supply and fault relay 10

3.3 LED indicators 11

3.4 Ports 12

3.4.1 RJ-45 ports 12

3.4.2 Cabling 12

4 Network topologies / Redundancy 13

4.1 Star structure 13

4.2 Ring structure 14

5 Web application 15

5.1 Preparations 15

5.2 System login 16

5.3 Web interface 16

5.4 Start page with main overview 17

5.5 System information 18

5.5.1 Status and diagnosis 18

5.5.2 Alarms / Notifications 19

5.5.3 Port statistics 22

5.5.4 Syslog messages 23

5.5.5 Leakage current 25

5.5.6 Link Layer Discovery Protocol (LLDP) – Topology 25

5.6 Basic settings 27

5.6.1 IP configuration 27

5.6.2 Password 29

5.6.3 Time setting 30

5.7 Port configuration 32

5.7.1 Port mirroring 33
5.8 Redundancy 34
5.8.1 Media Redundancy Protocol (MRP) 35
5.8.2 Rapid Spanning Tree Protocol (RSTP) 36
5.8.2.1 Device settings 36
5.8.2.2 Port settings 38
5.9 Profinet 40
5.10 Switching 41
5.10.1 IGMP snooping 41
5.10.2 VLAN 802.1Q 42
5.10.3 Quality of Service (QoS) 44
5.10.4 Bandwidth control 46
5.11 Access 47
5.11.1 Simple Network Management Protocol (SNMP) 47
5.12 Maintenance 48
5.12.1 SD card 48
5.12.2 Backup 48
5.12.3 Restore 49
5.12.4 Firmware update 50
5.12.5 Default Settings 51
5.12.6 Restart 51
5.12.7 Licenses 52
6 Notes on troubleshooting 53
7 Technical specifications 54

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 P9* - Functionality

The ***PROmesh P9*** devices are industrial Ethernet switches with management and Profinet functions that can be easily and conveniently configured via a Web application. It allows for an uncomplicated installation of bus, star and ring structures with switching functionality.

Features:

- Web application for configuration
- Redundant power supply 24V DC +/-20% with reverse voltage protection
- Monitoring the individual input voltages via configurable alarms
- A relay contact that is controlled via configurable alarms
- 10BASE-T/100BASE-TX (RJ45)
- PHY and MAC completely compatible to IEEE 802.3, IEEE802.3u and IEEE 802.3x
- Auto MDI/MDI-X crossover function for 100BASE-T and 10BASE-T ports
- Store-and-forward switching architecture with 2048 MAC address table
- PROFINET Conformance Class B
- PROFINET Netload Class III
- Quality of Service (QoS) with four priority queues
- Prioritisation via IEEE 802.1p Class of Service (COS), Type of Service (TOS) / DiffServ or Port priority
- Limitation of incoming and outgoing packages
- Port Mirror for TX or TX and RX packages
- Port-based VLAN / 802.1Q Tagged VLAN
- Simple Network Time Protocol (SNTP)
- Simple Mail Transfer Protocol (SMTP) for signalling alarms
- Internet Gateway Management Protocol Snooping (IGMP Snooping)
- Dynamical Host Configuration Protocol (DHCP) Client function
- Simple Network Management Protocol (SNMP)
- Updating, saving and backing up the system configuration via TFTP

1.2 Scope of supply

The scope of supply comprises the following individual parts:

- ***PROmesh P9***
- 7-pole plug-in terminal block (power supply + alarm contact)
- CD with device manual and configuration software

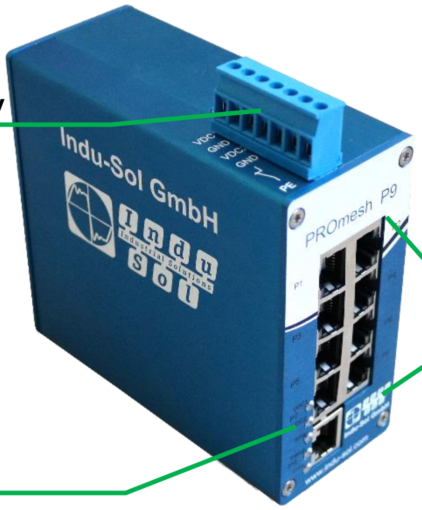
Please check the contents are complete before putting into operation.

1.3 Safety information

- Never open the housing of the ***PROmesh P9***
- Opening the housing immediately voids any warranty.
- If you think the device is defective, send it back to the supplier.

2 Device ports and status indicators

2.1 Device ports



X2 voltage supply and fault relay

VDC1	– DC 24V
GND	– 0V Ground
VDC2	– DC 24V
GND	– 0V Ground
	– Fault Relay
PE	– Protective Earth

X1 Network Ports

9 x RJ45

Status - LED

VDC1 / VDC2 / Ring / Status / Error

Figure 1: Device ports

3 Installation

3.1 Installation instructions

The ***PROmesh P9*** is installed horizontally inside the control cabinet on a 35 mm top-hat rail in accordance with DIN EN 60715.

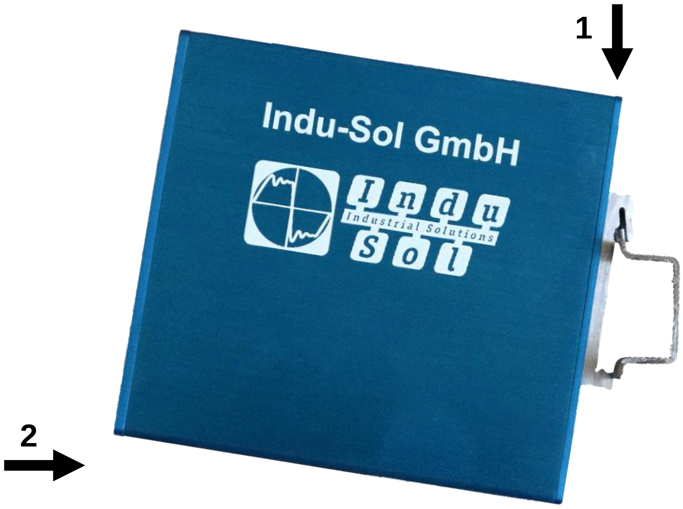


Figure 2: Device installation on top-hat rail

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

- From left and right: 20 mm
- From top and bottom: 50 mm

The removal of the device is displayed in Fig. 3.

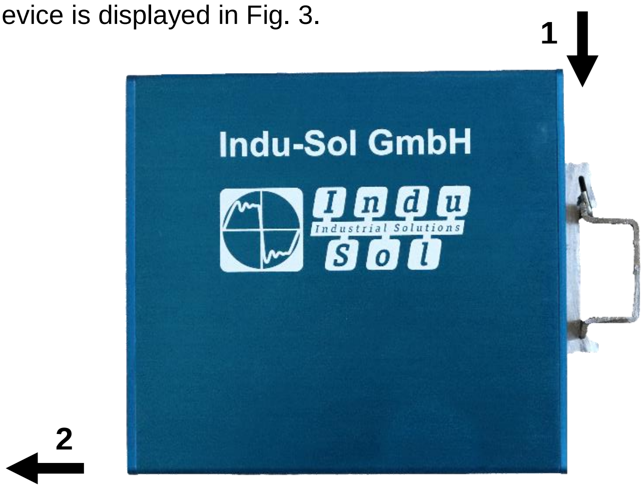


Figure 3: Removal

Do not mount the ***PROmesh P9*** switches directly next to device that emit strong electromagnetic interference fields, such as transformers, contactors, frequency inverter, etc.

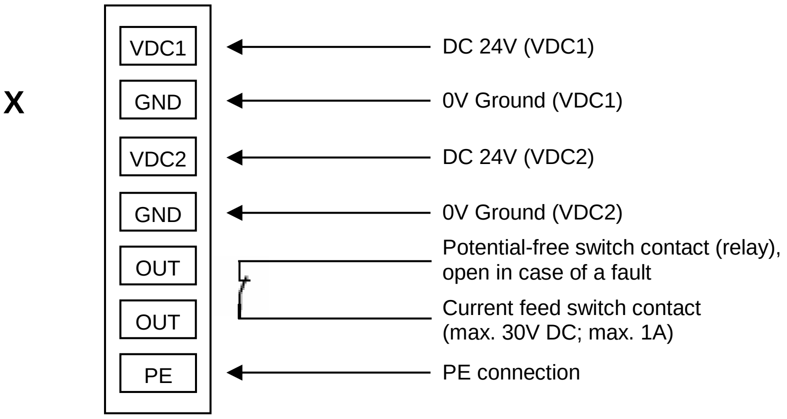
Do not mount the ***PROmesh P9*** switches directly next to devices that generate a lot of heat and protect the switch against direct sun light to prevent an undesirable warming up.

3.2 Connection voltage supply and fault relay

The terminal block for connecting the voltage supply as well as the switch contact is designed as a plug to make the mounting easier. Connect the supply voltage to the terminals VDC1 and GND. For a redundant voltage supply, you can connect to terminals VDC2 and GND as well. Both voltage inputs are protected internally against polarity reversal.

The permissible input voltage lies in the range of 24V DC +/-20%. The voltage needs to be an SELV/LPS-conforming voltage acc. to IEC 60950-1 / EN60950-1 / VDE0805-1. Please observe the note on SELV voltages under the legal information at the front of these operating instructions.

The 7-pole connector terminal block at the top of the device is assigned as follows:


X
VDC1
GND
VDC2
GND
OUT
OUT
PE
DC 24V (VDC1)
0V Ground (VDC1)
DC 24V (VDC2)
0V Ground (VDC2)
Potential-free switch contact (relay), open in case of a fault
Current feed switch contact (max. 30V DC; max. 1A)
PE connection

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 opens then for example in case of a voltage drop or an RJ45 port fault.

3.3 LED indicators

There are 5 diagnosis LEDs on the front panel of the switch. Additionally, each of the nine Ethernet ports features two status LEDs.

The diagnosis indicators provide real-time information on the status of the ***PROmesh P9*** (s. Table 1).

LED	Status	Meaning
VDC1	Green	There is sufficient voltage applied at connection VDC1
	Off	There is no sufficient voltage applied at connection VDC1
VDC2	Green	There is sufficient voltage applied at connection VDC2
	Off	There is no sufficient voltage applied at connection VDC2
Ring	Green	The switch is manager in the MRP ring
	Off	The switch is not 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
	Off	No voltage failure, no port fault and no configurable alarm active
FDX (Ethernet port)	Green	Full duplex mode
	Off	No connection (LNK/ACT off) or half duplex (LNK/ACT on)
LNK/ACT (Ethernet port)	Yellow	Connection available
	Flashing	Sending or receiving packages
	Off	No connection available

Table 1: LED functions

3.4 Ports

3.4.1 RJ-45 ports

The ***PROmesh P9*** features nine RJ-45 ports with transfer rates of 10 mbps or 100 mbps respectively. The baud rate is detected automatically by the respective port. The transmission and reception lines are crossed appropriately by MDI/MDI-X Autocrossover so that connections can be established to other devices independently from the cable type used (1:1 or crossed). MDI/MDI-X autocrossover can be deactivated by the web management.

3.4.2 Cabling

Use twisted-pair cables of the category 5 or better to connect the RJ-45 ports. The electric connection cable between the switch and the connection partner (switch, hub, workstation etc.) must not be longer than 100 metres.

4 Network topologies / Redundancy

By employing various protocols, the devices of the ***PROmesh P9*** product family can be implemented in star-shaped switched-Ethernet networks as well as in redundant networks such as intermeshed networks or rings.

4.1 Star structure

Classic Ethernet-star structures, see Figure 4, can be networked with the ***PROmesh P9*** switches without further configuration. The devices are functionable immediately.

