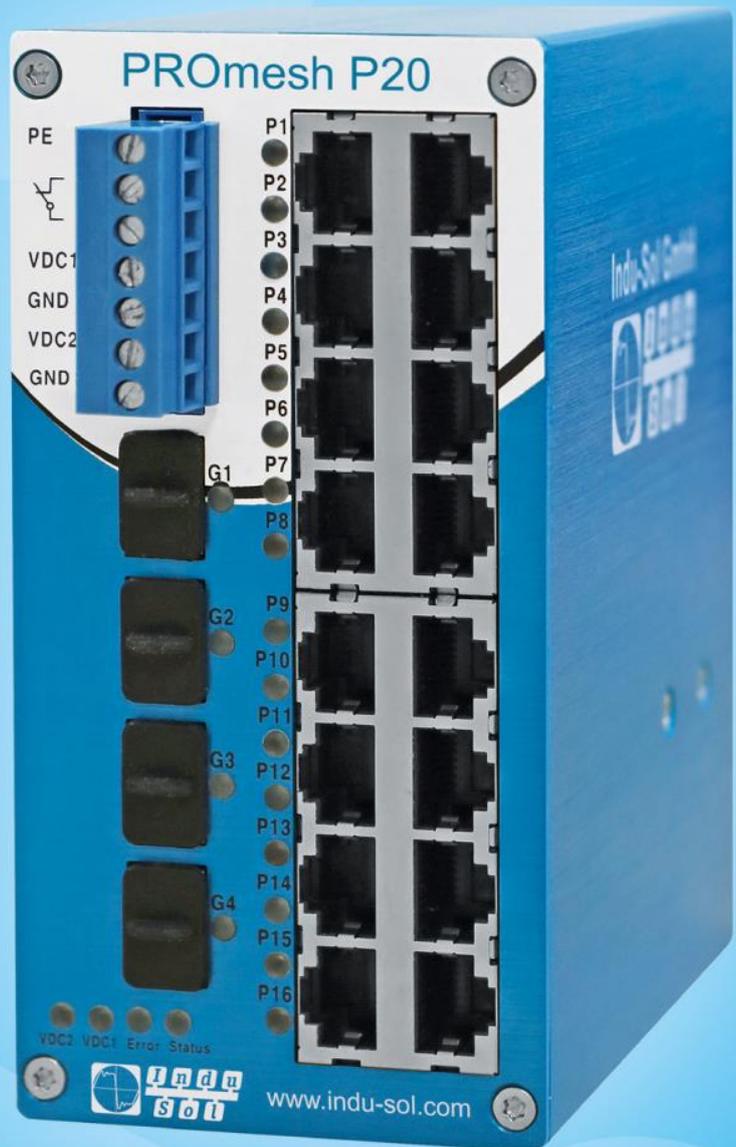


PROmesh P20

Benutzerhandbuch



Diagnose- und Servicetools für PROFINET

Indu-Sol GmbH

Blumenstraße 3

042626 Schmoelln

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

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.– 04:30 p.m. (CET). Or send us an e-mail to: support@indu-sol.com

Your system is at a standstill? 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)
24.01.2019	0	First version
07.05.2019	1	First version
29.05.2019	2	First version
22.06.2020	3	V1.1

© Copyright 2019 Indu-Sol GmbH

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. You can't derive any claims 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 P20** in the network can lead to severe bodily injury as well as property damage due to uncontrolled machine movements.

Contents

Revision overview	3
1 General information	6
1.1 Overview of the <i>PROmesh P20</i> functionality	6
1.2 Scope of delivery	7
1.3 Safety information	7
2 Device ports and status indicators	9
2.1 Device ports	9
2.2 Installation instructions	10
2.3 Voltage supply connection and fault relay	11
2.4 LED indicators	13
2.5 Network integration and commissioning	14
2.5.1 Data ports	14
2.5.2 Media selection and connection	14
2.5.3 Cabling	15
2.6 Network topology and media redundancy	16
2.6.1 Network topology	16
2.7 Ring structure	17
2.7.1 Ring redundancy	18
2.7.1.1 Netload balancing	19
2.7.1.2 NAT routing	19
3 Web application	19
3.1 Preparations	20
3.2 System login	21
3.3 Web interface	21
3.4 Start	22
3.5 System information	23
3.5.1 Basic setting	24
3.5.2 Network settings	24
3.5.3 User settings	27
3.5.4 Log information	28
3.5.5 SSH HTTP setting	29
3.5.6 Diagnostic test	29
3.5.7 Leakage current	30
3.5.8 PROFINET	30
3.6 Port configuration	32

3.6.1	Overview	32
3.6.2	Bandwidth control	33
3.6.3	Port speed limit	33
3.6.4	Port mirroring	34
3.6.5	Alarm settings	35
3.6.6	Link Aggregation	37
3.6.6.1	Static link aggregation	37
3.6.6.2	LACP Configuration	37
3.6.7	Port statistics	38
3.7	Layer 2 configuration	39
3.7.1	VLAN configuration	39
3.7.2	MAC configuration	41
3.7.3	Spanning Tree Protocol	41
3.7.4	IGMP snooping	44
3.7.5	Media Redundancy Protocol (MRP)	45
3.8	Network security	46
3.8.1	Access control	46
3.8.2	E-mail alarm	46
3.9	NAT configuration	47
3.9.1	NAT configuration rules	47
3.9.2	NAT binding	48
3.10	Advanced config	48
3.10.1	Quality of Service (QoS)	48
3.10.2	Link Layer Discovery Protocol (LLDP) – Topology	49
3.10.3	Simple Network Management Protocol (SNMP)	50
3.10.4	DNS setting	51
3.10.5	NTP setting	51
3.11	System maintenance	52
3.11.1	Configuration file management	52
3.11.2	Restart	52
3.11.3	Restore factory settings	52
3.11.4	Online update	52
3.11.5	HTTP update	52
3.11.6	SD card	53
4	Notes on troubleshooting	54
5	Technical specifications	55

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 P20* functionality

The *PROmesh P20* 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 store-and-forward 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
- 12-48 V supply, protected against polarity reversal, redundant operation possible
- Configurable alarms for monitoring all input voltages
- 16x RJ45, 10Base-T, 100Base-TX
- 4x SFP 10/100Base-TX, 1000Base-X
- PHY and MAC completely compatible to IEEE 802.3, IEEE802.3u and IEEE 802.3x
- Auto MDI/MDI-X for 10/100BASE-TX, autonegotiation
- Switch mode: Store and forward
- MAC address table: 16K (16384 addresses)
- PROFINET Conformance Class B
- PROFINET Netload Class III
- Layer 3 NAT routing
- 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 mirroring (Tx / Rx / Rx and Tx packages)
- Port-based VLAN / tagged VLAN IEEE 802.1q
- 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), v1, v2c, v3
- Updating, saving and backing up the system configuration via HTTPs, TFTP and memory card

1.2 Scope of delivery

The scope of delivery comprises the following individual parts:

- **PROmesh P20**
- 7-pin plug-in terminal block, 5.0 mm (power supply + alarm contact)
- Quick-start user guide (hardcopy)
- USB stick with following files: Commissioning and user manual (PDF), quick-start user guide (PDF), ServiceTool (ZIP), Switch explanatory video (MP4)
- Micro SDHC memory card, 8GB

Please check that the contents 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).

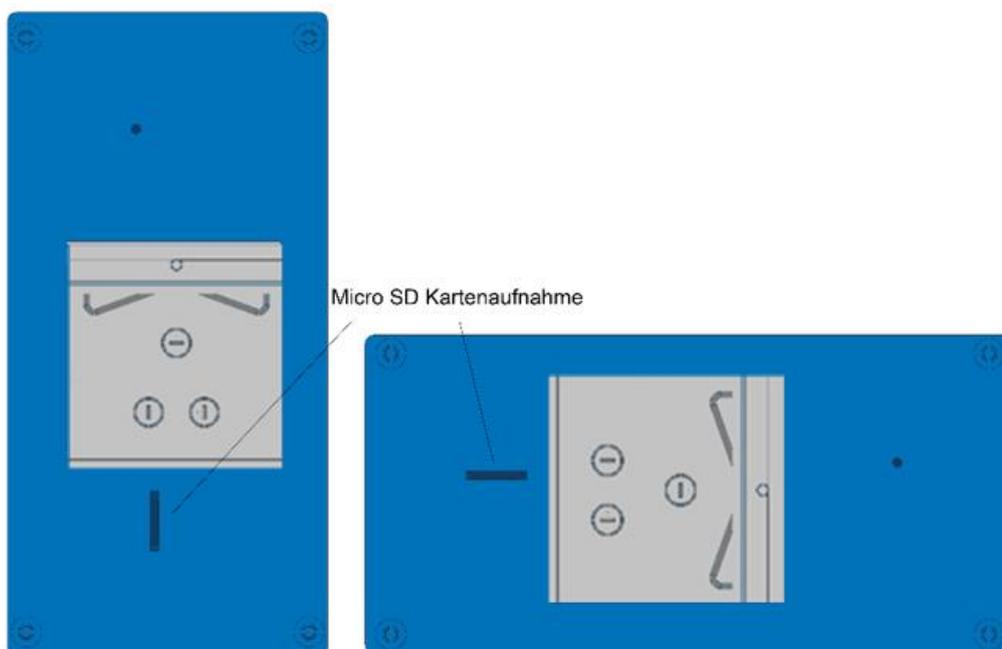


Figure 1: Micro SD card slot at the rear of the PROmesh P20

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 P20 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 P20** 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, layout and wiring of the data port.
-  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

2.1 Device ports

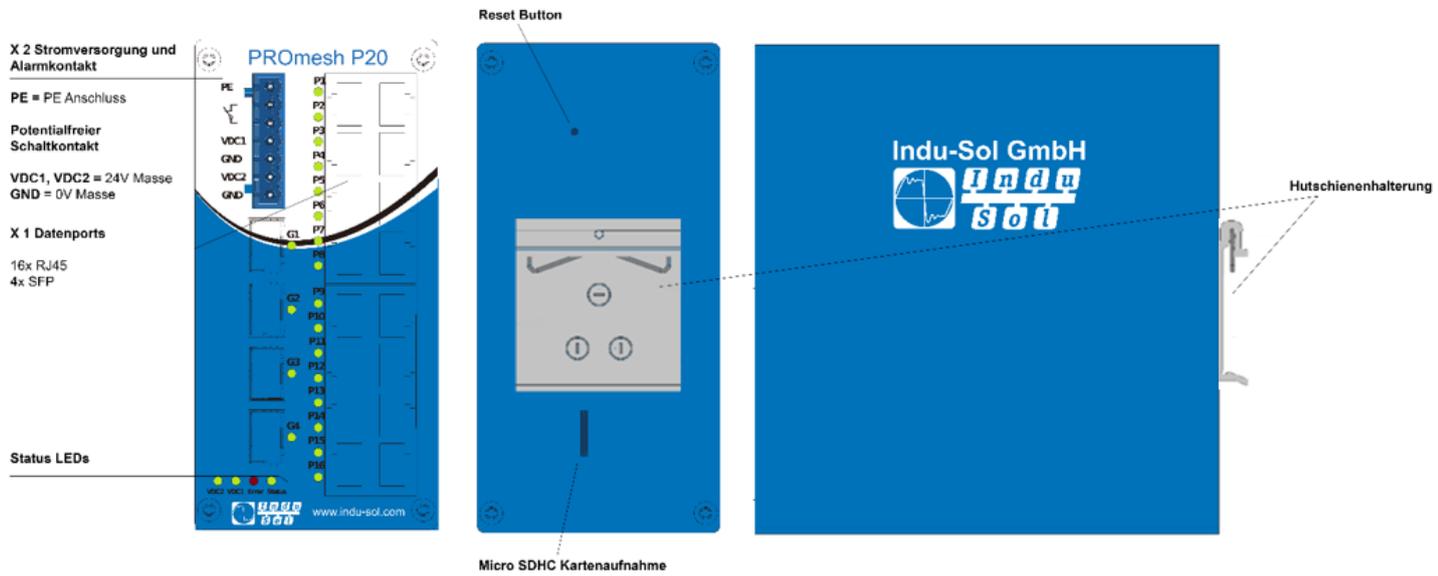


Figure 2: Device ports

Installation

The PROmesh P20 has been designed for individual use in different kinds of control cabinets and can therefore be mounted on a standard 35 mm DIN top-hat rail, in positions with 0°, 90° and 180° rotation.

Use only the provided DIN-rail fasteners to mount the device, or, if necessary, purchase appropriate spare parts to mount the device in your system in such a way that it has adequate electrical contact and can withstand the mechanical stress.

2.2 Installation instructions

The *PROmesh P20* is installed horizontally inside the control cabinet on a 35 mm top-hat rail in accordance with DIN EN 60715.

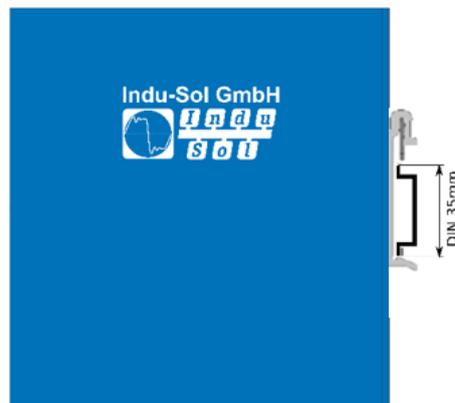


Figure 3: Side view, with connection terminal on the right



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

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

Installation and removal of the device is displayed in Fig. 3.



Figure 4: Installation on and removal from the top-hat rail

- 

Do not mount the **PROmesh P20** switches directly next to devices that emit strong electromagnetic interference fields, such as transformers, contactors, frequency inverters, etc.
- 

Do not mount the **PROmesh P20** 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 P20 against additional heat radiation and observe the approved temperature range for storage and operation.