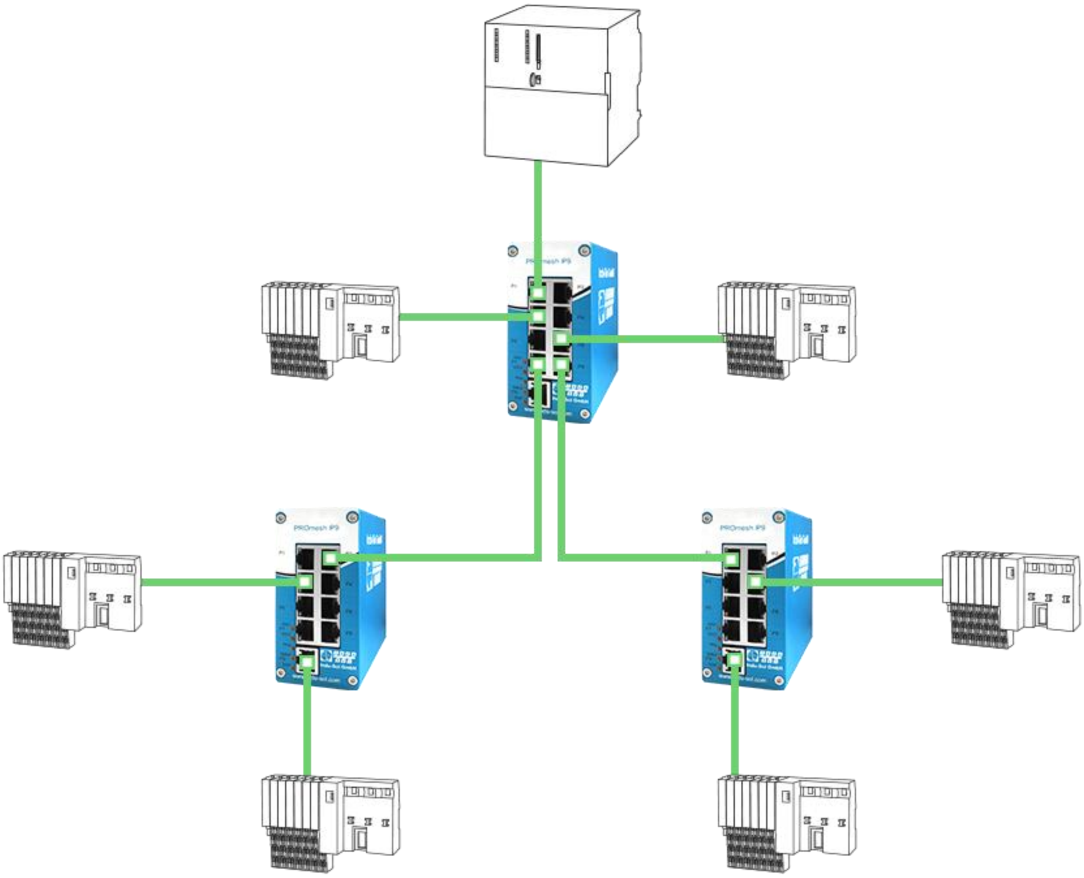


Figure 4: *PROmesh P9* in a star-shaped network

4.2 Ring structure

The ***PROmesh P9*** supports the Media Redundancy Protocol acc. to IEC 62429 (MRP Ring), which makes it possible for the system to recover within 200 ms or less in case of a network failure. The MRP ring thereby increases the reliability in the network. Figure 5 illustrates an example for an application with ring functionality.

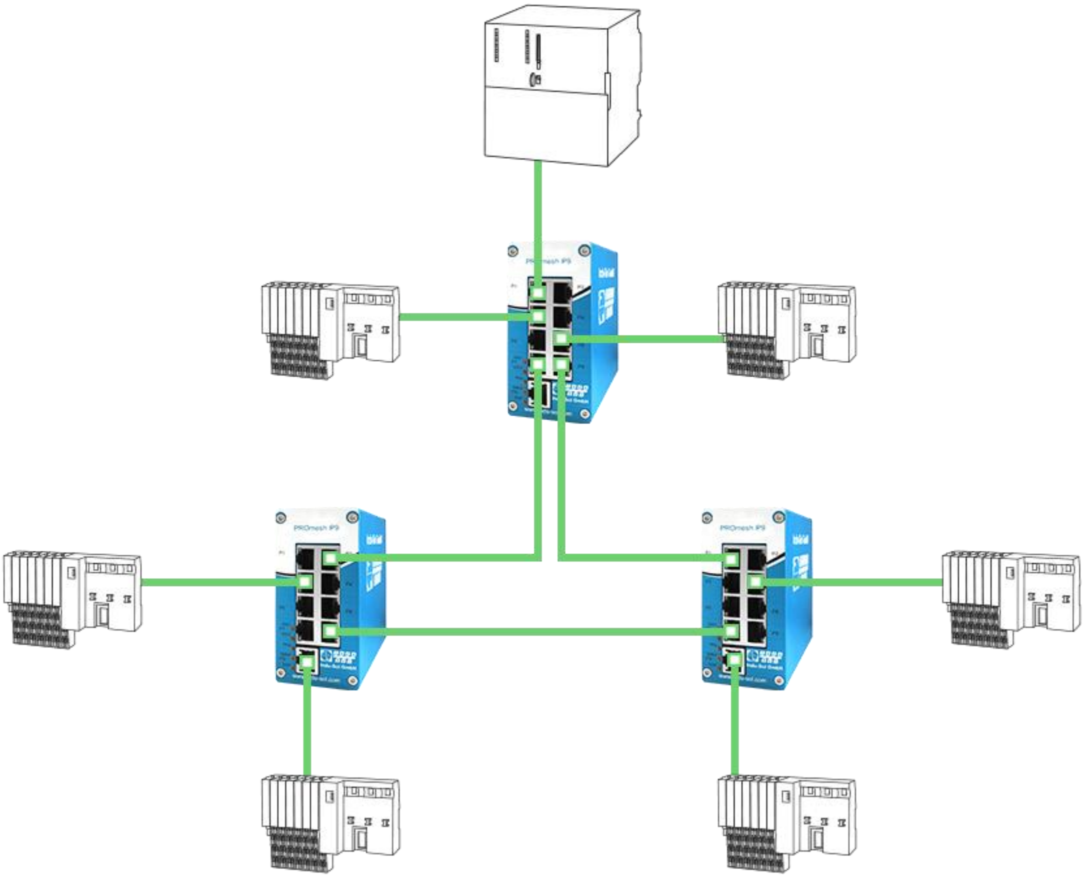


Figure 5: *PROmesh P9* in a ring-shaped network

5 Web application

The ***PROmesh P9*** switches are equipped with a modern web interface by which they can be conveniently configured from any web browser.

5.1 Preparations

Install the ***PROmesh P9*** 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. In delivery status of the device, the following IP address, subnet masks, administrator user name and password are set:

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

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/support/downloads/software/.
After installation and opening of 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.

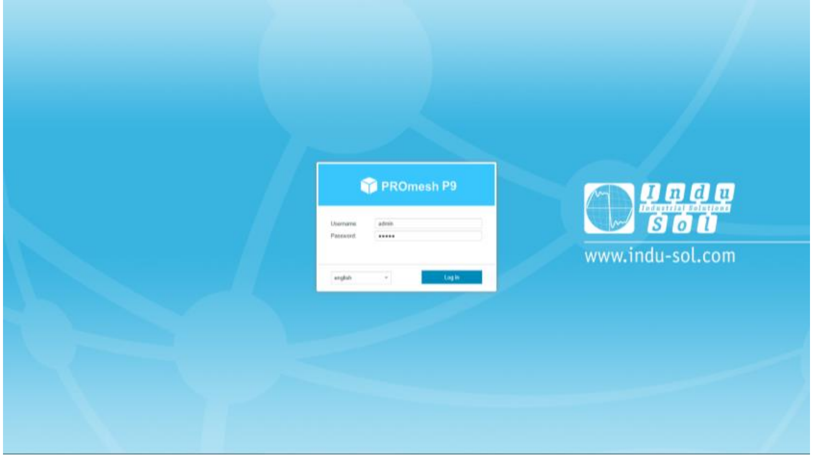
If you include the switch in a Profinet system in the hardware configuration of the controller, the corresponding address settings are carried out automatically by it afterwards.

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**

5.2 System login

1. Start a web browser on your computer.
2. Enter the IP address of the ***PROmesh P9*** switches used by you and confirm by pressing the "**Enter**" button.
3. The login mask of the device appears then on the screen.



Username: admin
Password: •••••

Figure 6: Login mask

4. Select the desired menu language (German/English).
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.

5.3 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. It is urgently necessary 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.

5.4 Start page with main overview

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 and to block the device. The Help button will show you information and explanations for the individual pages.

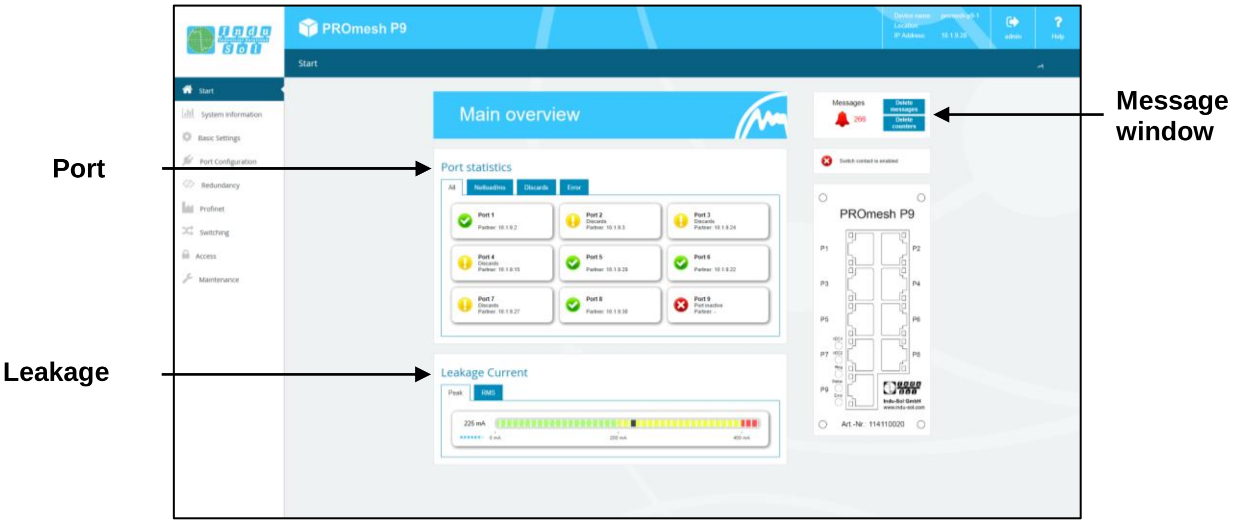
In the Port Statistics you will see an overview of the status of the available ports since the start or reset of the switch. Additionally the corresponding IP address of the communication partner is shown as well. By selecting the sub-items Network Limit, Discards and Error, you can call up the respective detail information.

The relevant period of evaluation can be selected by switching the time window between “current” and “history”. The “current” setting always displays the port condition at that particular moment. With the “history” pre-selection, all data is displayed since the beginning of the recording or the last time the “Delete counters” function was commanded.

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 current (Peak) and the effective value (RMS). Interference currents, which can lead to direct communication problems, are made visible early on by this information.

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.



Device name promeshp9-1
Location
IP Address 10.1.9.20

266

Switch contact is enabled

Port 1 Partner: 10.1.9.2
Port 2 Discards Partner: 10.1.9.3
Port 3 Discards Partner: 10.1.9.24
Port 4 Discards Partner: 10.1.9.15
Port 5 Partner: 10.1.9.29
Port 6 Partner: 10.1.9.22
Port 7 Discards Partner: 10.1.9.27
Port 8 Partner: 10.1.9.30
Port 9 Port inactive Partner: -

225 mA
0 mA
200 mA
400 mA

Indu-Sol GmbH
www.indu-sol.com
Art.-Nr.: 114110020

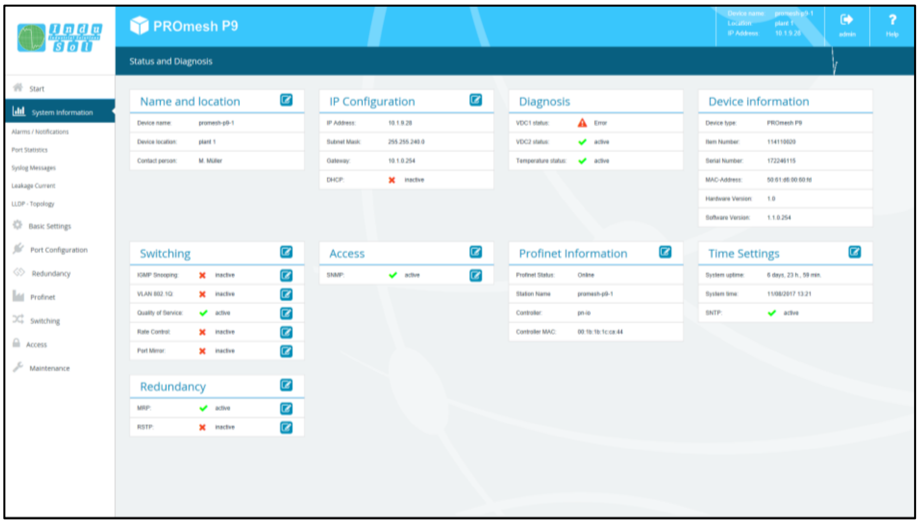
Figure 7: Main overview

5.5 System information

The System Information offers you a complete overview of the status and the current configuration of the ***PROmesh P9***.