2.3 Voltage supply connection and fault relay

Operate your **PROmesh P20** with a nominal voltage of DC 12 V to 48 V. To safeguard your system availability, connect the redundant supply circuits 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.

Always make sure that all connections are connected in the correct order, in accordance with the technical specification on page 55.

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

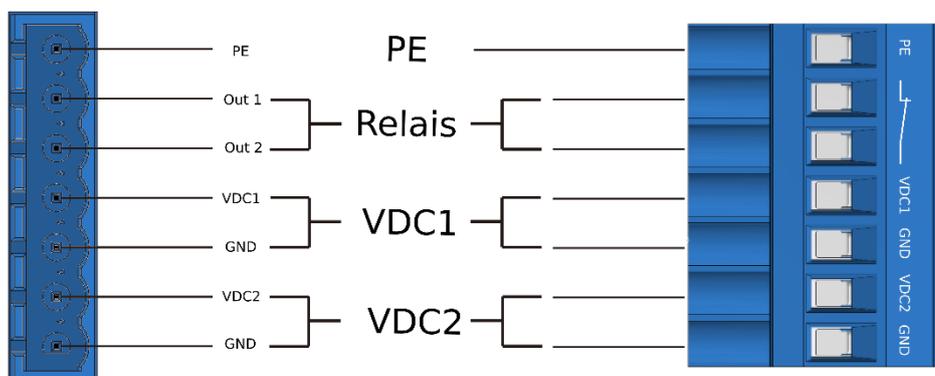


Figure 5: Assignment of 7-pin, 5.0 mm terminal block

Device ports and status indicators

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 an RJ45 port fault.

2.4 LED indicators

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

Additionally, each of the 20 data ports feature two status LEDs.

The status LEDs show the most important diagnostic information regarding the device and connection status of the PROmesh P20 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
Status	Green	PROFINET connection to controller is active
	Yellow	PROFINET connection to controller is inactive
Error	Red	Voltage failure, port fault or configurable alarm active
	Off	No malfunction at port
Data	Green	Connection available
	Flashing	Sending or receiving packages
	Off	No connection available

Table 1: LED functions

2.5 Network integration and commissioning

2.5.1 Data ports

The **PROmesh P20** is equipped with 20 data ports, which enable data transmission in compliance with the PROFINET-IO standard, with up to 100 Mbps in acc. with the 10Base-T and 100Base-Tx (RJ45) standard, as well as up to 1000Base-X (SFP). The actual baud rate is automatically detected and regulated depending on the network device. MDI/MDI-X Autocrossover has to be crossed appropriately, 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 means of the web management.

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

If a suitable SFP transceiver is installed at the SFP slot, the configuration of the transceiver can be monitored and adapted via the Web-Based Management (WBM) of the PROmesh P20.



The PROmesh P20 fully supports all media types and associated functions of the PHY layer and LNK layer, also via the four SFP slots.

Take care to select appropriate SFP transceiver modules and appropriately assigned line layouts when connecting the SFP transceiver modules, to ensure that all functions for your media integration, such as e.g. half-/full-duplex mode, can be used.

2.5.2 Media selection and connection

In addition to the 16 data ports for connecting RJ45 copper lines, the PROmesh P20 is equipped with four 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 P20 into your automation network by using different media types, such as copper lines, single-mode fibreglass lines and multi-mode fibreglass 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 line lengths and cascading of network segments in acc. with your media type (copper, optical fibres, etc.).

2.5.3 Cabling



To connect your PROmesh P20 via the equipped RJ45 data port, use twisted-pair cables, Cat 5 or higher, with a max. line length of up to 100 m. The actual line length has to be limited depending on the project planning and commissioning, as well as the attenuation values measured locally when setting up your network topology. To improve the shield termination, we recommend the RJ45 PROFINET connector of Indu-Sol.

2.6 Network topology and media redundancy

Using the PROFINET application in your automation network makes it possible to flexibly integrate and configure devices in your PLC domain, based on the Ethernet protocol.

This not only enables a higher data data throughput, but also makes it possible to distribute and integrate the network devices among each other along different paths. A network segment in Ethernet-based networks thus spans between each device pair.

Switches such as the **PROmesh P20** thus play a key role in your automation network and should be suitable for use in different network structures, to allow flexible expansion and adaptation of your system structure.

The **PROmesh P20** makes it possible to achieve this expediently and conveniently, as it offers extensive functions for networking and securing the communication of all network devices within the PLC domain.

2.6.1 Network topology

Typical Ethernet star structures (see Figure 5) can be networked with the **PROmesh P20** switches without further configuration. The devices are operable immediately.

In comparison to basic fieldbus systems, the PROFINET application allows MxN connection of all devices, based on an Ethernet network structure, and thus enables direct network communication between two devices. Basic meshing is described as a star structure (see Figure 6) in which each device can exchange information with the other network devices via a central distributor. If the network structure is expanded by meshing several star structures, a media-redundant multi-channel communication can be set up between two devices. This increases the fail safety of the automation system significantly.

Here the switch, as a central element for forwarding this information, plays the key roll in forwarding data to the appropriate receiver unchanged and with as little delay as possible. Additionally, the communication should be restricted to one propagation path, to limit the strain on the line capacity that occurs in the case of multi-path propagation.

The **PROmesh P20** supports you in the task of setting up a slimline, expandable and efficient network structure for your PROFINET domain.

In addition to full integration into the PROFINET domain, the **PROmesh P20** can be subjected to a load of up to Netload Class III (network limit).

Additionally, the **PROmesh P20** supports the use of redundancy functions for intermeshed structures as well.

Depending on the existing intermeshed structure in the PLC domain, different protocol functions have shown to provide varying levels of performance and suitability.

The **PROmesh P20** supports the following redundancy functions for preventing multi-path propagation of the data communication in standard cases and to define an alternative route as fast as possible in the event of an error.

The following protocols are supported by the *PROmesh P20*.

- STP
- RSTP
- MSTP

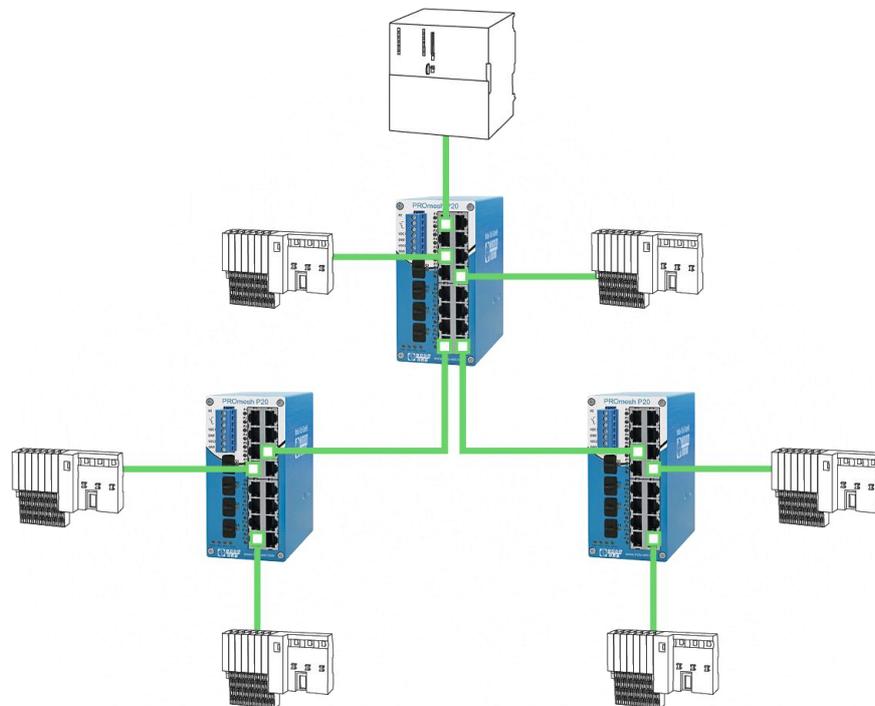


Figure 5: *PROmesh P20* in a star-shaped network

2.7 Ring structure

Ethernet-based networks make it possible to set up ring structures. These are characterized by each device being able to forward data in the form of Ethernet packages to the other network devices along at least two physical paths.

Using this network structure in your PROFINET domain thus makes it possible to establish redundant availability of all network devices if a connection between two devices of the ring structure should be interrupted.

The industrial Ethernet switch plays a key role in the implementation of a redundant network structure, by logically restricting the forwarding of data of all network devices to only one path and switching over to the alternative forwarding path in the event of an error. Thus unambiguous communication, low netload and simple media redundancy are all safeguarded simultaneously. Within the scope of the PROFINET standard, it is recommended to set up ring structures based on the MRP protocol (as per IEC 62439), to identify a secured interruption of ring structures in the PLC domain, as well as the associated switchover, and react to it through technical measures.

The **PROmesh P20** 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, convergence times of max. 200 ms (500 ms) thus becomes possible.

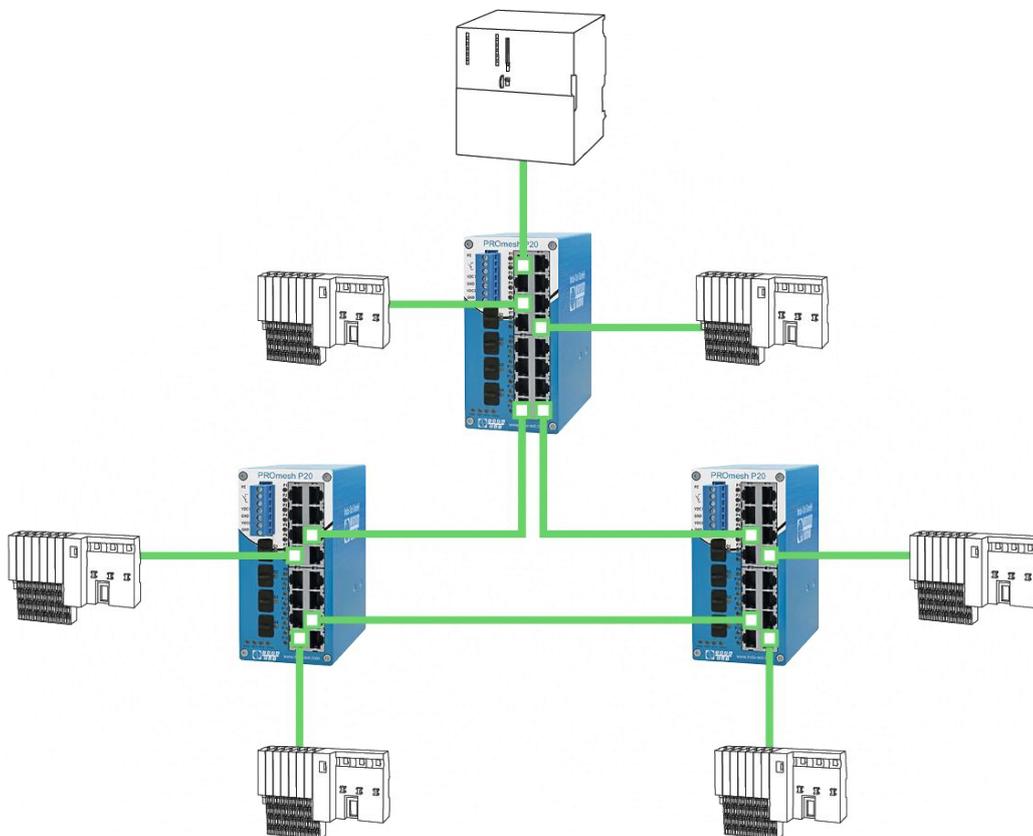


Figure 6: **PROmesh P20** in a ring-shaped network

2.7.1 Ring redundancy

The **PROmesh P20** makes it possible to set up simple ring redundancies, as described in Section 2.7.

The following function protocols are used to set up ring structures.

2.7.1.1 Netload balancing

In the meshed networking of subnetworks, specific connections frequently have high data traffic.

It is particularly noticeable that this data traffic frequently takes the form of load peaks in the communication and thus it is difficult for system operators to calculate it. To ensure fail-safe operation of the automation system, unlimited data forwarding is required even under these conditions.

The **PROmesh P20** supports the application of aggregated network resources, i.e. the logical coupling of several physical connections to a logical connection. With this, an optimal netload distribution is enabled for selected connections with high data traffic and the physical bandwidth of a connection is expanded logically in the event of a high load. To this end, the **PROmesh P20** can be configured using the link aggregation protocol.

2.7.1.2 NAT routing

Industrial networks are characterized by integration of all communication devices within one PLC domain.

As the meshing of these (sub)networks increase, it becomes increasingly necessary to handle monitoring and control tasks that are not within the operational level of the automation system.

The basis for achieving these tasks is that a connection has to be established between different address areas in the Ethernet-based communication. Simultaneously, access to important resources and network resources within the automation task is to be strictly prevented.

Therefore, the **PROmesh P20** has been equipped with complete Layer-3 support, as well as NET routing functionality with basic firewall properties.

Network devices within the LAN automation environment are thus efficiently protected against access of network components that are outside of this environment. Simultaneously, a defined gateway becomes possible through the introduction of NAT rules.

Filtering based on the blacklist procedure therefore only allows connections that have been clearly defined in advance.

To also support this characteristic physically, access to the automation network is limited to network components with connection to Port 20 of the **PROmesh P20**.

For more characteristics and properties for configuring the NAT functions, refer to Section 3.9 of this manual.

3 Web application

The **PROmesh P20** 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 P20** 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. Connect the PC to one of the data ports with a suitable data line (P1-16, G1-G4). The PROmesh P20 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 P20.

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.

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 P20** switch and confirm by pressing the *Enter* button.
3. The login mask of the device then appears on the screen.