5.5.1 Status and diagnosis

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 function to make settings there.



Status and Diagnosis

Name and location

Device name:	promesh-p9-1
Device location:	plant 1
Contact person:	M. Müller

IP Configuration

IP Address:	10.1.9.28
Subnet Mask:	255.255.240.0
Gateway:	10.1.0.254
DHCP:	✗ inactive

Diagnosis

VDC1 status:	⚠ Error
VDC2 status:	✓ active
Temperature status:	✓ active

Device information

Device type:	PROmesh P9
Item Number:	114110020
Serial Number:	172246115
MAC-Address:	50:61:d6:00:60:fd
Hardware Version:	1.0
Software Version:	1.1.0.254

Switching

IGMP Snooping:	✗ inactive
VLAN 802.1Q:	✗ inactive
Quality of Service:	✓ active
Rate Control:	✗ inactive
Port Mirror:	✗ inactive

Access

SNMP:	✓ active

Profinet Information

Profinet Status:	Online
Station Name	promesh-p9-1
Controller:	pn-io
Controller MAC:	00:1b:1b:1c:ca:44

Time Settings

System uptime:	6 days, 23 h., 59 min.
System time:	11/08/2017 13:21
SNTP:	✓ active

Redundancy

MRP:	✓ active
RSTP:	✗ inactive

Figure 8: Status and diagnosis

5.5.2 Alarms / Notifications

The Alarms / Notifications (Figure 9) 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 device temperature
- Failure of a supply voltage
- MRP protocol event
- Leakage current too high
- Detecting a change of the port connection (Wrong Neighbour)
- Exceeding the network utilisation at a port

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

- Fault relay
- SNMP trap
- E-mail alarm

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

The configured alarm assignments are displayed in lists with consecutive IDs. By using the tabs Alarm trigger and Alarm receiver, the view can be switched between:

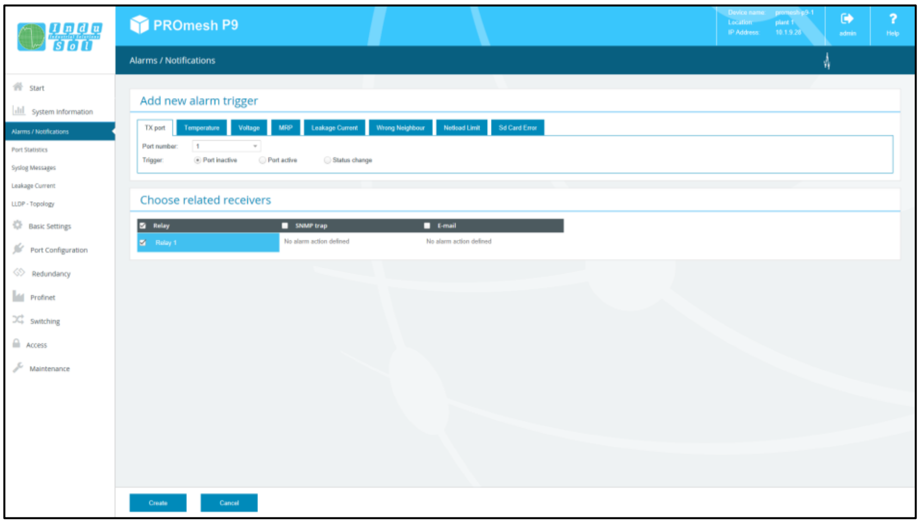
- Alarm trigger with assigned Alarm receiver
- Alarm receiver with assigned Alarm trigger

The alarm receiver “Profinet” is permanently system-internally set in a Profinet network (5.9 Profinet) 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.

Adding and editing alarm triggers

Under the tab Alarm trigger (Figure 9), new alarms can be added by clicking on the "+" button above the table. If alarms are already available, then the user has the option to edit or delete them by the click of a button (right column in the overview). In the upper part of the page "Add new alarm trigger" that is displayed then, the user can specify the various alarms. Within the creation and editing of the alarms, the corresponding receivers can be selected in the lower part of the page and thus linked to the alarm trigger. The following alarm triggers are possible:

- The network ports can trigger an alarm during activity, inactivity and status change.
- The menu item Temperature serves to specify the lower and upper temperature limits. If the temperature measured by the device reaches a value outside of the defined limits, an alarm is triggered.
- In the Voltage option, the monitoring of the input voltage(s) is defined. A specification can be made here which alarm should be triggered if either one or even both voltage supplies malfunction.
- With an active MRP ring redundancy, alarms can be triggered for detected changes of the ring configuration.
- If a defined leakage current is exceeded here, an alarm can be triggered. Additionally to this alarm, the frequency spectrum incl. RMS value is saved.
- By activating the point Wrong Neighbour, an alarm is triggered and also the port assignment of the output configuration.
- With the option Network Limit, messages for the exceeding of the configured limit can be sent.



Add new alarm trigger

Port number: 1

Trigger: ● Port inactive ○ Port active ○ Status change

Choose related receivers

☑ Relay	□ SNMP trap	□ E-mail
☑ Relay 1	No alarm action defined	No alarm action defined

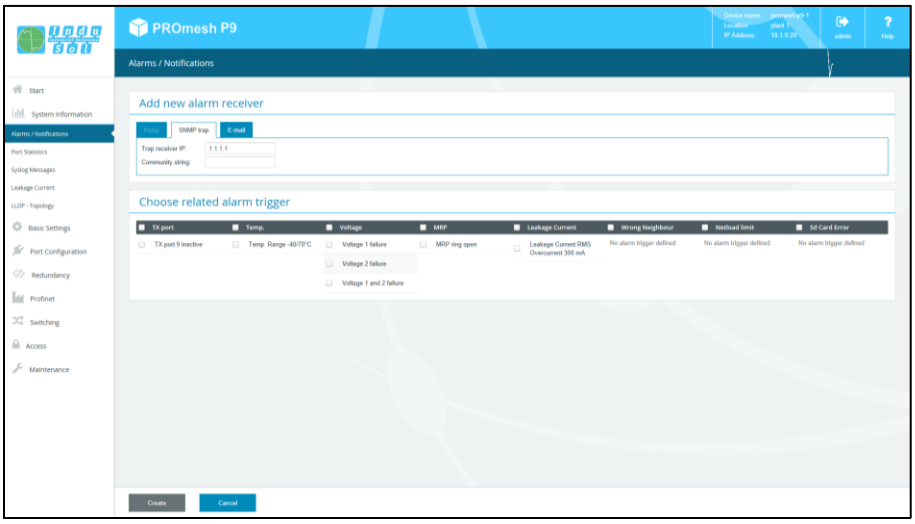
Figure 9: Alarms / Notifications: Adding an alarm trigger

Adding and editing alarm receivers

Click the button with the "+" symbol above the table to add further alarm receivers on the Alarm receiver (Figure 10) page. The device-internal relay is already specified as alarm receiver and cannot be deleted but only linked to alarm triggers. Once the menu item "Add new alarm action” has been selected, a choice is given to the user between SNMP trap and e-mail. The corresponding alarm triggers can be linked in the lower part of the page to the current receiver.

- In the Simple Network Management Protocol (SNMP), fault 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 respective user. Optionally, the authentication can be activated. Please enter the necessary access data for that.

The alarm receivers are linked to the alarm triggers by activating the checkboxes in the lower part of the page and activated by clicking on Create or Apply.



Device name: promesh-p9-1
Location: plant 1
IP Address: 10.1.9.28

Add new alarm receiver

Trap receiver IP: 1.1.1.1
Community string:

Choose related alarm trigger

■ TX port	■ Temp.	■ Voltage	■ MRP	■ Leakage Current	■ Wrong Neighbour	■ Netload limit	■ Sd Card Error
□ TX port 9 inactive	□ Temp. Range -40/70°C	□ Voltage 1 failure	□ MRP ring open	□ Leakage Current RMS Overcurrent 300 mA	No alarm trigger defined	No alarm trigger defined	No alarm trigger defined
		□ Voltage 2 failure					
		□ Voltage 1 and 2 failure					

Figure 10: Adding an alarm receiver

5.5.3 Port statistics

The Port Statistics (Figure 11) page provides information on the data traffic of the individual ports, which is helpful for diagnosis purposes in case of overload or network problems. The maximum network limit and the total number of sent, received, faulty and colliding packages are displayed.

The display of the graphic port load is displayed depending on the selected port, the current incoming or outgoing network load, as well as the minimum, average and maximum values.

The calculation of this netload is done specifically down to the millisecond for the low update rates of industrial Ethernet protocols.

Furthermore, the size of the individual packages is recorded statistically up to various limit values in the statistic details.

Amongst the sent packages, a difference is made between:

- Number of all packages
- Number of the Unicast packages (packages to one receiver)
- Number of the non-Unicast packages (packages to several receivers)

Amongst the received packages, a difference is made between:

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

The column CRC faults provides information about the number of faultily received data packages. The cyclic redundancy check CRC determines a test value based on the transmitted data. This value is sent together with the data and is evaluated by the receiver. Faulty packages are detected thereby and discarded.

The total number of all collisions and those of the late collisions are displayed in the Collisions column.

The column Packages up to bytes provides information about the number of packages in various sizes. The number of the received packages up to 64, 127, 255, 511, 1023 or 1518 byte size are recorded.

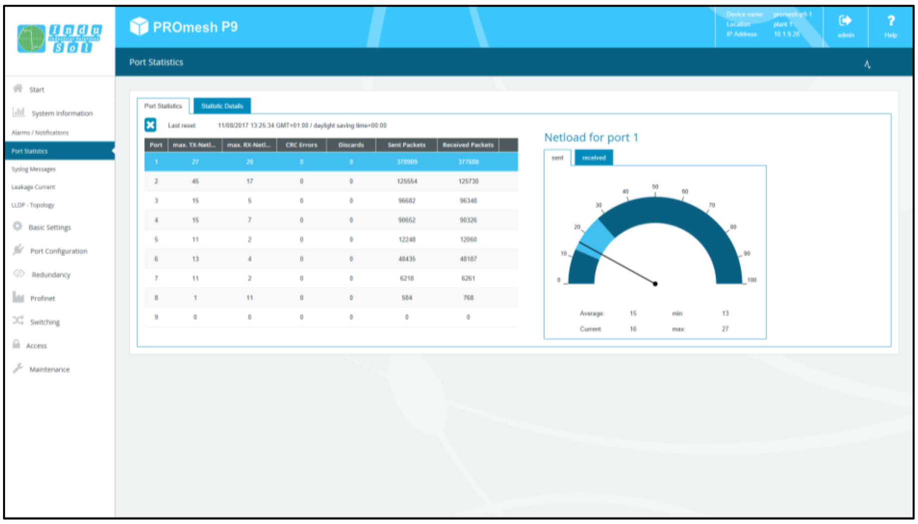
Updating and resetting the values

In the status bar over the table, the counters of all ports can be reset and a new evaluation started in this manner. The time point at which the evaluation was started is displayed as last reset in the status line.

Sorting and hiding the entries

The statistic details offer valuable information for the network diagnosis. To simplify the diagnosis further, there is an option to limit the display to the most important columns.

Individual columns can be hidden or sorted for this purpose via pull-down menus in the table headers.