Figure 7: Login mask

4. Select the desired menu language (DE / EN).
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 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 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.

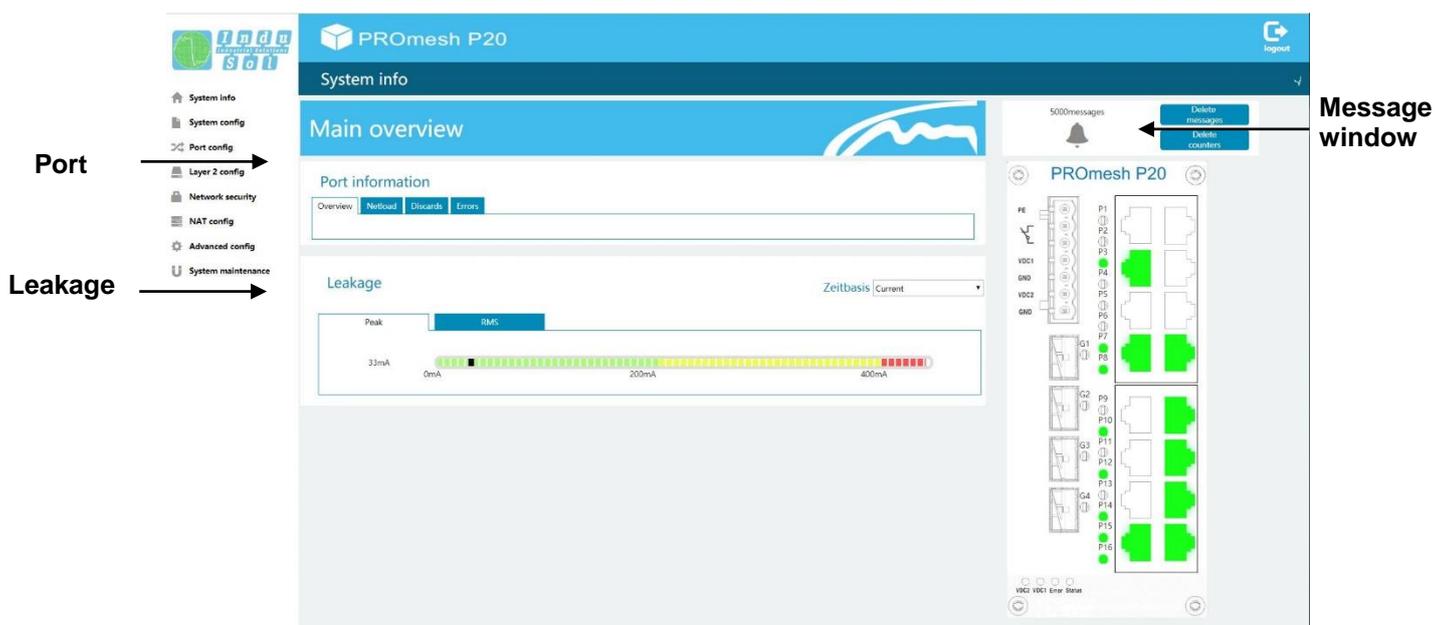


Figure 8: Main overview

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 function to make settings there.

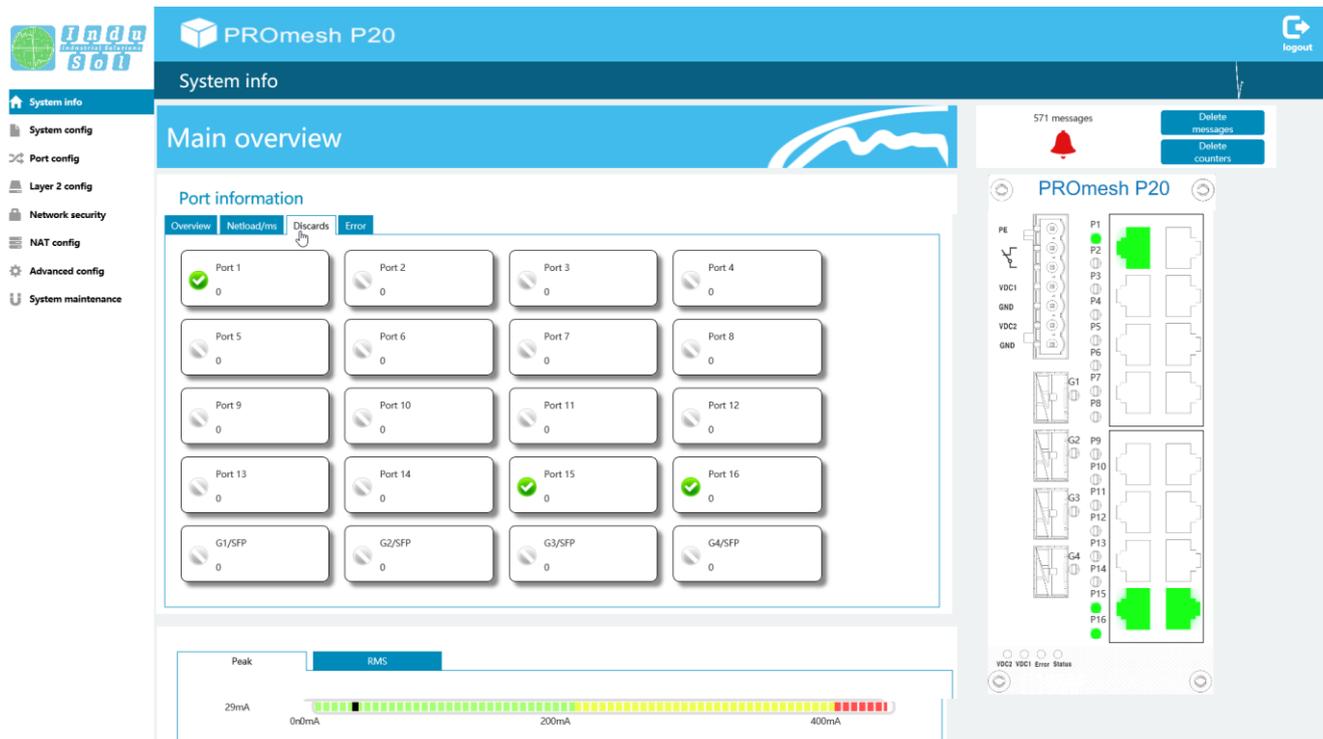


Figure 9: Status and diagnosis

3.5.1 Basic setting

The Basic Settings page allows you to assign the device a unique device name, an installation location and a contact person (see Figure 9).

- 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: Enter a contact person for this device.

The input boxes are configured in such a way 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.

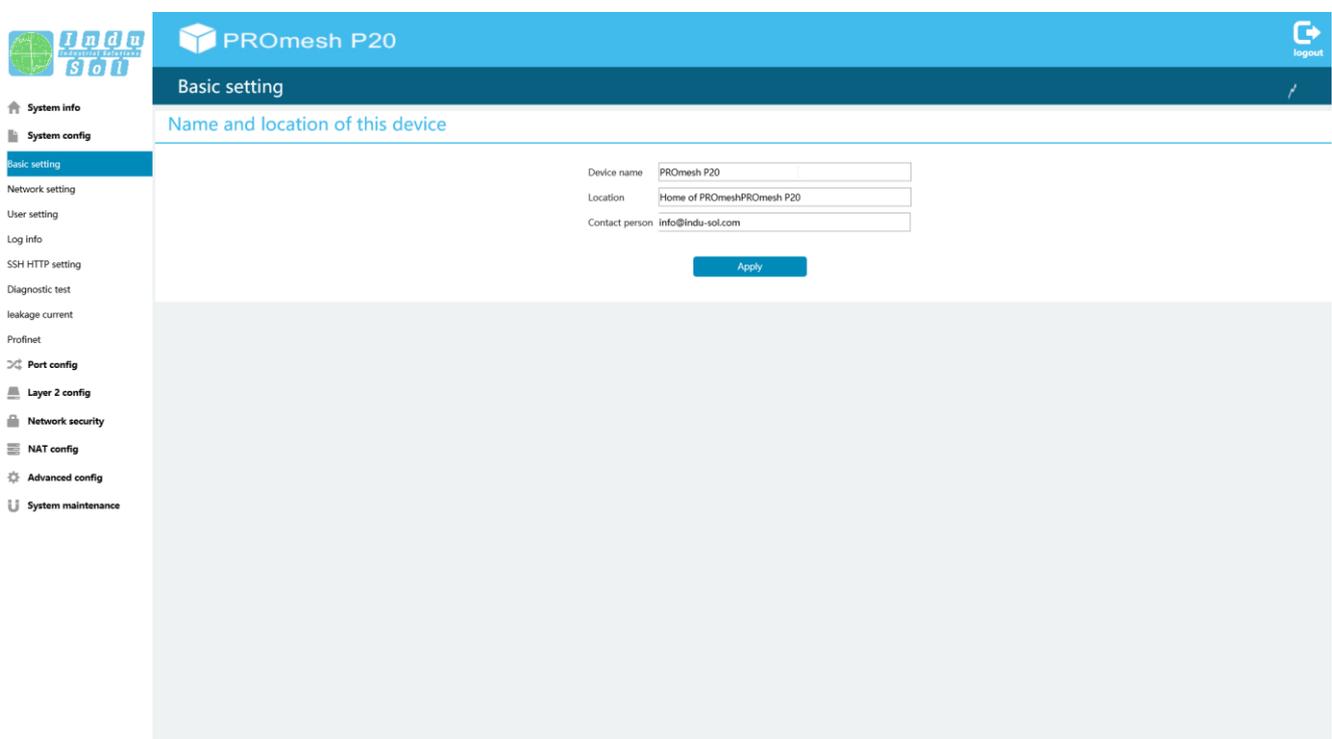


Figure 9: Basic settings of the *PROmesh P20*

3.5.2 Network settings

The IP can be configured (see Figure) 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

Web application

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.

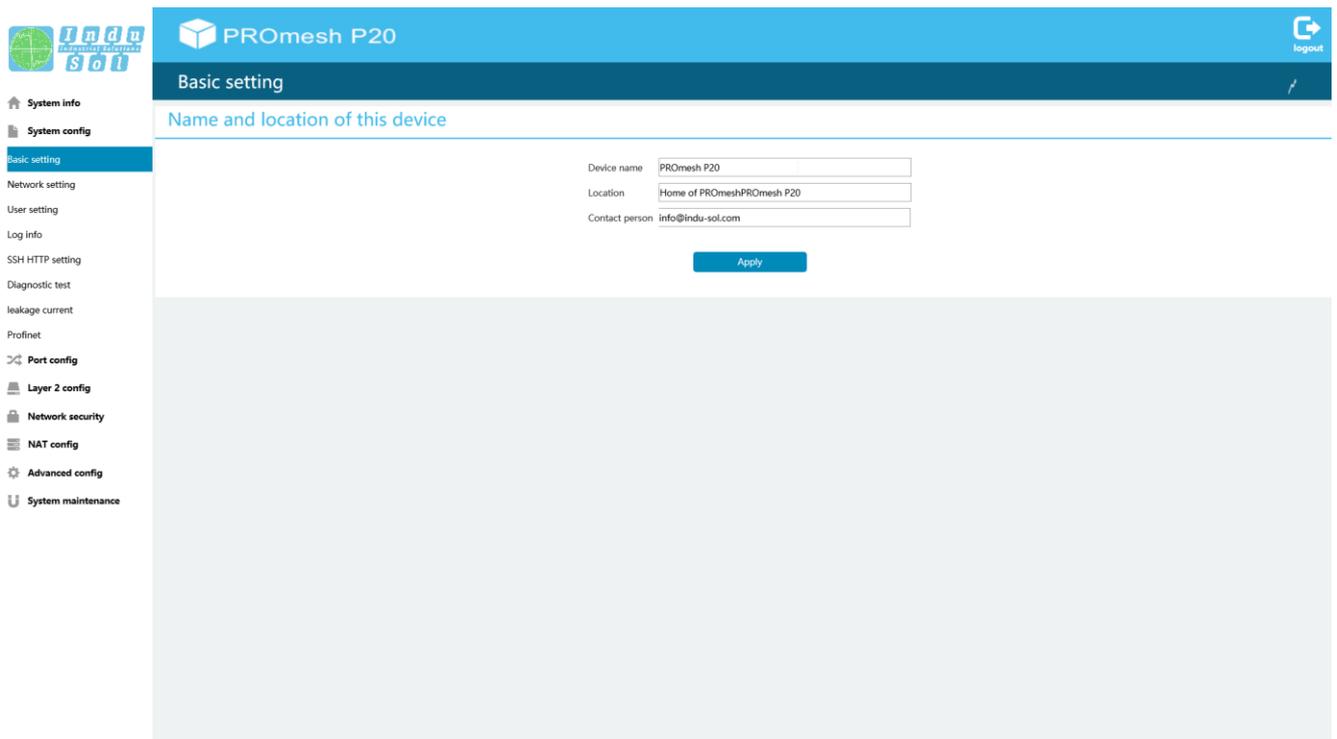
Since the device has now received a new IP address, it can no longer be reached via the standard IP. Please contact your network administrator, if necessary, or use the Indu-Sol ServiceTool to get a new IP address.

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:

- IPv4 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. Next to the IP address, please enter the associated subnet mask. 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. This gateway is used to communicate with devices outside of your subnetwork.



The screenshot shows the web application interface for the PRomesh P20 device. The top navigation bar includes the Indu logo, the device name 'PRomesh P20', and a 'logout' button. The main content area is titled 'Basic setting' and 'Name and location of this device'. It contains three input fields: 'Device name' (pre-filled with 'PRomesh P20'), 'Location' (pre-filled with 'Home of PRomeshPRomesh P20'), and 'Contact person' (pre-filled with 'info@indu-sol.com'). An 'Apply' button is located below these fields. A sidebar on the left lists various configuration categories: System info, System config, Basic setting (highlighted), Network setting, User setting, Log info, SSH HTTP setting, Diagnostic test, leakage current, Profinet, Port config, Layer 2 config, Network security, NAT config, Advanced config, and System maintenance.