Device name: promesh-p9-1
Location: plant 1
IP Address: 10.1.9.28

Last reset: 11/08/2017 13:25:34 GMT+01:00 / daylight saving time+00:00

Port	max. TX-Netl...	max. RX-Netl...	CRC Errors	Discards	Sent Packets	Received Packets
1	27	20	0	0	378909	377688
2	45	17	0	0	125554	125730
3	15	5	0	0	96682	96348
4	15	7	0	0	90652	90326
5	11	2	0	0	12248	12060
6	13	4	0	0	48435	48187
7	11	2	0	0	6218	6261
8	1	11	0	0	584	768
9	0	0	0	0	0	0

Average 15 min 13
Current 16 max 27

Figure 11: Port Statistics

5.5.4 Syslog messages

The Syslog Messages (Figure 12) help the user to receive status and fault message of the various functions and protocols. The messages are displayed in the overview with date and time as well as a code, a description and a reference. To archive the messages permanently, an option is provided to write them on an SD card as a storage medium or also on an external syslog server.

Using the syslog server

To archive or save the messages on a syslog server, activate this function via the marking box in the top bar. Enter the IP address of the syslog server written with decimal points and save the settings using the Apply button that appears at the bottom end. Please check if the server can be reached and saves the messages in a file.

Saving the syslog messages on SD card

To save the messages on the SD card, make sure that an SD card has been inserted and activate this function. Save the settings afterwards using the Apply button that appears in the lower area. Please check then whether there is enough free memory available on the SD card and whether the messages have been saved in a file.

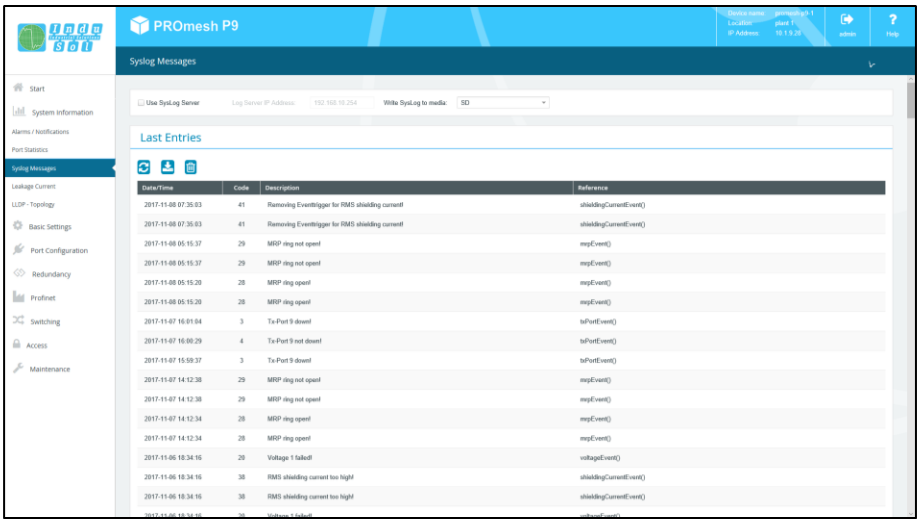
Updating, exporting and resetting the entries

The following buttons are available here:

- Press the Update button in the status bar located above the table to reload the table.
- The CSV Export button creates a CSV file (Comma-Separated Values) with all entries of the table and saves them in the download directory of the browser. The messages are written separated by commas, line-by-line into a file.
- The button to Delete the log file removes all entries from the table and shows all messages that occur after this time point. The time point of the deleting of the entries can be seen at the newly appearing log entry.

Sorting and hiding the entries

Individual columns of the syslog messages can be hidden or sorted via pull-down menus in the table headers.



□ Use SysLog Server   Log Server IP Address: 192.168.10.254   Write SysLog to media: SD

Last Entries

Date/Time	Code	Description	Reference
2017-11-08 07:35:03	41	Removing Eventtrigger for RMS shielding current!	shieldingCurrentEvent()
2017-11-08 07:35:03	41	Removing Eventtrigger for RMS shielding current!	shieldingCurrentEvent()
2017-11-08 05:15:37	29	MRP ring not open!	mrpEvent()
2017-11-08 05:15:37	29	MRP ring not open!	mrpEvent()
2017-11-08 05:15:20	28	MRP ring open!	mrpEvent()
2017-11-08 05:15:20	28	MRP ring open!	mrpEvent()
2017-11-07 16:01:04	3	Tx-Port 9 down!	txPortEvent()
2017-11-07 16:00:29	4	Tx-Port 9 not down!	txPortEvent()
2017-11-07 15:59:37	3	Tx-Port 9 down!	txPortEvent()
2017-11-07 14:12:38	29	MRP ring not open!	mrpEvent()
2017-11-07 14:12:38	29	MRP ring not open!	mrpEvent()
2017-11-07 14:12:34	28	MRP ring open!	mrpEvent()
2017-11-07 14:12:34	28	MRP ring open!	mrpEvent()
2017-11-06 18:34:16	20	Voltage 1 failed!	voltageEvent()
2017-11-06 18:34:16	38	RMS shielding current too high!	shieldingCurrentEvent()
2017-11-06 18:34:16	38	RMS shielding current too high!	shieldingCurrentEvent()
2017-11-06 18:34:16	20	Voltage 1 failed!	voltageEvent()

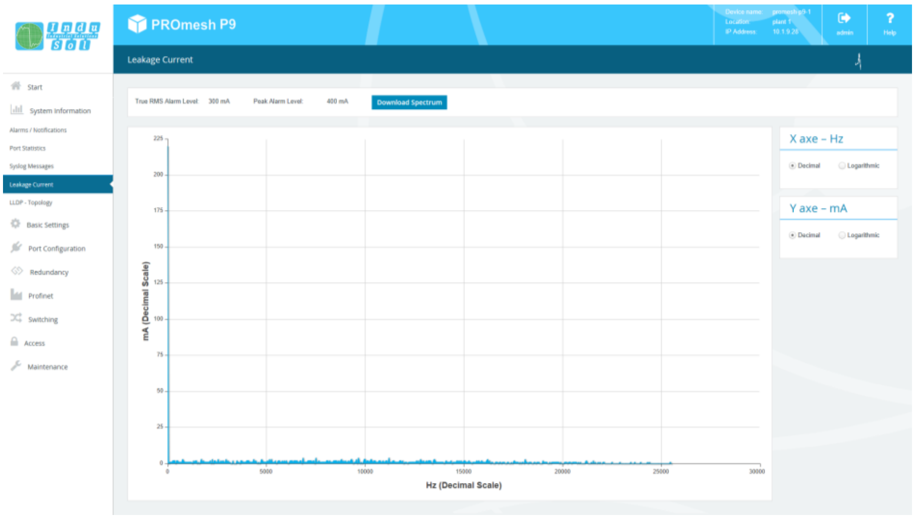
Figure 12: Syslog Messages

5.5.5 Leakage current

The Leakage Current Monitoring (Figure 13) makes it possible to permanently record and evaluate the sum of all shielding 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.

Further functions for this are:

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



True RMS Alarm Level: 300 mA

Peak Alarm Level: 400 mA

X axe – Hz: ● Decimal ○ Logarithmic

Y axe – mA: ● Decimal ○ Logarithmic

Figure 13: Leakage Current

5.5.6 Link Layer Discovery Protocol (LLDP) – Topology

The LLDP topology presents the neighbouring devices by ports with IP addresses and description (see Figure 14). 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 own status in periodic intervals and receives information from the neighbouring devices.

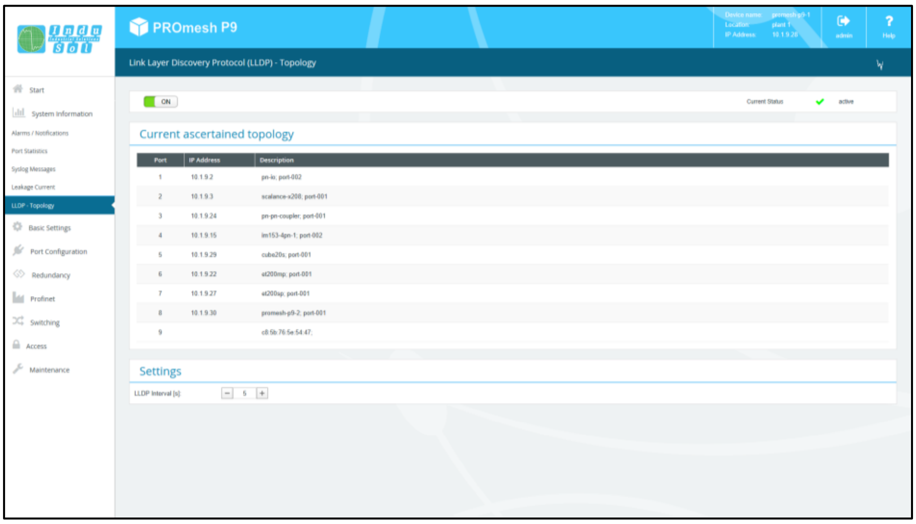
Since this takes place independently from each other, the LLDP is also termed a one-way protocol.

The following information is compiled and sent by the LLDP:

- System name
- System description
- Port description

LLDP interval

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



Link Layer Discovery Protocol (LLDP) - Topology

ON

Current Status ✓ active

Current ascertained topology

Port	IP Address	Description
1	10.1.9.2	pn-io; port-002
2	10.1.9.3	scalance-x208; port-001
3	10.1.9.24	pn-pn-coupler; port-001
4	10.1.9.15	im153-4pn-1; port-002
5	10.1.9.29	cube20s; port-001
6	10.1.9.22	et200mp; port-001
7	10.1.9.27	et200sp; port-001
8	10.1.9.30	promesh-p9-2; port-001
9		c8:5b:76:5e:54:47;

Settings

LLDP Interval [s]: − 5 +

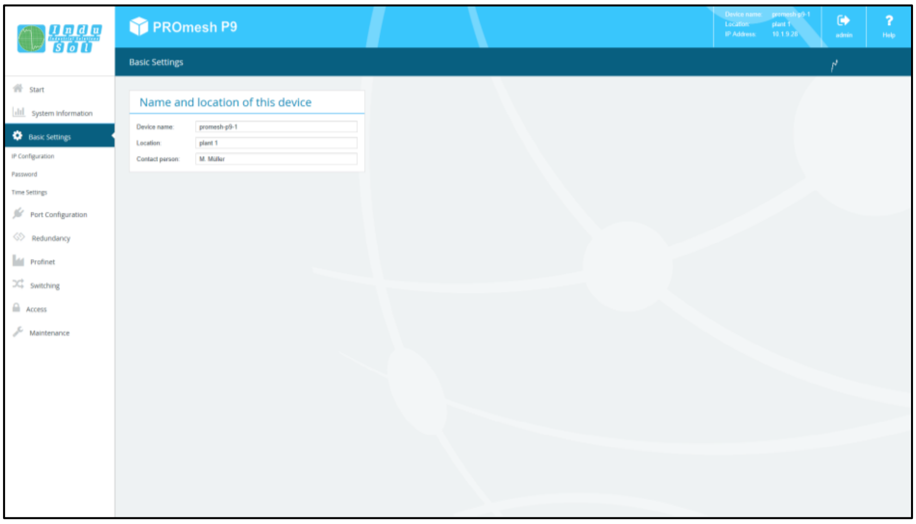
Figure 14: LLDP – Topology

5.6 Basic settings

The Basic Settings page (Figure 15) allows you to give the device a unique device name, a location of installation 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 so that up to 50 characters can be entered. Using special symbols is permitted. Device name and location are displayed in the information bar at the top right and help you assign the web interface to a device.



Name and location of this device

Device name: promesh-p9-1

Location: plant 1

Contact person: M. Müller

Figure 15: Basic settings of the ***PROmesh P9***

5.6.1 IP configuration

The IP Configuration (Figure 16) can be done either by the PROFINET controller via the Dynamic Configuration Protocol (DCP), automatically using the Dynamic Host Configuration Protocol (DHCP) or by manual settings. Depending on the settings of the DHCP servers, the IP address can change with the automatic address assignment after a device restart.

On an existing PROFINET connection, no automatic or manual IP configuration is possible.

PROFINET

If the device is configured in a PROFINET network, the device receives its IP configuration from the PROFINET controller via the DCP protocol.