Figure 10: IP Configuration

3.5.3 User settings

On the Password page, the preset default password for the *Admin* user can be changed (see Figure). To do this, the user must know the current password and has to enter it to confirm the change.

The following form boxes are available:

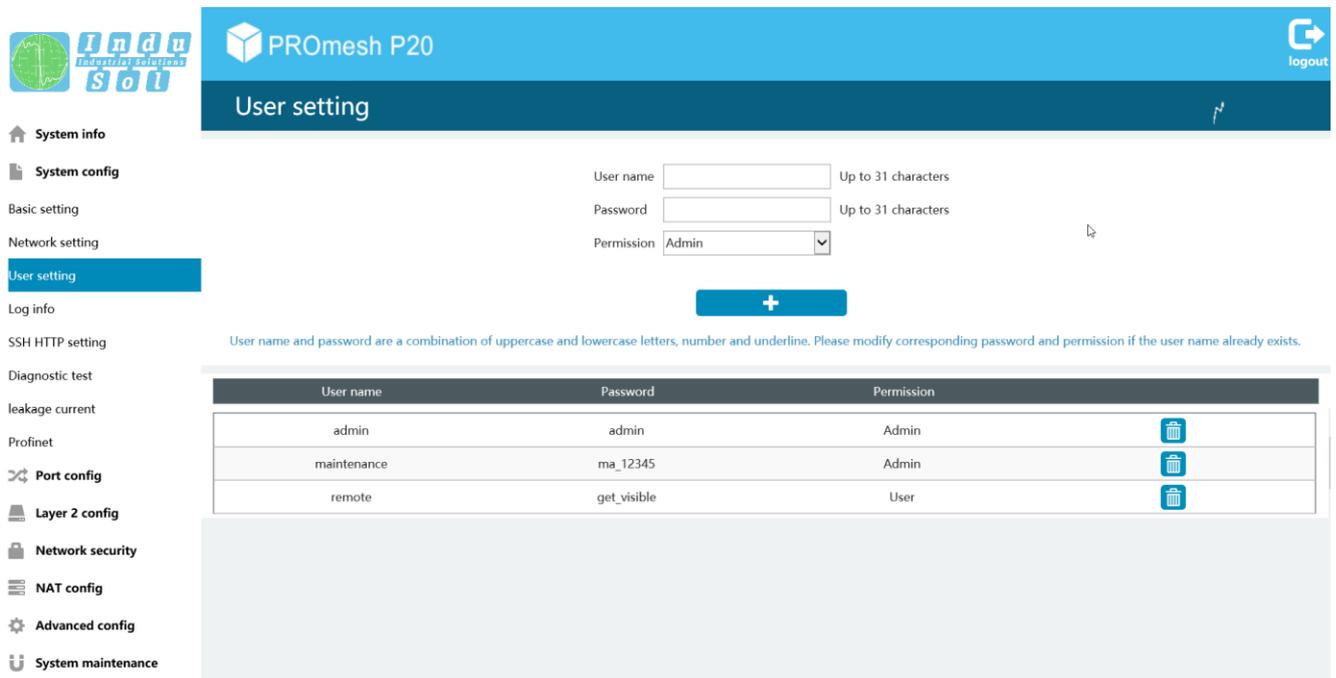
- User name: Enter the name for a new user here. The user name has to be at least 4 characters long.
- Password: Please enter in this box the password specified by you for the previously selected user. Please also observe the instructions in the lower section about assigning passwords.
- Permission: Select an access permission here. You can choose between the *User* and *Admin* profiles. As *Admin*, you have full access to the web interface. For the *User* profile, access to some services are blocked.

Notes on the passwords

The security of your system depends significantly on the security of your passwords. Therefore the following recommendations should be followed when selecting the password:

- Avoid dictionary entries.
- Choose complex character strings.
- Create combinations of letters, numerals and special characters.
- Use uppercase and lowercase letters.

- Password length: At least 8 characters.
- Do not write down passwords.



User name Up to 31 characters

Password Up to 31 characters

Permission

User name and password are a combination of uppercase and lowercase letters, number and underline. Please modify corresponding password and permission if the user name already exists.

User name	Password	Permission	
admin	admin	Admin	<input type="button" value="🗑️"/>
maintenance	ma_12345	Admin	<input type="button" value="🗑️"/>
remote	get_visible	User	<input type="button" value="🗑️"/>

Figure 11: Changing the password for administrator and guest access

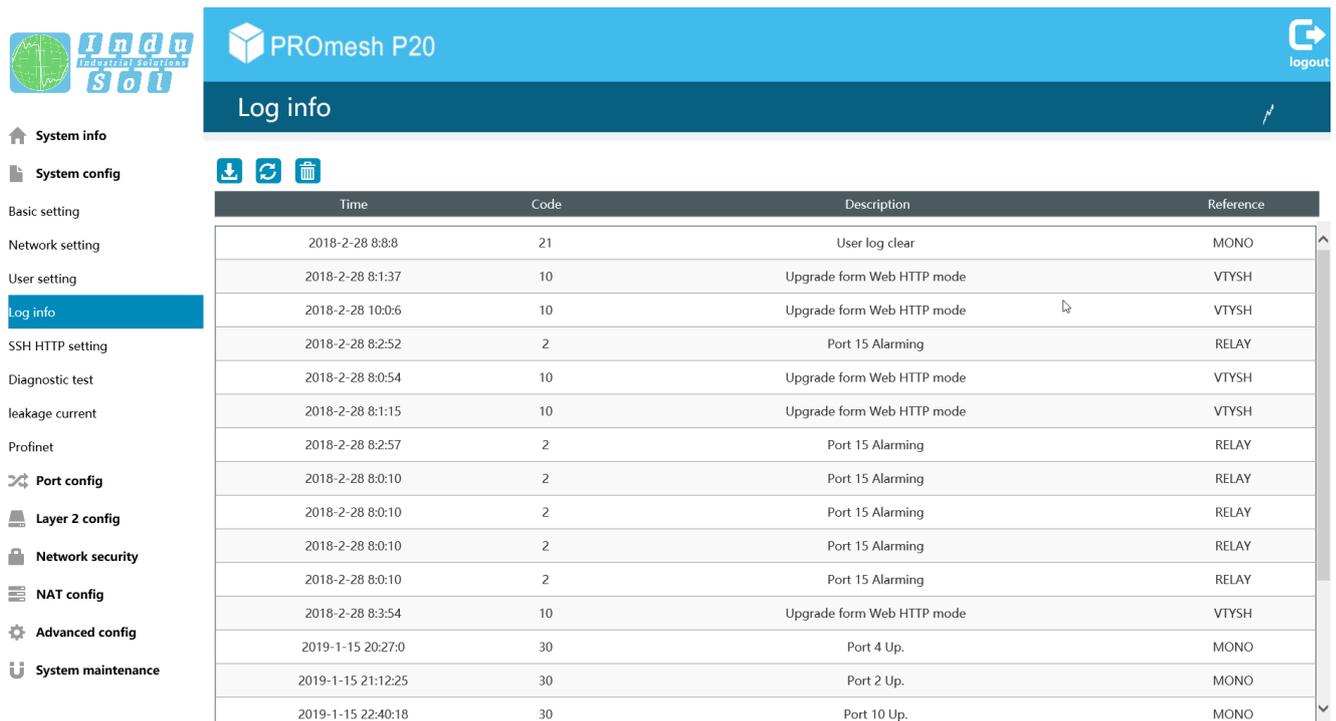
3.5.4 Log information

The log messages (**Fehler! Verweisquelle konnte nicht gefunden werden.**) help the user to receive status and fault messages 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 permanently archive the messages, you can download them onto the computer on which the web interface is running.

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 Download button creates a log file with all entries of the table and saves them in the download directory of the browser. The messages are written line-by-line into a file, with the lines separated by commas.
- The Delete button for the log files removes all entries from the table and shows all messages that occur after this time point. The first log entry that appears after the entries have been deleted shows the timestamp of the deletion.



Time	Code	Description	Reference
2018-2-28 8:8:8	21	User log clear	MONO
2018-2-28 8:1:37	10	Upgrade form Web HTTP mode	VTYSH
2018-2-28 10:0:6	10	Upgrade form Web HTTP mode	VTYSH
2018-2-28 8:2:52	2	Port 15 Alarming	RELAY
2018-2-28 8:0:54	10	Upgrade form Web HTTP mode	VTYSH
2018-2-28 8:1:15	10	Upgrade form Web HTTP mode	VTYSH
2018-2-28 8:2:57	2	Port 15 Alarming	RELAY
2018-2-28 8:0:10	2	Port 15 Alarming	RELAY
2018-2-28 8:0:10	2	Port 15 Alarming	RELAY
2018-2-28 8:0:10	2	Port 15 Alarming	RELAY
2018-2-28 8:0:10	2	Port 15 Alarming	RELAY
2018-2-28 8:3:54	10	Upgrade form Web HTTP mode	VTYSH
2019-1-15 20:27:0	30	Port 4 Up.	MONO
2019-1-15 21:12:25	30	Port 2 Up.	MONO
2019-1-15 22:40:18	30	Port 10 Up.	MONO

Figure 10: Log info

3.5.5 SSH HTTP setting

Secure Shell or SSH provides a simple option for establishing an encrypted connection with another device. In this menu, you can activate or deactivate the service. The Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (**HTTPS**) are communication protocols in the World Wide Web.



Contrary to HTTP, **HTTPS offers advanced security mechanisms**. In this menu, you can activate or deactivate the protocols. The default port for HTTP is port 80. You can change this here, if necessary. Keep in mind that, in the browser bar, the new port has to be entered after the IP address of the switch, with a colon separating them. Thus you can continue to access the web interface (e.g. 192.168.1.254:85). If you want to use HTTPS, write *https://* in front of the IP address of the switch in the browser bar.

3.5.6 Diagnostic test

Ping

In this menu, you can send pings from your switch to other devices in your network. Thus you can make sure that the devices are available and can measure the time delay that occurs when the packages are transmitted. Now enter the *IP address* of the device for which you want to check the connection with the **PRomesh P20**.

Traceroute

In this menu, you can send traceroutes from your switch to other devices in your network. You can use this to check via which devices the communication between the **PROmesh P20** and the end device is transmitted and how much time is needed per node. Enter the *IP address* of the device for which you want to check the connection with the switch.

3.5.7 Leakage current

The leakage current monitoring (Figure 11) makes it possible to permanently record and evaluate the sum of all shield currents of the PROFINET lines 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

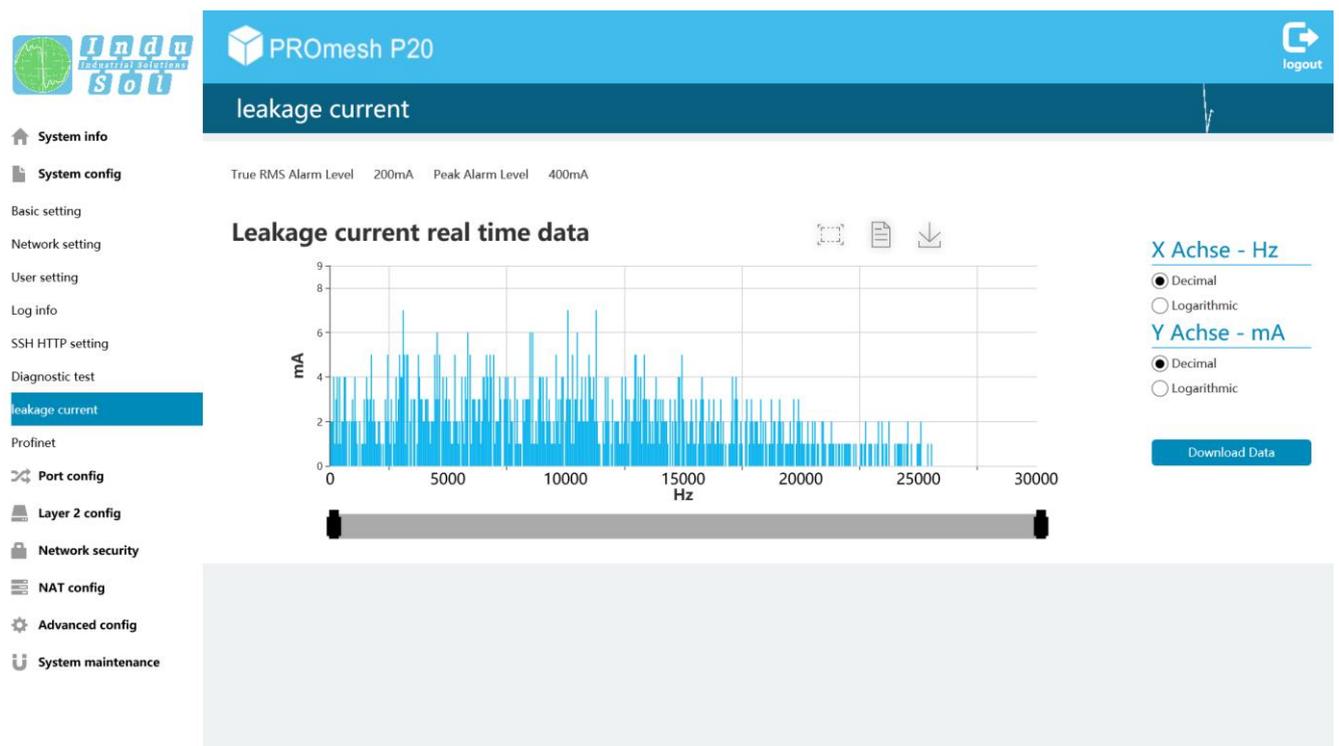


Figure 11: Leakage Current

3.5.8 PROFINET

The abbreviation PROFINET stands for Process Field Network and designates 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 Conformance Class B. You can configure the port settings for DCP on this page and download the configuration file.