Automatic

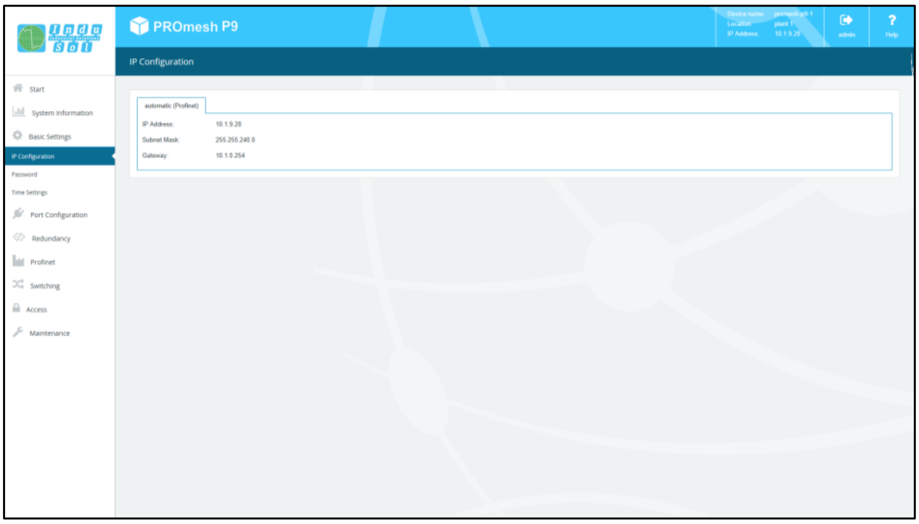
Activate the DHCP client function to receive a configuration of the IP address, the subnet mask and the standard gateway from a server operating in the network with appropriate functionality.

Once you have saved the settings by clicking on the Apply button, the device will send a query into the network 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

In case your network does not feature a DHCP or BootP server or the setting should be made manually, then select the manual IP configuration in the upper area of the page. Please check carefully which settings you make so that there are no problems with double IP addresses that can negatively influence your entire network. The format of the IP address, the subnet mask and the gateway has to be entered with decimal points. The following settings are necessary:

- 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.



IP Configuration

automatic (Profinet)

IP Address: 10.1.9.28

Subnet Mask: 255.255.240.0

Gateway: 10.1.0.254

Figure 16: IP Configuration

5.6.2 Password

On the Password page (Figure 17), the preset standard password for the users Admin and User can be changed. The current or old password needs to be known for that and entered. The user names and rights of the administrator and user are permanently specified and cannot be changed.

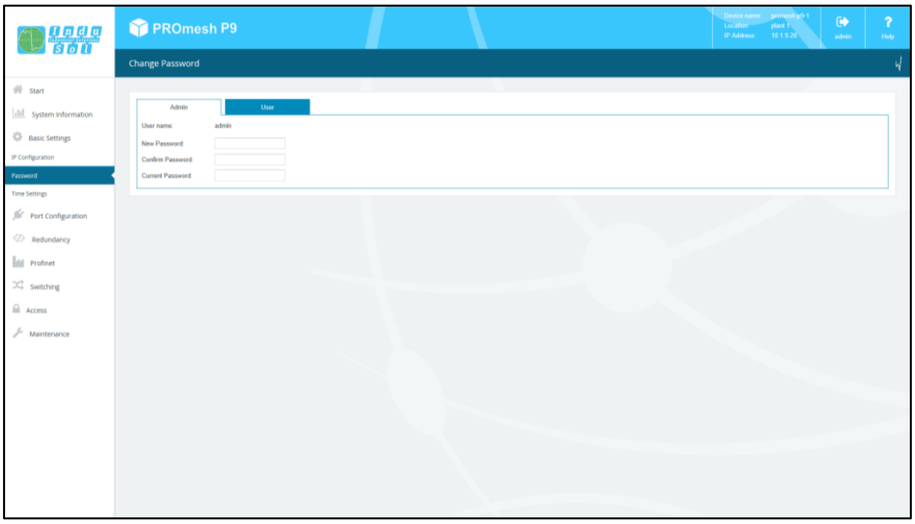
The following form boxes are available:

- 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 that should be changed now.

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 rather 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



Device name: promesh-p9-1
Location: plant 1
IP Address: 10.1.9.28

Change Password

User name: admin
New Password:
Confirm Password:
Current Password:

Figure 17: Changing the password for administrator and guest access

5.6.3 Time setting

This page displays the system time and the current date in the upper area (Figure 18). The system uptime follows in the middle. The currently used settings of the system time and a possible shift due to daylight saving time are presented way on the right.

When setting the data and time, you can choose between using a time server and a manual configuration. The automatic configuration of the system time by Simple Network Time Protocol (SNTP) updates the time at regular intervals.

Setting the system time automatically by SNTP

To set the system time via SNTP, a connection to an SNTP server is necessary. On this page you can make the corresponding settings to synchronise the system time of the device.

A precise system time is useful in particular if log files need to be evaluated in case of a malfunction. This may help localise the cause of a fault easier and to assign to an event. The following settings are necessary when using SNTP:

- SNTP server IP address: Enter the IP address of a time server here. Please enter with decimal points.
- SNTP server IP address (redundancy): In this box you can enter the IP address of a second, redundant time server. In case the first server cannot be reached, the time will be synchronised via this SNTP server.
- Update interval: Enter the intervals here by which the device should synchronise itself with the time server.
- Time zone: Enter the time zone in which the device is located.

Entering the system time by hand

When setting the system time manually, you have the option to use the time of the browser or to enter and save the date and time by hand.

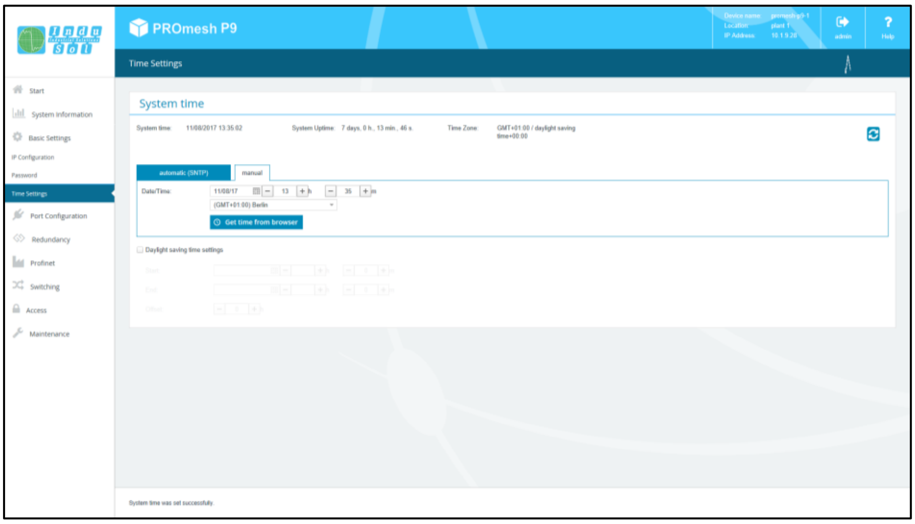
To use the browser's time, press the Use time of the browser button, check the entry in Date/Time and save the values with the Apply button.

In case you want to make the settings by hand, select the current date first of all by input box. You can also enter the data using the keyboard: First two positions for the month, then two for the day and finally two or four positions for the year. Enter the time and the corresponding time zone and check if everything was saved properly. Save the settings finally using the Apply button.

Daylight saving time settings

In case you wish to use the automatic switching between normal and daylight saving time, activate the option Daylight saving time settings.

- Begin: Define at which date and at what time daylight saving time should start.
- End: Define at which date and at what time daylight saving time should end and the time changed back to normal time.
- Offset: Please enter the time shift that lies between daylight saving time and standard time.



System time

System time: 11/08/2017 13:35:02 System Uptime: 7 days, 0 h., 13 min., 46 s. Time Zone: GMT+01:00 / daylight saving time+00:00

automatic (SNTP) | manual

Date/Time: 11/08/17 13 h 35 m
(GMT+01:00) Berlin
Get time from browser

□ Daylight saving time settings

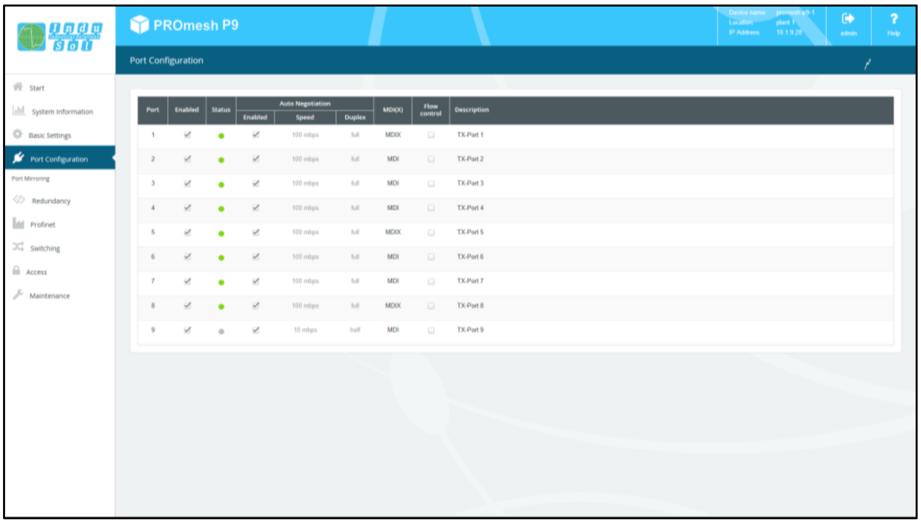
Start:
End:
Offset:

System time was set successfully.

Figure 18: Configuration of the time settings

5.7 Port configuration

The table for Port Configuration (Figure 19) provides an overview of the current settings of the individual ports. Additionally, you can configure the columns Enabled, Auto Negotiation, Flow Control and Description. The remaining boxes are partially updated by a changed port assignment and subsequent reloading of the page or they serve to provide a better overview.



Device name: promesh-p9-1
Location: plant 1
IP Address: 10.1.9.20

Port Configuration

Port	Enabled	Status	Auto Negotiation			MDI(X)	Flow control	Description
			Enabled	Speed	Duplex			
1	✓	●	✓	100 mbps	full	MDIX	□	TX-Port 1
2	✓	●	✓	100 mbps	full	MDI	□	TX-Port 2
3	✓	●	✓	100 mbps	full	MDI	□	TX-Port 3
4	✓	●	✓	100 mbps	full	MDI	□	TX-Port 4
5	✓	●	✓	100 mbps	full	MDIX	□	TX-Port 5
6	✓	●	✓	100 mbps	full	MDI	□	TX-Port 6
7	✓	●	✓	100 mbps	full	MDI	□	TX-Port 7
8	✓	●	✓	100 mbps	full	MDIX	□	TX-Port 8
9	✓	●	✓	10 mbps	half	MDI	□	TX-Port 9

Figure 19: Overview of the Port Configuration

The following columns are displayed:

- 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 switch and the connected receiver coordinate the settings automatically with each other. If auto negotiation is deactivated, you can make the settings 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): By standard, the device can execute autocrossover detection. 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. The connected device is simultaneously signalled that it ceases the 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 diagnosis in case of malfunction. Click directly on the port description and edit the name in this row.

5.7.1 Port mirroring

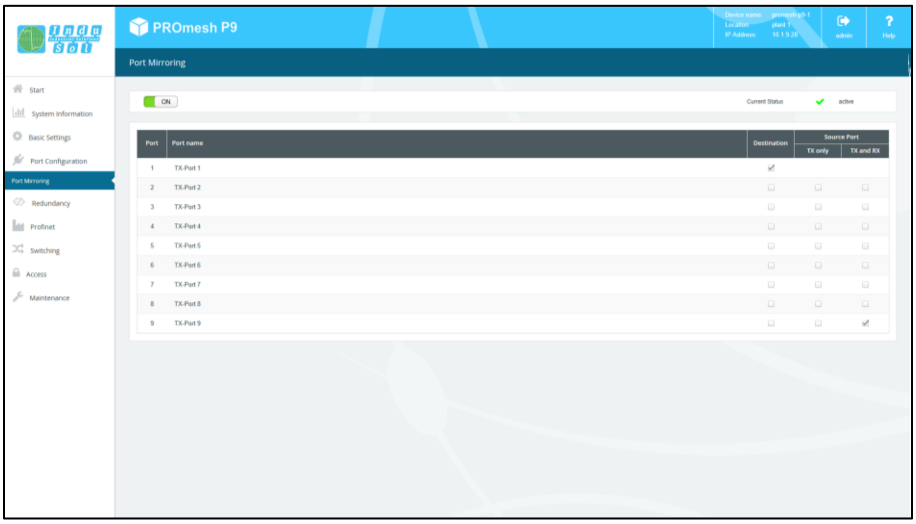
Port Mirroring (Figure 20) is a method in networks to route the traffic of one port (source) simultaneously to a second port (destination) and to check that. This means that the received and sent packages of the source port to the port to be monitored are duplicated.