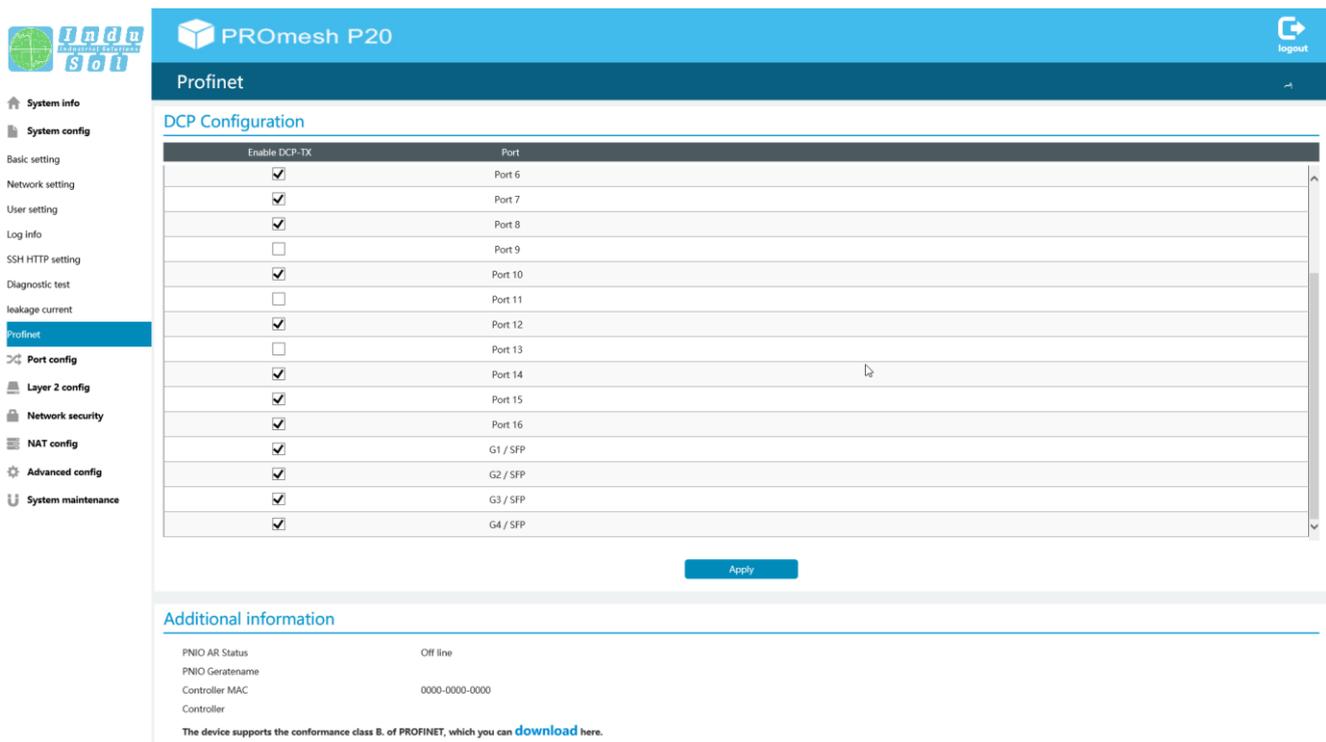
Port settings:

- 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 to the individual devices in a PROFINET IO system.

Configuration file

The configuration file saved on this page describes the 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/>



The screenshot shows the 'Profinet' configuration page in the PROmesh P20 web interface. The 'DCP Configuration' section contains a table with columns for 'Enable DCP-TX' and 'Port'. The 'Enable DCP-TX' column has checkboxes, and the 'Port' column lists ports 6 through 16, plus G1/SFP, G2/SFP, G3/SFP, and G4/SFP. An 'Apply' button is located below the table. Below the table is an 'Additional information' section with fields for PNIO AR Status, PNIO Geratename, Controller MAC, and Controller.

Enable DCP-TX	Port
<input checked="" type="checkbox"/>	Port 6
<input checked="" type="checkbox"/>	Port 7
<input checked="" type="checkbox"/>	Port 8
<input type="checkbox"/>	Port 9
<input checked="" type="checkbox"/>	Port 10
<input type="checkbox"/>	Port 11
<input checked="" type="checkbox"/>	Port 12
<input type="checkbox"/>	Port 13
<input checked="" type="checkbox"/>	Port 14
<input checked="" type="checkbox"/>	Port 15
<input checked="" type="checkbox"/>	Port 16
<input checked="" type="checkbox"/>	G1 / SFP
<input checked="" type="checkbox"/>	G2 / SFP
<input checked="" type="checkbox"/>	G3 / SFP
<input checked="" type="checkbox"/>	G4 / SFP

Additional information

PNIO AR Status	Off line
PNIO Geratename	
Controller MAC	0000-0000-0000
Controller	

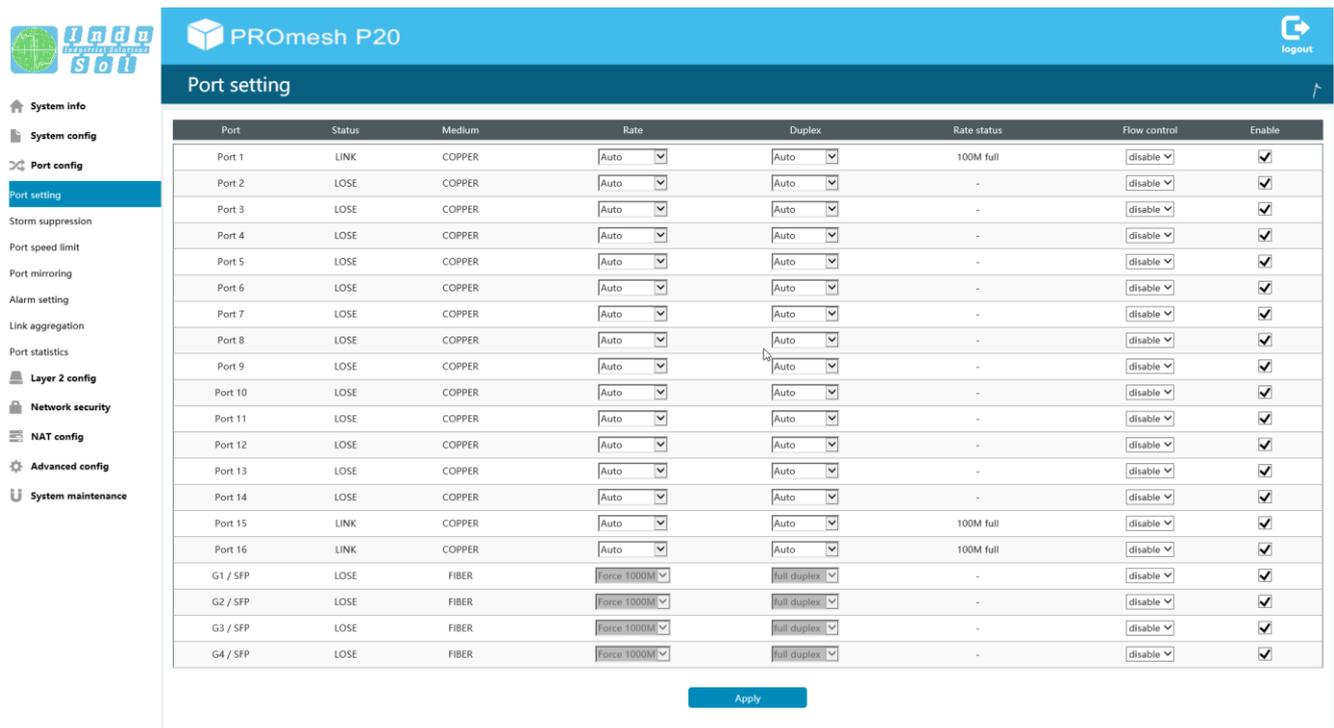
The device supports the conformance class B. of PROFINET, which you can [download here](#).

Figure 14: PROFINET – DCP configuration

3.6 Port configuration

3.6.1 Overview

The table for Port Configuration (Figure) provides an overview of the current settings of the individual ports. Additionally, you can configure the columns Enable, Transmission Rate, Flow Control and Description. Some of the remaining boxes are updated when the port assignment is changed and the website subsequently refreshed, and serve to provide a better overview.



Port	Status	Medium	Rate	Duplex	Rate status	Flow control	Enable
Port 1	LINK	COPPER	Auto	Auto	100M full	disable	<input checked="" type="checkbox"/>
Port 2	LOSE	COPPER	Auto	Auto	-	disable	<input checked="" type="checkbox"/>
Port 3	LOSE	COPPER	Auto	Auto	-	disable	<input checked="" type="checkbox"/>
Port 4	LOSE	COPPER	Auto	Auto	-	disable	<input checked="" type="checkbox"/>
Port 5	LOSE	COPPER	Auto	Auto	-	disable	<input checked="" type="checkbox"/>
Port 6	LOSE	COPPER	Auto	Auto	-	disable	<input checked="" type="checkbox"/>
Port 7	LOSE	COPPER	Auto	Auto	-	disable	<input checked="" type="checkbox"/>
Port 8	LOSE	COPPER	Auto	Auto	-	disable	<input checked="" type="checkbox"/>
Port 9	LOSE	COPPER	Auto	Auto	-	disable	<input checked="" type="checkbox"/>
Port 10	LOSE	COPPER	Auto	Auto	-	disable	<input checked="" type="checkbox"/>
Port 11	LOSE	COPPER	Auto	Auto	-	disable	<input checked="" type="checkbox"/>
Port 12	LOSE	COPPER	Auto	Auto	-	disable	<input checked="" type="checkbox"/>
Port 13	LOSE	COPPER	Auto	Auto	-	disable	<input checked="" type="checkbox"/>
Port 14	LOSE	COPPER	Auto	Auto	-	disable	<input checked="" type="checkbox"/>
Port 15	LINK	COPPER	Auto	Auto	100M full	disable	<input checked="" type="checkbox"/>
Port 16	LINK	COPPER	Auto	Auto	100M full	disable	<input checked="" type="checkbox"/>
G1 / SFP	LOSE	FIBER	Force 1000M	full duplex	-	disable	<input checked="" type="checkbox"/>
G2 / SFP	LOSE	FIBER	Force 1000M	full duplex	-	disable	<input checked="" type="checkbox"/>
G3 / SFP	LOSE	FIBER	Force 1000M	full duplex	-	disable	<input checked="" type="checkbox"/>
G4 / SFP	LOSE	FIBER	Force 1000M	full duplex	-	disable	<input checked="" type="checkbox"/>

Figure 15: Overview: port setting

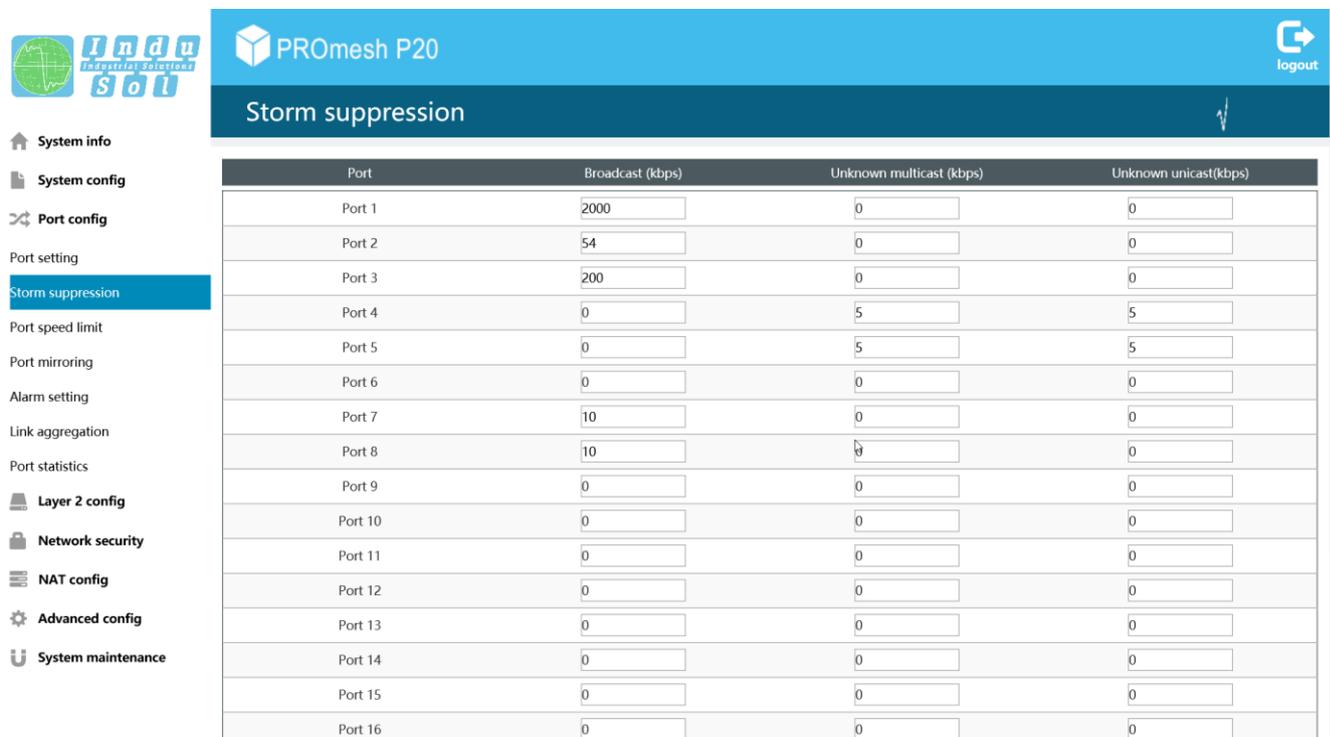
The following columns are displayed:

- **Port:** Displays the port number that is also marked on the housing.
- **Description:** The transmission medium is displayed here (copper or optical fibre).
- **Status:** Status signals the current status of the port:
 - **Link:** The port is activated and a connection has been established.
 - **Lose:** The port is inactive or deactivated.
- **Transmission rate:** The baud rate of the ports can be permanently specified. The options are a baud rate of 10 Mbps or 100 Mbps. The 4 SFP ports (G1 / SFP – G4 / SFP) are permanently set to 1000 Mbps.
- **Duplex:** The duplex mode can be switched between semi- and full-duplex. This setting is thus permanently specified for one connection.
 - **Half duplex:** It is not possible to send and receive at the same time.
 - **Full duplex:** It is possible to send and receive at the same time.

- Current transmission rate: Here you can see the transmission rate that is currently being used by the respective port.
- Enable: The individual ports can be enabled or disabled. With that, you specify whether or not a port can be used.
- Flow control: When an overload occurs at a port, all incoming data packages are rejected. To prevent the resulting loss of data, flow control is used. In the event of an overload, the connected device is signalled to stop sending for a certain period or to limit transmission to a lower bandwidth.

3.6.2 Bandwidth control

Bandwidth Control (Figure 16) allows you to throttle various types of packages to a definable baud rate. If the respective baud rate is exceeded, the excess data packages are rejected. This setting affects only incoming packages.



Port	Broadcast (kbps)	Unknown multicast (kbps)	Unknown unicast(kbps)
Port 1	2000	0	0
Port 2	54	0	0
Port 3	200	0	0
Port 4	0	5	5
Port 5	0	5	5
Port 6	0	0	0
Port 7	10	0	0
Port 8	10	0	0
Port 9	0	0	0
Port 10	0	0	0
Port 11	0	0	0
Port 12	0	0	0
Port 13	0	0	0
Port 14	0	0	0
Port 15	0	0	0
Port 16	0	0	0

Figure 16: Storm suppression

The tabular overview provides the following settings:

- Port: Displays the port number that is also marked on the housing.
- Broadcast: The set limits are valid for all broadcast packages (at all devices in the network).
- Multicast: Only multicast packages (packages at receiver groups) are limited.
- Unknown Unicast: Unicast packages to an unknown receiver are limited.

Once you have carried out the desired settings, click on *Apply* to activate them.

3.6.3 Port speed limit

Here you can define the max. available bandwidth for incoming and outgoing data traffic for each port.

You can configure the following settings:

- **Limit ingress rate:** You can limit the bandwidth for incoming data traffic. The default value is 0 (zero). The bandwidth is not limited.
- **Limit egress rate:** You can limit the bandwidth for outgoing data traffic. The default value is 0 (zero). The bandwidth is not limited.

3.6.4 Port mirroring

Port mirroring (Figure 17) is a method to route the data traffic of a port (source) to a second port (destination) simultaneously and to thus analyse it. 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 diagnostics and error analysis.

- **Status:** Here you can activate or deactivate port mirroring.
- **Source port:** Here you can select which ports should be monitored and duplicate their packages to the destination port.
- **Destination:** Select a destination to which all source port data to be monitored is to be forwarded.
- **Direction:** Please select which package direction you want to mirror. It is possible to mirror only incoming, only outgoing or both incoming and outgoing packages. This setting affects all source ports that are to be mirrored.

Once you have configured 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. Else it is not possible to use the selected destination port.

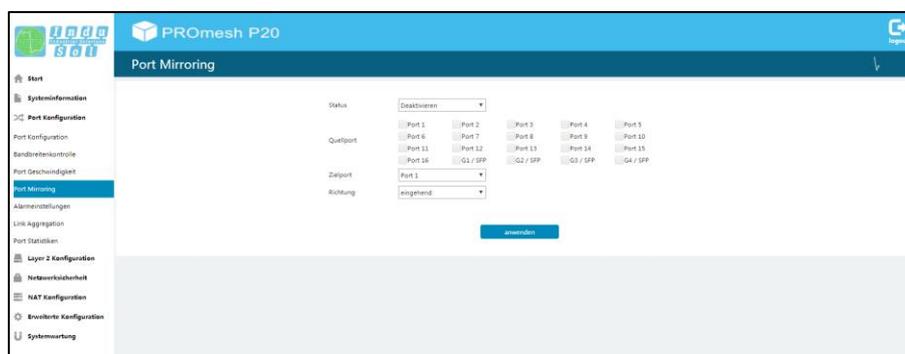


Figure 17: Port mirroring

3.6.5 Alarm settings

The Alarms / Notifications (Figure) menu item is used for the configuration of alarm triggers.

Alarms can be specified for the following events:

- **Status change of a port:** The network ports can trigger an alarm during activity, inactivity and status change.
- **Too high or too low device temperature:** 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.
- **Failure of a supply voltage:** In the Voltage option, the monitoring of the input voltage(s) is defined. Here you can specify which alarm is to be triggered if a voltage supply fails.
- **MRP protocol event:** With an active MRP ring redundancy, alarms can be triggered for detected changes of the ring configuration.
- **Leakage current too high:** If a defined leakage current is exceeded here, an alarm can be triggered.
- **Wrong neighbour:** By activating the point Wrong Neighbour, an alarm is triggered and also the port assignment of the output configuration.
- **Exceeding the network utilisation at a port:** With the option Network Limit, messages can be sent if the configured limit is exceeded.
- **SD card error:** If an error occurs in the SD card, a message is issued.

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

- SNMP Trap (in the SNMP menu, under Alarm, several trap receivers can be defined)
- Relay contact
- E-mail alarm (a receiver can be defined in the E-Mail Alarm menu)

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

Additionally, the alarms mentioned above can be stored in the hardware configuration of the controller. If a trigger is activated, the switch issues an alarm message to the controller. This information can then be processed further by programs in the PLC.

The respective alarm receiver can be defined in separate menus. Receivers for SNMP traps are defined in the SNMP configuration menu (Advanced config → SNMP config). Receivers for e-mails can be defined in the E-Mail Alarm menu (Network security → E-mail alarm)

PROmesh P20
logout

Alarm setting

- System info
- System config
- Port config
- Port setting
- Storm suppression
- Port speed limit
- Port mirroring
- Alarm setting
- Link aggregation
- Port statistics
- Layer 2 config
- Network security
- NAT config
- Advanced config
- System maintenance

Port
Temperature
Voltage
MPP
Leakage
Neighbor
Network load
SD card error
Discard
Errors

Alarm mode Relay SNMP trap E-mail

Port	Enable	Status
Port 1	Disable ▼	Not connected
Port 2	Disable ▼	Not connected
Port 3	Disable ▼	Not connected
Port 4	Disable ▼	Not connected
Port 5	Disable ▼	Not connected
Port 6	Disable ▼	Not connected
Port 7	Disable ▼	Not connected
Port 8	Disable ▼	Not connected
Port 9	Disable ▼	Not connected
Port 10	Disable ▼	Not connected
Port 11	Disable ▼	Not connected
Port 12	Disable ▼	Not connected
Port 13	Disable ▼	Not connected
Port 14	Disable ▼	Not connected
Port 15	Disable ▼	Not connected
Port 16	Disable ▼	Connected
G1 / SFP	Disable ▼	Not connected
G2 / SFP	Disable ▼	Not connected
G3 / SFP	Disable ▼	Not connected
G4 / SFP	Disable ▼	Not connected

Apply

Figure 18: Alarm setting: Adding an alarm trigger

3.6.6 Link Aggregation

The link aggregation function combines several physical LAN interfaces into a logical interface. The resulting increased bandwidth is the sum of the bandwidths of each individual connection. If, for example, two 100 Mbps lines are linked by means of link aggregation, 200 Mbps is now available for the new connection. In addition to the data throughput, the link aggregation also provides redundancy for the created connection and thus increases the fail safety of your network.

3.6.6.1 Static link aggregation

In the Static Link Aggregation menu, you can join several physical ports into one group ID, and thus combine them into one logical port. To do so, you have to configure the following settings:

- **LACP settings:** Here you can assign the same priority to all dynamic trunk lines. Several trunk lines with the same priority are considered to be one trunk line and are used as such.
- **Group ID:** Here you select a group ID under which you want to combine the ports.
- **Port list:** From this list, select the ports that are to be combined into a logical port.



Keep in mind that a port can only be assigned to a group.

3.6.6.2 LACP Configuration

In this menu, you can decide whether LACP should be done dynamically, statically, or not at all. The following settings have to be configured:

- **Type:** Select whether LACP should be done dynamically, statically, or not at all.
- **Group ID:** This setting is relevant if you want to use static link aggregation. To this end, combine ports into a group by entering the same Group ID.
- **Mode:** This setting is relevant for dynamic LACP. In active mode, the LACP protocol is active for the port. In passive mode, the LACP protocol is only active for the port if the counterpart of the port connection is also in active mode. The protocol is sent to bridge a connection failure without losing packages.
- **Port priority:** This setting is relevant for dynamic LACP. If another port is required for a logical connection, the vacant dynamic port with the highest port priority is selected. The lower the number, the higher the priority.



In the case of dynamic link aggregation, at least one side of the connection has to be configured as active part.

3.6.7 Port statistics

The Port Statistics (Figure 19) 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 bytes
- Sent bytes
- Receive filtering

The Receive Filtering column provides information on the number of received data packages that are faulty.

Updating and resetting the values

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

Detailed port statistics

In the graphical display for the port load, the current incoming or outgoing netload, as well as the minimum, average and maximum values for the selected port are displayed. In particular for the low update rates of industrial Ethernet protocols, this netload is calculated on the millisecond level.

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 more than 1023 Byte.)

Amongst the sent packages, a difference is made between:

- Number of all packages
- Sent bytes
- Number of multicast packages
- Number of broadcast packages
- Number of Unicast packages (packages to one receiver)
- Sent pause messages

Amongst the received packages, a differentiation is made between:

- Number of all packages
- Total number of bytes
- Number of multicast packages
- Number of broadcast packages
- Number of unicast packages
- Received pause messages

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

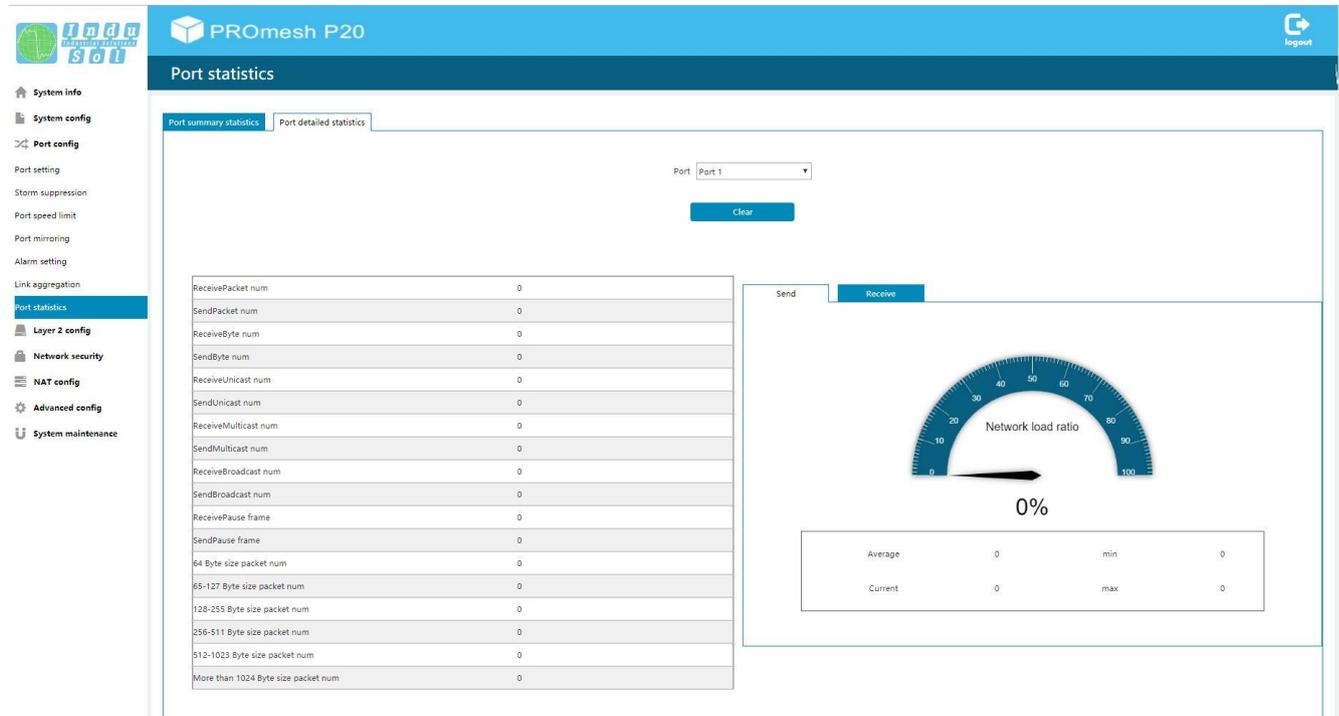


Figure 19: Detailed port statistics

3.7 Layer 2 configuration

3.7.1 VLAN configuration

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.