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. 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 specify up to eight source ports in the switch. Mark the respective checkbox to select the corresponding port.

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

Deactivate Port Mirroring in normal mode and use it only for problem analysis.



Port Mirroring

ON Current Status ✓ active

Port	Port name	Destination	Source Port	
			TX only	TX and RX
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	TX-Port 9	□	□	☑

Figure 20: Port Mirroring

5.8 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 at a time. Press the Edit buttons to go to the protocol settings 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.

5.8.1 Media Redundancy Protocol (MRP)

The Media Redundancy Protocol (Figure 21) 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.

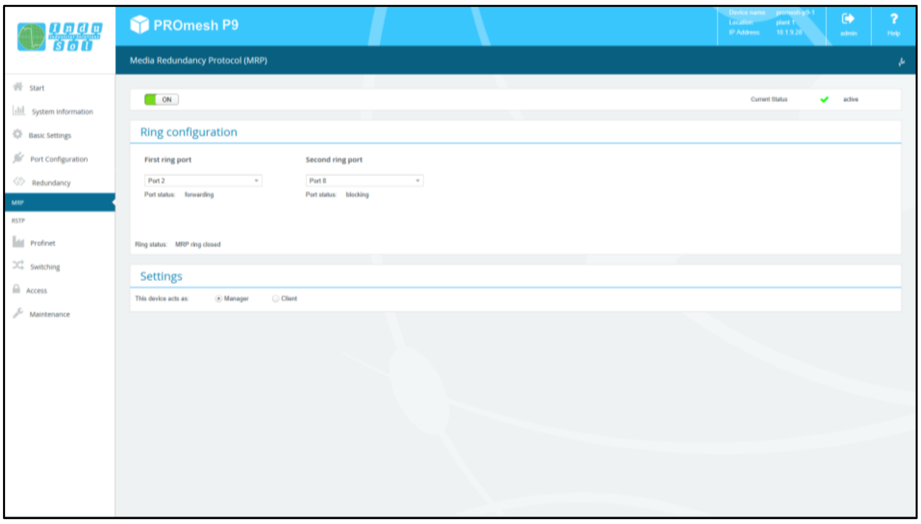
MRP uses a redundancy manager that uses specific test packages to check the continuity of the ring and reconfigures the network in case of an error and also informs all devices about that. The guaranteed reconfiguration time at up to 50 devices in the ring is 200 ms. In a typical application, the reconfiguration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

The ring may be closed physically only when MRP has been completely configured.

Ring configuration

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 cannot be a primary ring port at the same time.
- Ring status: Specify whether the ***PROmesh P9*** should act as manager or as client. Please also note thereby that only one manager may be used per ring.



Media Redundancy Protocol (MRP)

ON

Current Status ✓ active

Ring configuration

First ring port: Port 2
Port status: forwarding

Second ring port: Port 8
Port status: blocking

Ring status: MRP ring closed

Settings

This device acts as: ● Manager ○ Client

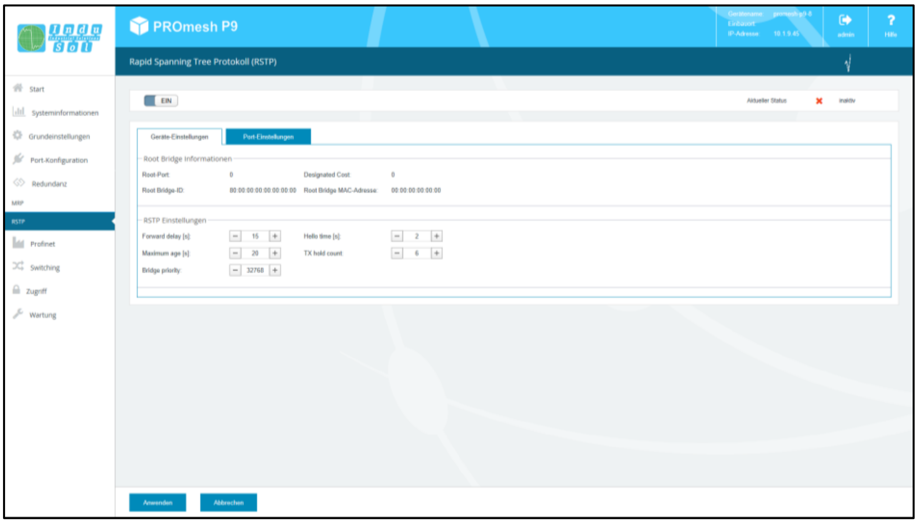
Figure 21: Media Redundancy Protocol (MRP)

5.8.2 Rapid Spanning Tree Protocol (RSTP)

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

Activate the RSTP function global before configuring the corresponding parameters.

5.8.2.1 Device settings



Rapid Spanning Tree Protokoll (RSTP)

EIN

Aktueller Status ✗ inaktiv

Root Bridge Informationen

Root-Port: 0
Designated Cost: 0
Root Bridge-ID: 80:00:00:00:00:00:00:00
Root Bridge MAC-Adresse: 00:00:00:00:00:00

RSTP Einstellungen

Forward delay [s]: 15
Hello time [s]: 2
Maximum age [s]: 20
TX hold count: 6
Bridge priority: 32768

Figure 22: Rapid Spanning Tree Protocol (RSTP) – Device settings

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.

RSTP Settings

Configure the protocol for your application case:

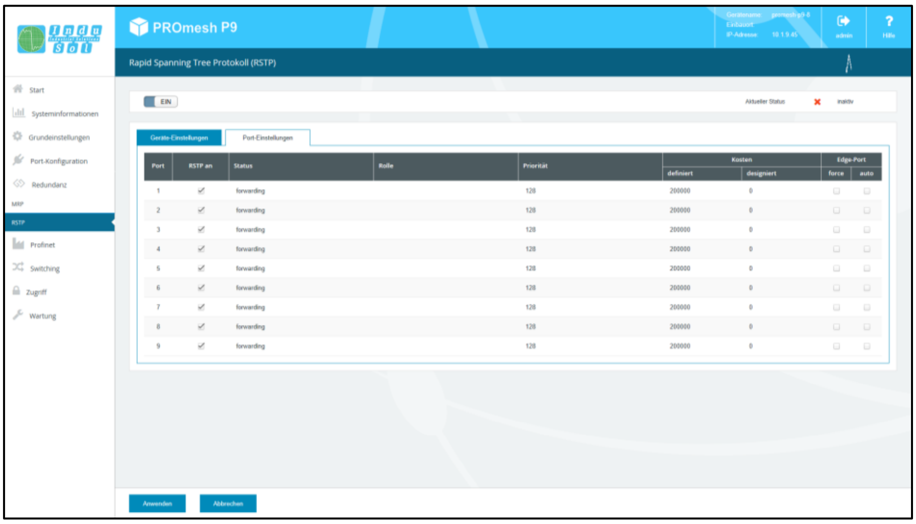
- Forward delay: The time that a port waits before it switches from RSTP Learning and Listening status in den Forwarding status. Enter a value between 4 and 30 seconds.
- Maximum age: The time that a bridge waits before trying a new configuration without receiving messages from the Spanning Tree configuration 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.

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 find 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.

5.8.2.2 Port settings



Port	RSTP an	Status	Rolle	Priorität	Kosten		Edge-Port	
					definiert	designiert	force	auto
1	✓	forwarding		128	200000	0	□	□
2	✓	forwarding		128	200000	0	□	□
3	✓	forwarding		128	200000	0	□	□
4	✓	forwarding		128	200000	0	□	□
5	✓	forwarding		128	200000	0	□	□
6	✓	forwarding		128	200000	0	□	□
7	✓	forwarding		128	200000	0	□	□
8	✓	forwarding		128	200000	0	□	□
9	✓	forwarding		128	200000	0	□	□

Figure 23: Rapid Spanning Tree Protocol – Port Settings

The following entries are displayed in the settings for the ports:

- Port: Display of the port number.
- 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 path 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 to take cable lengths or maximum baud rates into account.
    - 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 reconfiguration time of the redundancy protocol.
    - Force: The port is configured by standard as edge port.
    - Auto: The detection as edge port is done automatically.

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

5.9 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 Profinet IO Device for the connection of distributed periphery to a Profinet controller and supports the Conformance Class B. You can configure the port settings for DCP on this page and download the configuration file.

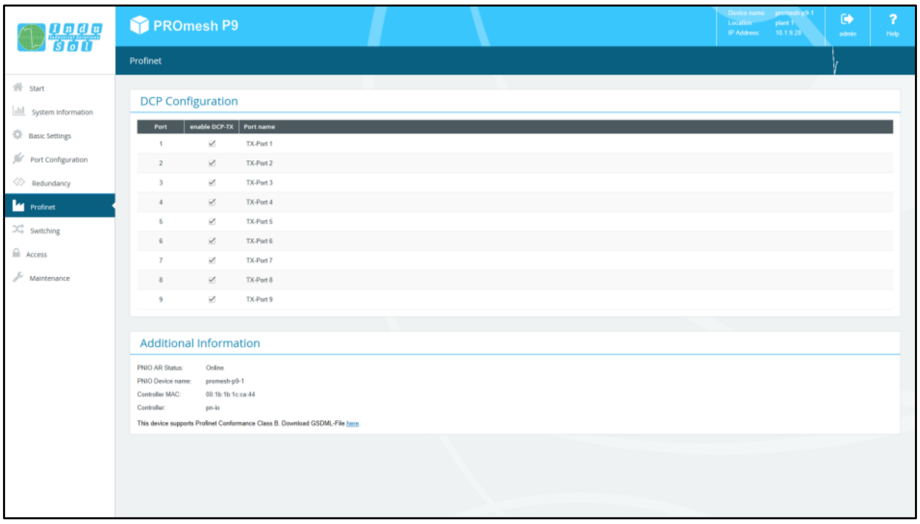
Port settings:

- 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.

Configuration file

The configuration file saved on this page and the license page serves to describe Profinet field devices. The file is written in General Station Description Markup Language (GSDML) and serves as a basis for planning the configuration of a Profinet IO system.

The option is also available to download the GSDML file via the following link: https://www.indu-sol.com/support/downloads/software/



DCP Configuration

Port	enable DCP-TX	Port name
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	✓	TX-Port 9

Additional Information

PNIO AR Status: Online
PNIO Device name: promesh-p9-1
Controller MAC: 00:1b:1b:1c:ca:44
Controller: pn-io

This device supports Profinet Conformance Class B. Download GSDML-File here.

Figure 24: Profinet

5.10 Switching

This page provides an overview of the activated and deactivate 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.

Aging Time: Enters the time frame, in which a MAC address is still maintained after the disconnection from the port or switching off the device. You can select values between 16 and 4080 seconds, in steps of 16 seconds each. Standard setting is 304 seconds.

5.10.1 IGMP snooping

The Internet Group Management Protocol (IGMP) is a protocol of the Internet protocol family. IGMP Snooping (Figure 25) 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:

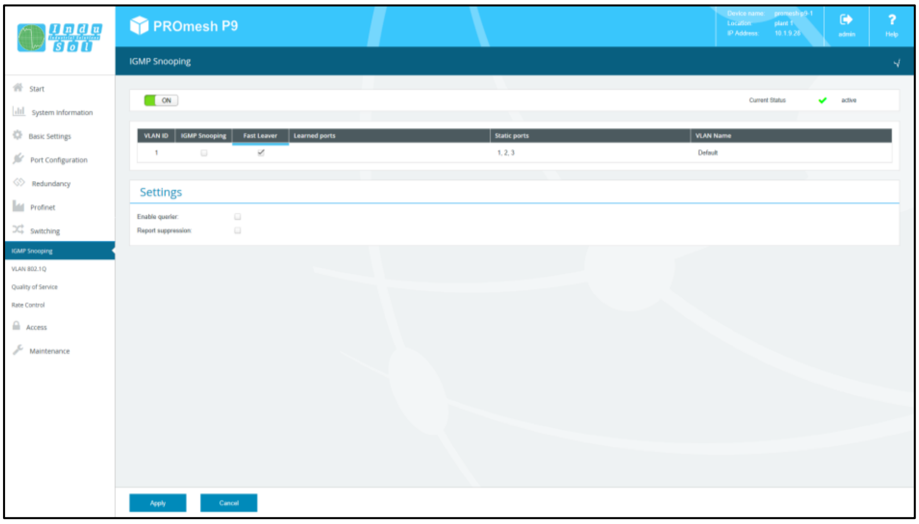
- IGMP Queries: Are queries from IGMP router or switch that require an answer from all hosts of a multicast group.
- IGMP Reports: Are queries from hosts to become member of a report group or messages that they already belong to the group.
- IGMP Leave Group: Is a message from a host that wants to leave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

Settings per stream

- VLAN ID: IGMP snooping operates on VLAN basis and can by activated for the individual VLAN IDs.
- 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.
- Learned Ports: Shows to which ports Multicast receiver are connected to 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. The network limit is reduced by the limitation on necessary reports.



IGMP Snooping

ON

Current Status ✓ active

VLAN ID	IGMP Snooping	Fast Leaver	Learned ports	Static ports	VLAN Name
1	□	☑		1, 2, 3	Default

Settings

Enable querier: □

Report suppression: □

Figure 25: IGMP Snooping

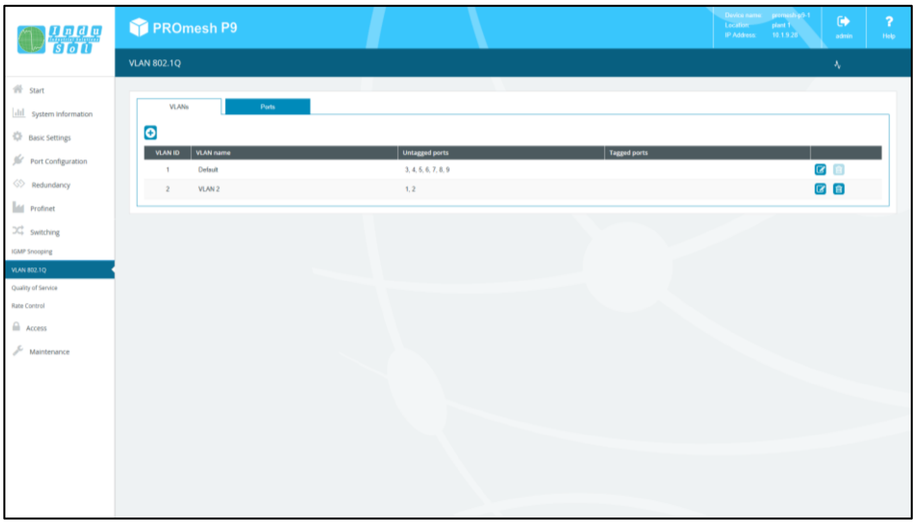
5.10.2 VLAN 802.1Q

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.

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 separate button (except VLAN ID 1 and the current management VLAN).

You can choose between three views. The overview of the VLANs displays the IDs and names of all virtual LANs and shows the tagged and untagged ports based on the port number. The overview of the ports displays the port number and name of a port and lists all VLANs with ID that include port tagged or untagged. In the Management VLAN view, you configure the VLAN ID which is used to access the device (e.g. web interface, PROFINET, etc.).



VLAN ID	VLAN name	Untagged ports	Tagged ports
1	Default	3, 4, 5, 6, 7, 8, 9	
2	VLAN 2	1, 2	

Figure 26: VLAN 802.1Q

Add new VLAN

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

- 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 Name: Enter the name here for the new VLAN. Maximum permitted length of the VLAN name is 50 characters.
- Port: Select how a port should behave in the newly created VLAN.
- 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 is displayed here that you issued in the Port Configuration menu.

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.

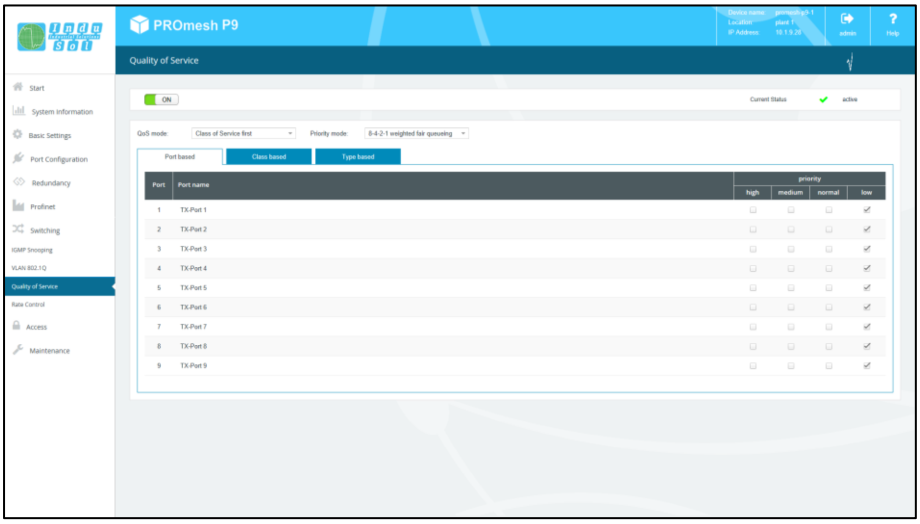
Packages of the default VLAN are output on all ports. The default VLAN should therefore be used only for management packages if at all. Ports without VLAN assignment have to be assigned to a VLAN that is not used so that packages that are received on these ports cannot get into the default VLAN.

Packages with VLAN Tag 1 are received at all ports and output on all ports.

5.10.3 Quality of Service (QoS)

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.



Quality of Service

ON

Current Status ✓ active

QoS mode: Class of Service first

Priority mode: 8-4-2-1 weighted fair queueing

Port based | Class based | Type based

Port	Port name	priority			
		high	medium	normal	low
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	TX-Port 9	□	□	□	☑

Figure 27: Quality of Service

QoS mode and priority scheme

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

- Port based: You can specify a priority for the data transmission for each port. The switch forwards the data packages of the respective port according to their priority.
- Class based (Class of Service - COS): 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 based (Type of Service - TOS): TOS uses the 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.

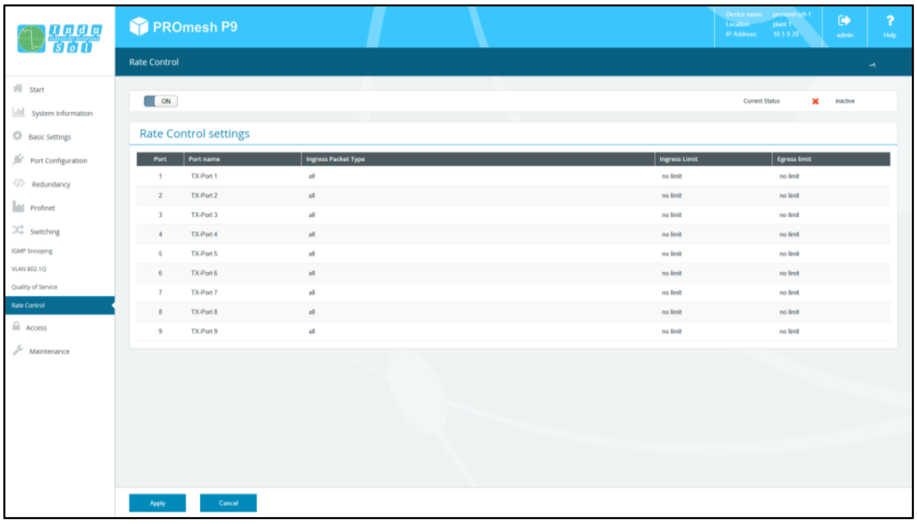
- Select possibilities QoS mode:
  - Only port based: The prioritisation is done exclusively based on the priority of the ports.
  - Only Class of Service: A prioritisation is done exclusively based on the Class of Service data field of the packages.
  - Only Type of Service: A prioritisation is done exclusively based on the Type of Service data field of the packages.
  - Class of Service first: In this variant, the prioritisation is carried out in the sequence of COS, then (if necessary) according to TOS and finally according to port.
  - Type of Service first: In this variant, the prioritisation is decided based on TOS, then (if necessary) according to COS and finally according to port.

- Selection priority mode:
  - 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 package with the lowest queue are never sent. This mode is recommended if there really strong real-time requirements.
  - 8-4-2-1 weighted sequence: This approach prevents that low-priority packages are never sent if high-priority packages are to be permanently sent. Only minor increased latency occurs then for the high-priority packages. The switch sends 8 high-priority packages, then 4 packages with medium, 2 packages with normal and finally 1 package with lowest priority. Afterwards another sending cycle begins with the same scheme.

When using Quality of Service, the flow control ought to be switched off because data packages are transmitted throttled regardless of the priority when the flow control is activated.

5.10.4 Bandwidth control

Bandwidth Control (Figure 28) allows you to throttle various types of package to an adjustable baud rate. You can specify various sending and receipt rates for every port for this (incoming/outgoing package) and apply them to certain package types.



Rate Control

ON — Current Status ✗ inactive

Rate Control settings

Port	Port name	Ingress Packet Type	Ingress Limit	Egress limit
1	TX-Port 1	all	no limit	no limit
2	TX-Port 2	all	no limit	no limit
3	TX-Port 3	all	no limit	no limit
4	TX-Port 4	all	no limit	no limit
5	TX-Port 5	all	no limit	no limit
6	TX-Port 6	all	no limit	no limit
7	TX-Port 7	all	no limit	no limit
8	TX-Port 8	all	no limit	no limit
9	TX-Port 9	all	no limit	no limit

Figure 28: Settings of the Bandwidth Control

The tabular overview provides the following settings:

- Port: Displays the port number that is also marked on the housing.
- Type incoming packages: This setting is exclusively for incoming packages. Select a package type according to which you want to filter.
  - All: All package of all types are limited to the set data amount.
  - Broadcasts: The set limits are valid for all broadcast packages (at all devices in the network).
  - Multicasts: Only Multicast packages (packages at receiver groups) are limited.
  - Unknown Unicasts: Only Unicast packages (to one device) of unknown receivers are limited.
- Limit incoming packages: Select the effective ingress rate of the port. Possible settings are 128 kbps, 256 kbps, 512 kbps, 1 mbps, 2 mbps, 4 mbps and 8 mbps. The standard value is defined as "No limit".
- Limitation of outgoing packages: The baud rates for outgoing package refer to all package types. Select the effective egress rate of the port. Possible settings 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 activate them.

5.11 Access

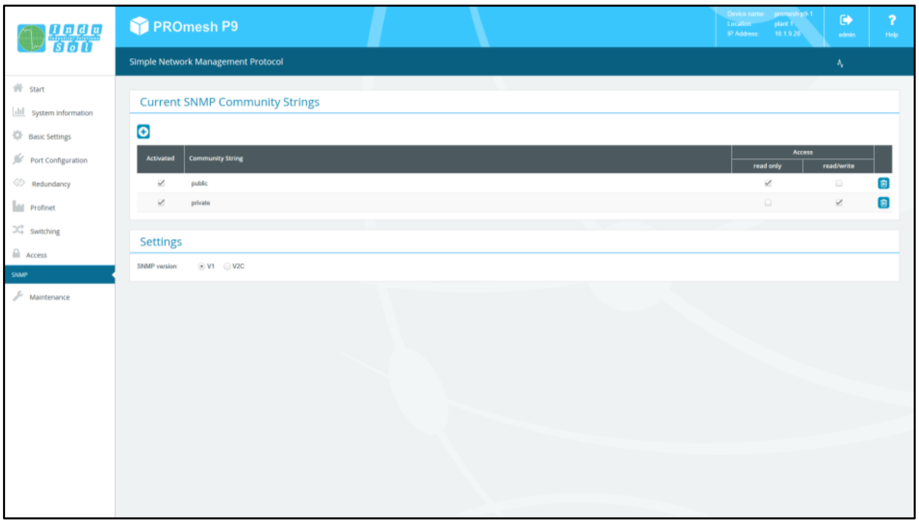
In this point, you can specify the time till the automatic logout. With that you specify how long a session in the web management may run without activity before an automatic logout takes place. You can specify a duration here between 3 and 30 minutes. Standard setting is 10 minutes.