The VLAN configuration is divided into 3 menus:

- VLAN configuration
- PVLAN configuration
- Trunk configuration

VLAN configuration

In this menu, you can create new VLANs. To do so, you only have to enter a VLAN ID. A value from 1 – 4094 can be entered. Optionally, you can also add a description for the VLAN.

PVLAN configuration

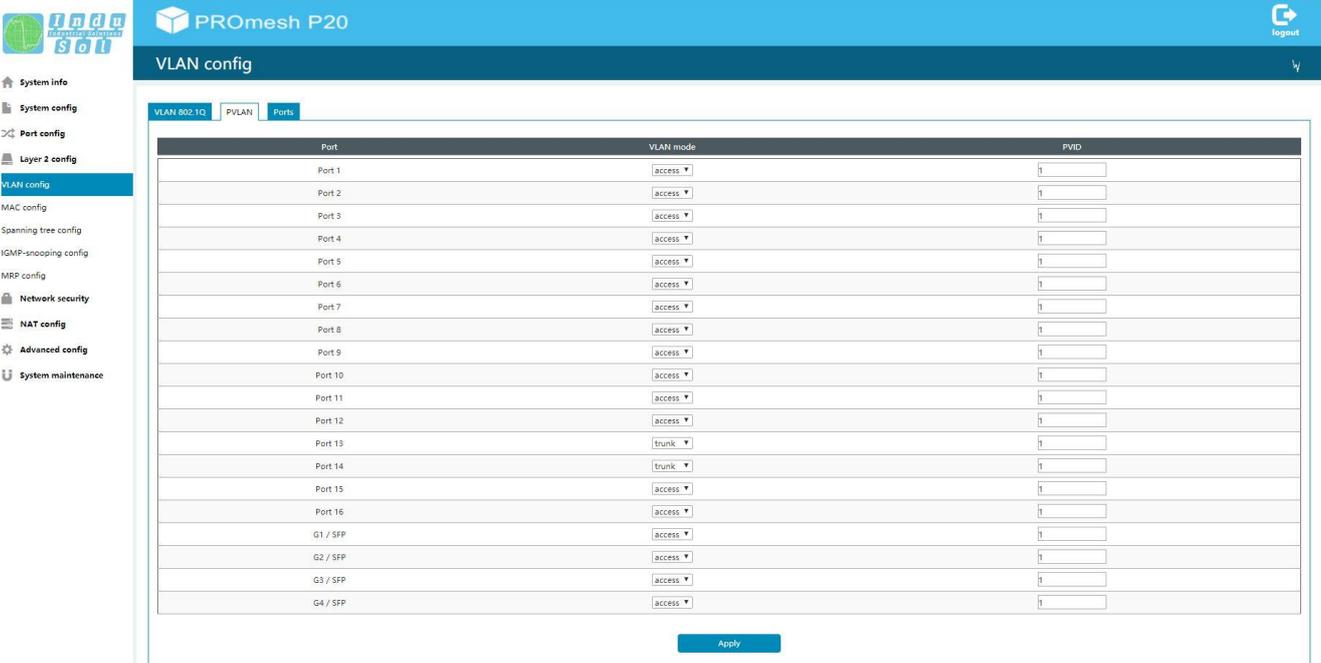
In this menu, you can configure two settings:

- **VLAN Mode:** Here you can select between the Trunk and Access modes. The Access mode should be selected for connections to end devices. For connections that expand the VLAN beyond the individual **PROmesh P20** (for example a connection to another switch), the Trunk mode has to be selected.
- **PVID:** Here you can enter the desired VLAN for each port. Connected devices can only communicate with each other if the ports to which the devices are connected have been configured for the same VLAN.

Trunk configuration

In this menu, you can configure the settings in detail for ports that are in Trunk mode. Ports that are in Trunk mode can be tagged or untagged ports. Untagged ports can only transport the packages of one VLAN per port. If packages of different VLANs are transported via a port, the two ports involved in the connection have to be in tagged mode.

If you configure a port as tagged or untagged and assign it to a VLAN, the port automatically switches from Access mode to Tagged mode.



VLAN config

VLAN 802-1Q PVLAN Parts

Port	VLAN mode	PVID
Port 1	access	1
Port 2	access	1
Port 3	access	1
Port 4	access	1
Port 5	access	1
Port 6	access	1
Port 7	access	1
Port 8	access	1
Port 9	access	1
Port 10	access	1
Port 11	access	1
Port 12	access	1
Port 13	trunk	1
Port 14	trunk	1
Port 15	access	1
Port 16	access	1
G1 / SFP	access	1
G2 / SFP	access	1
G3 / SFP	access	1
G4 / SFP	access	1

Apply

Figure 20: VLAN configuration

3.7.2 MAC configuration

In this menu, you can get an overview of the MAC addresses of all devices that have data traffic flowing via the switch. The MAC address aging time is the time interval for which a device must have communicated with the **PRomesh P20** to stay in the MAC table. Else the device is deleted from the MAC table. You can freely choose a period between 10s-1000000s. The default setting is 300 seconds.

Static MAC

In this menu, you can manually define MAC addresses for individual ports. The device connected to the port is given this MAC address. Additionally, the device is assigned to a VLAN.

3.7.3 Spanning Tree Protocol

The Spanning Tree Protocol (STP) 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 STP function 'global' before configuring the corresponding parameters.

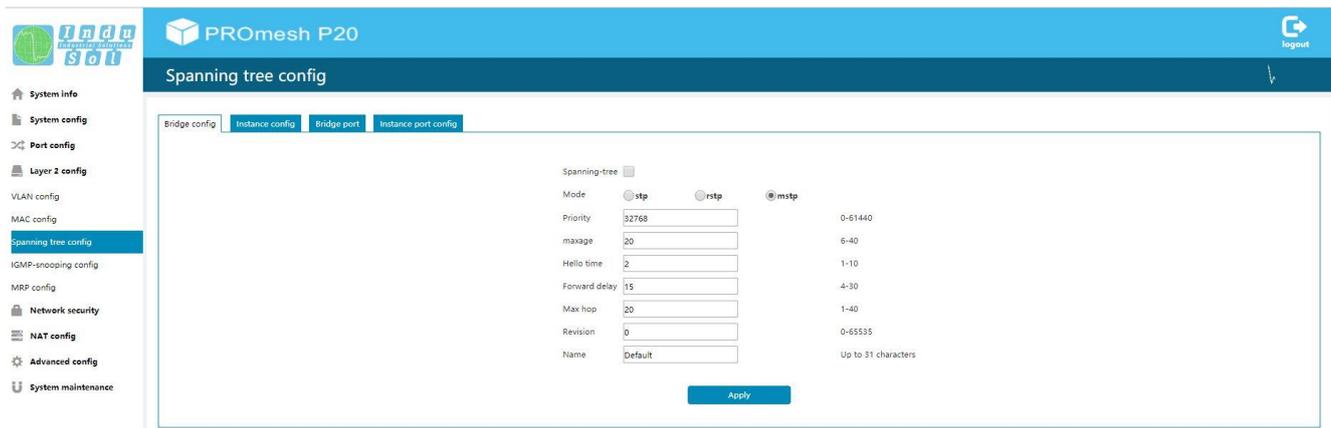


Figure 21: Spanning Tree Protocol (STP)

Bridge configuration

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.
- **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.
- **Max hop:** Here you can limit the number of hops. After the specified number has been reached, the BPDU package is rejected.
- **Revision & Name:** These values are important for MSTP. Switches that use the same values belong to a single MST region.



Use the rule mentioned below to configure Forward Delay, Maximum Age and Hello Time:
 $2 * (\text{ForwardDelayTime} - 1) \geq \text{MaxAge} \geq 2 * (\text{HelloTime} + 1)$

Recommended procedure for setting the parameter: First select a value for the *Hello Time*. Subsequently calculate the lower limit of the Maximum Age with the formula $2 * (\text{Hello Time} + 1)$. Now select a value for the *Forward Delay Time*. From this, calculate the upper limit for the Maximum Age with the formula $2 * (\text{Forward Delay Time} - 1)$. Subsequently, set the Maximum Age to a value that lies between the lower and upper limits calculated earlier. Keep in mind that the value additionally must lie between 6 and 40 seconds. If this is not the case, use new values for *Hello Time* and *Forward Delay Time* to determine the Maximum Age with upper and lower limit.

After suitable values have been created, click Apply to save the changes. The Root bridge information is now displayed in the upper area of the page.

Instance Configuration

In this menu, you can create Multiple Spanning Tree instances. In principle, you could create a separate spanning tree for each VLAN. The following settings are required for this:

- **MSTI ID:** Select the "Multiple Spanning Tree Instance ID here. This ID has to be identical for all switches that belong to the same spanning tree.
- **Bridge Priority:** Each device participating in an MSTI can be assigned a priority. The values can be assigned in steps of 4096 (starting with 4096). The lower the value, the higher the assigned priority. The device that has the lowest priority is declared to be the spanning tree master.
- **VLAN Mapped:** Here you can determine a VLAN or a VLAN group for which the spanning tree is created.

Bridge port configuration

In this menu, you can configure the following settings:

- **Enable:** Enable the settings configured in this menu.
- **BPDU Guard:** The BPDU Guard is a security mechanism of STP and should be used activated on all Access ports. If these ports receive a BPDU, they are deactivated. Thus network interference by manipulated BPDUs can be avoided.
- **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. By specifying edge ports, you can accelerate the convergence time of the redundancy protocol.
 - Forcetrue: The port is configured as edge port by default.
 - Forcefalse: The port is not configured as edge port by default.
 - Auto: The detection as edge port is done automatically.
- **Point-to-Point:** Ports that are connected to at least one additional bridge are called point-to-point ports. The configuration can be done automatically or manually.

Instance port configuration

In this menu you can select the instances specified in the Instance Configuration menu. The overview provides the following information:

- **Enable:** Here you can see whether the instance has been enabled.
- **Instance:** Here you can see the specified priority from the *Instance Configuration* menu.
- **Priority:** You can assign higher priorities to certain ports to influence the design of the tree structure. Enter a number between 0 and 240. The value has to be a multiple of 16.

- **Cost configuration:** Here you can define 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.
- **Cost:** The configured costs can be viewed here.
- **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.
- **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

3.7.4 IGMP snooping

The Internet Group Management Protocol (IGMP) is a protocol of the Internet protocol family. When the IGMP Snooping function (**Fehler! Verweisquelle konnte nicht gefunden werden.**) is active, the switch listens to the multicast traffic in the network. Thus it need not output incoming multicasts to all ports, but can instead send them only to the ports for which the respective multicast is relevant. Additionally, at one of its ports, the **PROmesh P20** can output all the information it gained through IGMP snooping. This can e.g. be applied when a new switch is installed in the network.

The Host Aging Time determines how long collected information is stored in the switch. This time is reset when the respective device answers an IGMP query again.

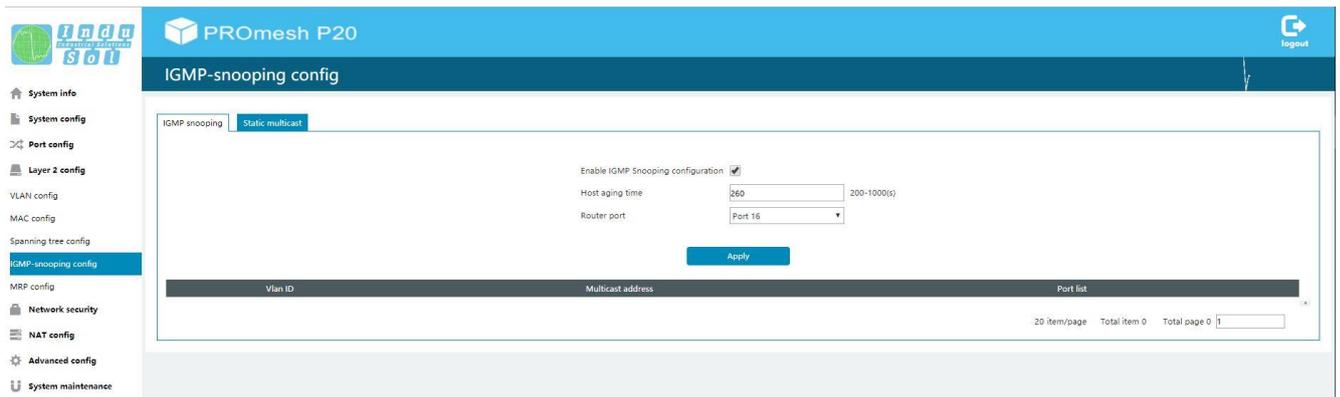


Figure 22: IGMP Snooping

Static multicast

In this menu, you can manually order forwarding of multicast packages. To do so, the following settings have to be configured:

- VLAN ID: Enter the VLAN ID to which the multicast is to be forwarded.
- Multicast Address: Enter a multicast address. Packages that are sent to this address are forwarded via the selected ports.
- Port List: Multicast packages are forwarded via ports selected here.

3.7.5 Media Redundancy Protocol (MRP)

The Media Redundancy Protocol (Figure 23) 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 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.



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

Ring configuration

The following settings are necessary when using MRP:

- Operating mode: Specify whether the *PRomesh P20* should act as manager or as client. Please keep in mind that only one manager may be used per ring.

- 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.
- Convergence time: Enter the time within which convergence for the ring has to be completed.

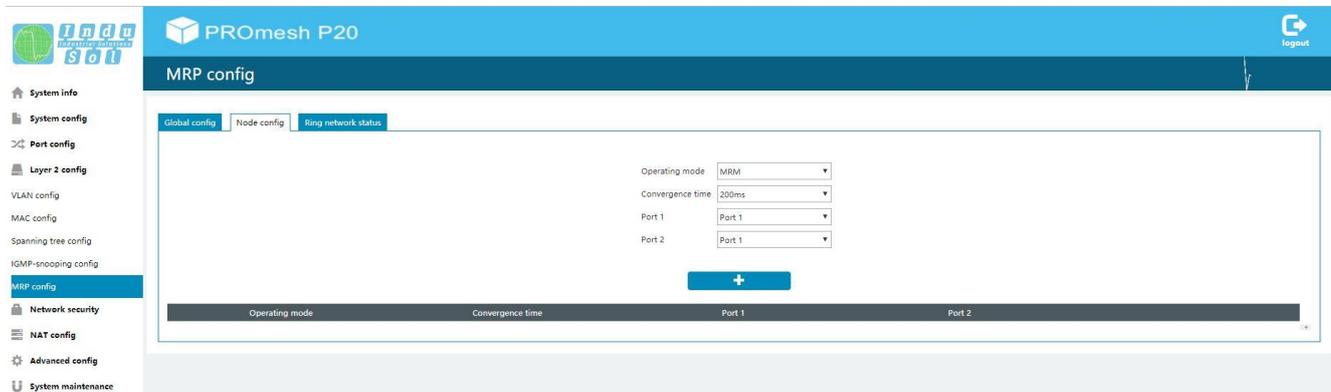


Figure 23: Media Redundancy Protocol (MRP)

Ring Status

Here the current ring status is displayed. Thus you can check whether both connections are intact, or whether the backup connection already has to be used.

3.8 Network security

3.8.1 Access control

In this menu, you can limit the access to the web interface. You can use either the blacklist or whitelist principle. When the blacklist principle is used, all devices are granted access. Simultaneously, access is prohibited for the devices on the list. When the whitelist principle is used, access is prohibited for all devices. However, devices that are on the list are granted access.

In this menu you can also determine the period of time after which an automatic logout from the web interface should be performed after no entries are detected from the user any more.

3.8.2 E-mail alarm

The PROmesh P20 has several alarm options. Here you can determine the alarm receiver for the alarm sent by e-mail. To this end, the following settings have to be configured:

- **User/Login/E-mail address:** Enter the account name of the e-mail address.
- **Authentication password:** Enter the password for the e-mail address via which you want to send the alarms.
- **Send e-mail address:** Enter an e-mail from which the alarms are to be sent.
- **Receive e-mail address:** Enter an e-mail to which the alarms are to be sent.
- **SMTP Server:** Enter the address of your SMTP server for the sender e-mail address.

- **Port:** If necessary, you can configure the port via which the message is sent here.

3.9 NAT configuration

The Network Address Translation (NAT) is a procedure for changing IP addresses in IPv4 packages. Thus you can enable communication between two networks whose devices normally cannot interact. It is also possible to separate an existing network. For this, the higher-level network has to be connected to the Layer 3 port of the switch. The default port for this is **Port 20**. You can connect devices for the internal network to the other 19 ports. With the NAT function, you can specifically define which devices of your internal network are permitted to communicate with the devices of the external (higher-level) network.

3.9.1 NAT configuration rules

In this menu, you can define Network Access Translation rules. To create a NAT rule, the following entries have to be made:

- **Name:** Enter a name for the NAT rule.
- **Mode:** Here you can determine whether the rule only applies for UDP, only for TCP, or for all protocols.
- **Internal IP address:** Enter the IP address of the device that is to be allowed to communicate with the higher-level (external) network.
- **Internal network port:** This entry is only necessary if you select TCP or UDP mode. The devices of the external network are only permitted to access one port of the internal device. None of the other ports can be accessed.
- **External IP address:** The IP address to be entered here can be chosen freely. It only has to be from the address range of the higher-level network, and must not be assigned yet. With this IP address, the device can be reached from the higher-level network.
- **External network port:** This entry is only necessary if you select TCP or UDP mode. The external device can only use this specified port to access the internal device.

Figure 24: NAT Configuration Rule

3.9.2 NAT binding

In this menu, you can specify the IP address of the Layer 3 port. This address has to be within the address range of the external network. After you have configured this setting, the address has to be coupled with the created NAT rules. To do so, select the NAT name and confirm the entry with the + button. A NAT rule only becomes active once it has been coupled with the address of the Layer 3 port.

3.10 Advanced config

3.10.1 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 (w0 – w3).

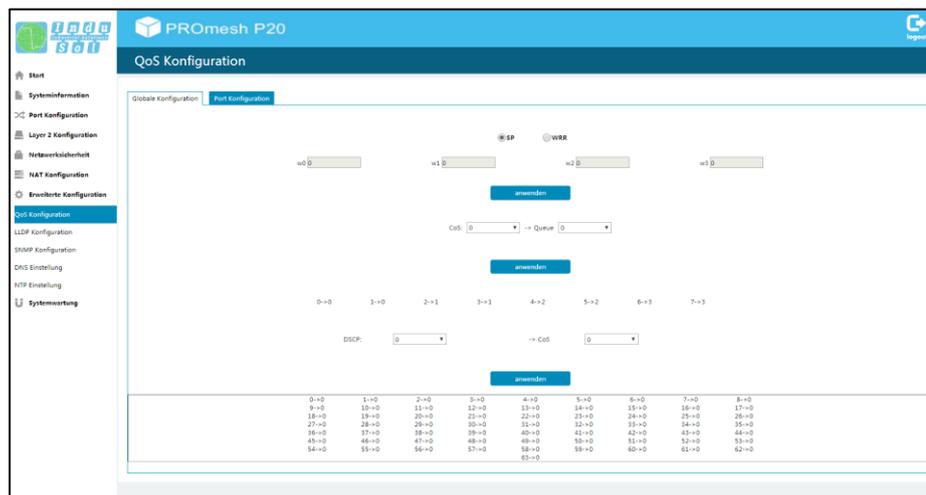


Figure 25: Quality of Service

QoS mode and priority scheme

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

- **Port-based only:** 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. You can configure settings for this type of QoS in the *Port Configuration* submenu.
- **Class of Service only:** 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 only:** 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. To do so, select the desired DSCP priority and assign it to a CoS priority.

Selection priority mode:

- **Strict Priority Scheme (SP):** 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.
- **Weighted fair queueing:** This approach ensures that not only high-priority packages but also packages with lesser priority are sent. This is made possible by sending packages of a queue based on a customizable weighting. Once all queues have been processed, the cycle restarts. This leads to only minor increased latency for the high-priority packages. To configure the weighting, enter values into fields w0 – w3. W3 is for packages with the highest priority. The following setting is recommended:
 - w3 = 8 packages
 - w2 = 4 packages
 - w1 = 2 packages
 - w0 = 1 packages



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

3.10.2 Link Layer Discovery Protocol (LLDP) – Topology

The Link Layer Discovery Protocol (LLDP) is a manufacturer-independent Layer-2 protocol which provides the possibility to exchange information between neighbouring devices.

The LLDP topology presents the neighbouring devices by ports with IP addresses and description (see Figure 26).

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. You can set the interval at which the information is sent under *Sending Cycle*. The default setting is 5 seconds.

The following information is compiled and sent by the LLDP:

- System name
- System description
- Port description

The web interface contains an up-to-date overview with information regarding directly neighbouring devices.

Information on the following is provided:

- **System name:** Here you can find the name of the connected device.
- **Chassis ID:** Here you can find the PROFINET name of the device.
- **Local interface:** Here you can find the port of the **PROmesh P20** to which the other device is connected.
- **Port ID:** Here you can find the port of the connected device via which the device is connected to the switch.
- **System description:** Here you can find a description of the connected device.

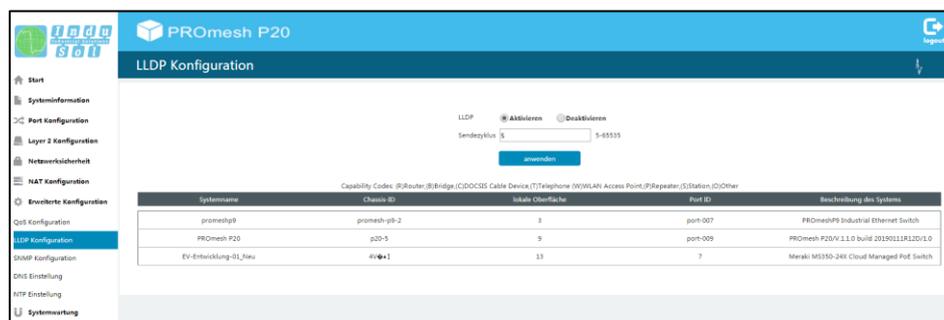


Figure 26: LLDP – Topology

3.10.3 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.

Community

SNMP queries are sent by the management station with a so-called community string that represents a simple access restriction. Community strings can be created or deleted in the SNMP menu (Figure 27). The overview table displays the currently defined community strings and access permissions. The following entries are required for creating a community string:

- **Community string:** Define a community string here. By default, the string *public* is used for read/write access and the string *private* for read-only access.
- **Mode:** Select whether the user can only read data from the device (read-only) or can also edit data (read/write).

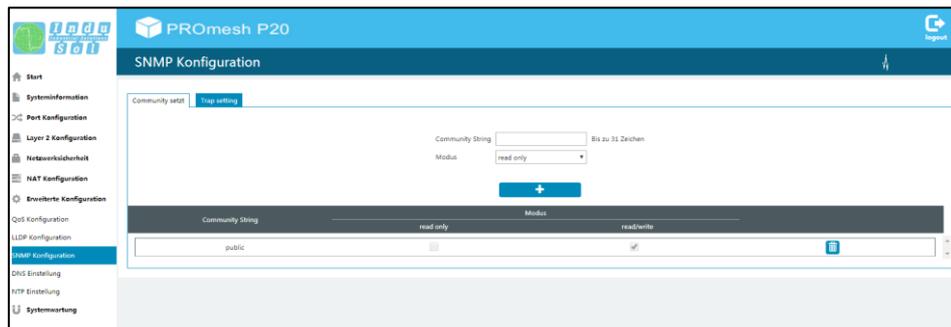


Figure 27: Overview of the currently available SNMP accesses

Trap setting

If an alarm is triggered, the **PROmesh P20** can send alarms to one or several management stations via SNMP. You can save the receiver addresses in this menu. Additionally, the community that you have created in the *Community* menu has to be entered.

3.10.4 DNS setting

The main purpose of the domain name system (DNS) is answering queries for resolving the name. This works like a telephone enquiry. The user only knows the domain name. The DNS server supplies the associated IP address that is needed to go to the website. When receivers for e-mail alarms are configured, an SMTP server has to be saved. If it is not entered as IP address, a DNS server has to be entered so that the SMTP server can be correctly resolved.

In this menu, you can enter a DNS server. You can enter a secondary SMTP server for security purposes.

3.10.5 NTP setting

In this menu, you can configure the device time of the **PROmesh P20**, which is also available in the *Device Time* field. If necessary, you can synchronize this with the time of the PC on which you have opened the web interface.

It is also possible to configure the device time by means of an NTP server. For this, the following steps are required:

- Activate the time synchronizations by means of the NTP server.
- Select the time zone where you are.
- Enter an interval at which the time of the switch is regularly updated with the NTP server.
- Enter the NTP server of your network.

3.11 System maintenance

3.11.1 Configuration file management

The Configuration File Management menu is divided into two additional menus. The *Global Config* menu contains a list of all configurations made. These can be saved in the *Configuration File Management* menu on the SD card. It is also possible to load existing configurations from the SD card and applying it for the switch.

Here you can also perform firmware updates or save the current firmware. Please use only a firmware version that you have received from Indu-Sol and that was developed specifically for the PROmesh switches.

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.

3.11.2 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.

3.11.3 Restore factory settings

With this menu item, the device can be restored to its default settings. Click the *Restore* button to execute the action and confirm this in the window that opens. Afterwards, the device needs to be rebooted.

3.11.4 Online update

In this menu, you can save your firmware to an TFTP server. To do so, the following entries have to be made:

- 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.

3.11.5 HTTP update

In this menu, you can install a new firmware for the *PROmesh P20*. Please use only a firmware version that you have received from Indu-Sol and that was developed specifically for the PROmesh switches.

3.11.6 SD card

In this menu, you can load an existing configuration from your SD card. To do so, select the file name and then click on the *Update* button.

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 P20** 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	16 x 10/100Base TX RJ45 ports 4 x 10/100 /1000BaseX SFP ports
10/100Base/ 1000Base TX ports	RJ45 / Autonegotiation / Auto MDI/MDI-X / supports cables up to a length of 100 m (CAT 5)
Power supply	12 V .. 48 V DC redundant voltage supply
Power consumption	Maximum 22 W
Potential isolation	500 V
Dimensions (H x W x D)	138 mm x 130 mm x 68 mm
Weight	0.96 kg
Housing	Aluminium, anodised
Storage temperature	-40°C .. 85°C
Operating temperature	0°C .. 55°C
Humidity	Humidity 5 % ... 95 %, RHD non-condensing
Protection class	IP30
Assembly	35 mm DIN top-hat rail
EMC	EN 61000-6-2 / EN 55022 Class A
LED indicators	Status LEDs / Port LEDs (green) / voltage supply (green)
IEEE	IEEE 802.3 10Base-T Ethernet / IEEE 802.3u 100Base-TX Fast Ethernet / IEEE 802.3z 1000Base-TX Gigabit 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, Reset, Port Mirror, IP Security Management, IGMP Management MIB
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 1488.000 pps for 1000Base-TX Gigabit Ethernet Port
MAC Address table	16K 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 four 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
NTP	NTP for time synchronisation
SMTP	SMTP server and E-mail account for event notifications
Port Mirror	Only TX packages, only RX packages, or TX and RX packages
Firmware update	SD card, TFTP server, from local PC
Alarm contact	Relay contact 25 V DC (1A) / 60 V 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 Schmölln

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

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

Wir sind zertifiziert nach DIN EN ISO 9001:2008