5.11.1 Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) serves to monitor and control network elements by a central station. It permits the reading and writing of system variables.

SNMP queries are sent by the management station with a so-called Community String that presents a simple access restriction. Community strings can be created, edited or deleted in the SNMP menu (Figure 29) of the ***PROmesh P9*** switch. The overview table shows you the currently defined Community Strings and access rights.

- Active: Shows which Community Strings are activated.
- 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.



Simple Network Management Protocol

Current SNMP Community Strings

Activated	Community String	Access		
		read only	read/write	
✓	public	✓	□	🗑
✓	private	□	✓	🗑

Settings

SNMP version: ● V1 ○ V2C

Figure 29: Overview of the currently available SNMP accesses

The ***PROmesh P9*** supports SNMP of the versions V1 and V2C. Please select the desired version. Save the settings by clicking the "Create" button.

5.12 Maintenance

The Maintenance menu item is divided in the points SD card, Backup, Recover, Firmware Update, Default Settings, Restart and Licenses, which are described in the following.

5.12.1 SD card

Select here whether or not the configuration should be loaded directly from a plugged-in SD card when the device is started.

In case you want to rewrite the contents of the SD card, you can also do this by selecting the reformat function.

5.12.2 Backup

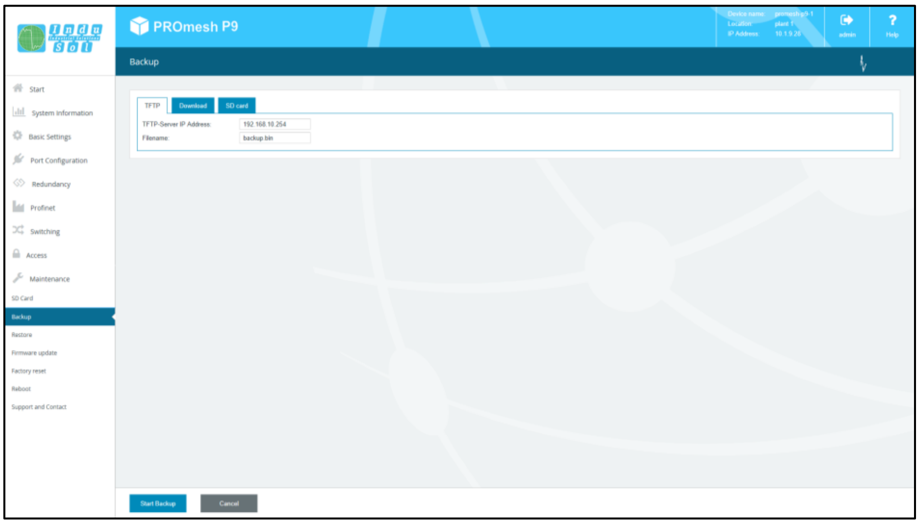
This menu item provides you with the option to backup the current device configuration in a file. The backup can be saved via TFTP, as download or on the SD card (Figure 30).

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

- TFTP: The backup file is saved in a TFTP server accessible in the network. The TFTP server uses the Trivial File Transfer Protocol, a quite simple file transfer system. The input of the IP address of the server and the file name is necessary for that.
- 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: A microSD 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 the SD card.

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.



TFTP-Server IP Address: 192.168.10.254

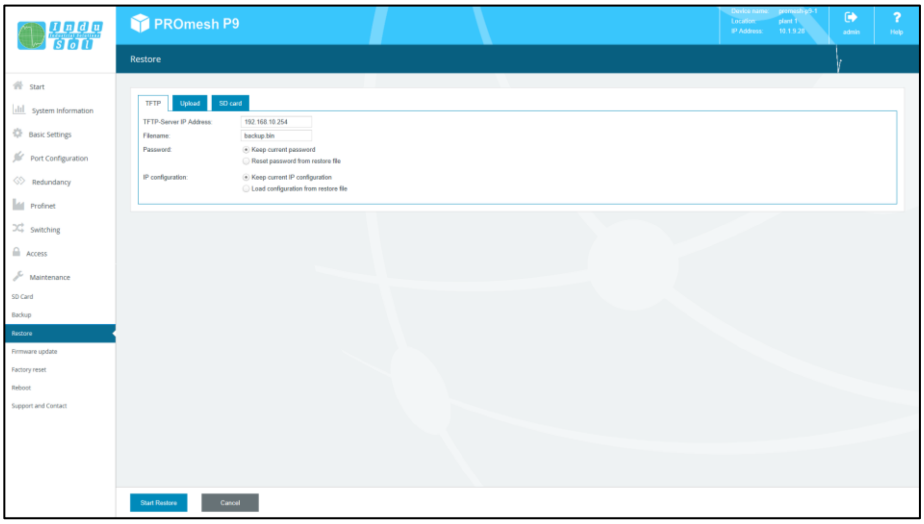
Filename: backup.bin

Figure 30: Backing up the device settings

5.12.3 Restore

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

- TFTP: The backup file is downloaded from a TFTP server existing in the network. It uses the Trivial File Transfer Protocol, a quite simple file transfer system.
- 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 the SD card in the device and is uploaded from there.



TFTP-Server IP Address: 192.168.10.254

Filename: backup.bin

Password: ● Keep current password ○ Reset password from restore file

IP configuration: ● Keep current IP configuration ○ Load configuration from restore file

Figure 31: Settings for recovering a configuration

Settings

- TFTP server IP address: Enter the IP address with decimal points of the TFTP server available in the network.
- File name: Enter the file name here 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 password should be maintained following the recovery or the password should be used that is saved in the backup file.
- IP Configuration: Enter whether the IP address, subnet mask and the gateway should be maintained after the recovery or copied to the specifications of the backup file.

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

5.12.4 Firmware update

The firmware of the ***PROmesh P9*** can be updated in the Firmware Update menu item.

Please use only a firmware version that you have received from Indu-Sol and that was developed specifically for the PROmesh switches.

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.

- TFTP Server: The firmware update is downloaded from a TFTP server existing in the network. It uses the Trivial File Transfer Protocol, a quite simple file transfer system.
- 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.

Preparation:

It is recommended to carry out the update only when the MRP protocol is deactivated. In this case, open the MRP ring first of all by pulling one of the cables and then deactivating the Media Redundancy Protocol. Afterwards, 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 disconnect any network connectors or replug them.

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

5.12.5 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 entered 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.

5.12.6 Restart

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

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

5.12.7 Licenses

On this page, you will find additional information (operating instructions, MIB file, license information, GSDML file) as well as the contact data of the manufacturer (Figure 32).

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.

Operating instructions

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 (e.g. Acrobat Reader from Adobe).

SNMP - Management Information Base

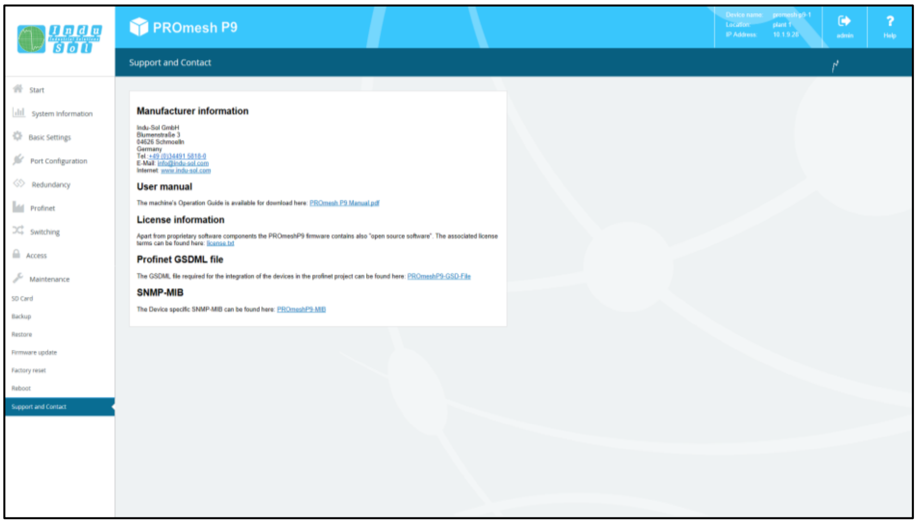
To configure the device via SNMP, the parameters of the switch need to be defined. The description of the parameters is done in a file termed Management Information Base.

License information

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

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.



Device name: promesh-p9-1
Location: plant 1
IP Address: 10.1.9.28

Support and Contact

Manufacturer information

Indu-Sol GmbH
Blumenstraße 3
04626 Schmoelln
Germany
Tel.:+49 (0)34491 5818-0
E-Mail: info@indu-sol.com
Internet: www.indu-sol.com

User manual

The machine's Operation Guide is available for download here: PROmesh P9 Manual.pdf

License information

Apart from proprietary software components the PROmeshP9 firmware contains also "open source software". The associated license terms can be found here: license.txt

Profinet GSDML file

The GSDML file required for the integration of the devices in the profinet project can be found here: PROmeshP9-GSD-File

SNMP-MIB

The Device specific SNMP-MIB can be found here: PROmeshP9-MIB

Figure 32: License information

6 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 P9*** switch back 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.

7 Technical specifications

10/100Base TX ports	RJ45 / Autonegotiation / Auto MDI/MDI-X / supports cables up to a length of 100 m (CAT 5)
Power supply	24V DC +/-20% redundant voltage supply
Power consumption	Maximum 8 W
Potential isolation	500 V
Dimensions (H x W x	105 x 49 x 112 mm
Weight	490 g
Housing	Aluminium, anodised
Storage temperature	-40 °C to +85 °C
Operating	0 °C to +55 °C
Humidity	Humidity 5 to 95 %, RHD non-condensing
Protection class	IP20
Assembly	35 mm DIN top-hat rail
EMC	EN 61000-6-2 / EN 55022 Class A
LED indicators	Status LEDs / Port LEDs (yellow/green) / Voltage supply (green)
IEEE	IEEE 802.3 10Base-T Ethernet / IEEE 802.3u 100Base-TX Fast Ethernet / IEEE802.1d spanning tree / IEEE802.1w rapid spanning tree / IEEE802.1p class of service / IEEE802.1Q VLAN Tag
Protocol	CSMA / CD
Management	SNMP management Web interface management
SNMP MIB	RFC 1213 MIBII / RFC 1493 Bridge MIB / RMON RFC 1757 / RFC 2674 VLAN MIB / RFC 1643 Ethernet as MIB / RFC 1215 Trap MIB Private MIB for Switch Information, Ring, Port Alarm, TFTP Firmware Update,
Technology	Store and Forward Switching Architecture
SNMP Trap	Trap Receiver / Cold start / Port link Up / Port link Down / Authentication fault / Private Trap for Power Status / Port alarm configuration / Fault alarm ring
Transfer Rate	14,880 pps for 10Base-T Ethernet Port 148,800 pps for 100Base-TX Fast Ethernet Port
MAC Address table	2K MAC Address table
Package filter	4 types of package filter rules with various package combinations
Ring	2 ports for the ring to ensure a recovery time of less than 300 ms
VLAN	Port-based VLAN Tagged VLAN IEEE 802.1Q
Class of Service	IEEE802.1p Class of Service with 4 priority queues per port
Spanning Tree	IEEE802.1d Spanning Tree and IEEE802.1w Rapid Spanning Tree
IGMP	IGMP v1 and Query mode with up to 256 groups
SNTP	SNTP for time synchronisation
SMTP	SMTP server and E-mail account for event notifications
Port Mirror	Only TX packages or TX and RX packages
Firmware update	TFTP firmware update, TFTP backup and restoring
Alarm contact	Relay contact 25V DC (1A) / 60V DC (0.3A)
Bandwidth Control	Ingress and egress with combination options
DHCP Client	DHCP Client function to receive an IP address from the DHCP server

Indu-Sol GmbH
Blumenstrasse 3
04626 Schmoelln

Telephone: +49 (0) 34491 5818-0
Telefax: +49 (0) 34491 5818-99

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

We are certified according to DIN EN ISO 9001:2008