

# *pe-light-S-switch*

Art. No.: 0685x4xxx



eks Engel FOS GmbH & Co. KG  
Schützenstrasse 2-4  
57482 Wenden-Hillmicke  
Germany

Tel.: +49 (0) 2762 9313-600  
Fax: +49 (0) 2762 9313-7906  
E-mail: [info@eks-engel.de](mailto:info@eks-engel.de)  
Internet: [www.eks-engel.de](http://www.eks-engel.de)

## Legal notice

This manual contains important notes and warnings that could lead to serious personal and property damage if ignored. Please read this manual carefully prior to commissioning the *pe-light-S-switches*. Correct transport, correct storage, and installation and careful operation and maintenance of the *pe-light-S-switch* are critical for safe operation.

## Intended use

The devices in the *pe-light-S-switch* product family may only be operated as described in this manual. These may only be used free of damage and according to the indicated environmental conditions. The enclosure of the *pe-light-S-switch* may only be opened by eks technicians; the devices do not contain any components that must be maintained by the customer.


## Personnel requirements

Installation and commissioning of the *pe-light-S-switch* may only be completed by trained personnel who are familiar with this operating manual. Furthermore, all work on electrical systems may only be completed by an electrician or under his direction and supervision. Applicable local and national safety conditions must be maintained at all times.

## Voltage supply

The devices in the *pe-light-S-switch* product family have been designed for operation with SELV voltages via an LPS (Limited Power Source). These may only be powered via SELV/LPS conform with IEC 60950-1/EN60950-1/VDE0805-1, which in turn are supplied with voltage via NEC Class 2 conform voltage supplies.

The shielding of the M12 sockets is connected with the enclosure of the *pe-light-S-switch* to discharge faults. Note any possible short circuits when using shielded cables.

	<h1>Software Operating Manual</h1>	MAN_pe-light-S-switch
		Version: 2021-09-13
		Authorized by: T.W.
		Page 3 of 61

## Laser equipment safety

The devices in the *pe-light-S-switch* product family include LED or LASER components as per IEC 60825-1 (2014): class 1 laser/LED product.

### Warning!

Do not use optical instruments (e.g. lenses, microscope) to look into the beam of the optical transceivers! Ignoring this warning may result in eye damage.



### Disposal notes

The devices must not be disposed with normal household waste but can be returned to eks Engel FOS GmbH & Co. KG for disposal.

WEEE-identification: DE 900 53 255



# Foreword

---

## Overview of the *pe-light-S-switch* product family

The devices in the *pe-light-S-switch* product family are industrial Ethernet switches including management features that can be configured comfortably and easily via a web application. These enable low-cost installation of industrial Ethernet bus, star, and ring structures with switching functionality.

## Properties

- » Web application for configuration
- » 10BASE-T/100BASE-TX/1000BASE-TX (M12) und 1000BASE-FX (MM or SM)
- » PHY and MAC completely compatible to IEEE 802.3, IEEE802.3u, and IEEE 802.3x
- » Auto MDI/MDI-X crossover-function für 10BASE-T, 100BASE-T and 1000BASE-T-Ports
- » Store-and-forward switching architecture with 2048 MAC address table
- » Quality of Service (QoS) with four priority queues
- » Prioritize via IEEE 802.1p Class of Service (COS), Type of Service (TOS)/DiffServ or port priority
- » Limitation of incoming and outgoing packets
- » Port mirror for TX or TX and RX packets
- » Port-based VLAN/802.1Q Tagged VLAN
- » Simple Network Time Protocol (SNTP)
- » Simple Mail Transfer Protocol (SMTP) for signaling alarms
- » Internet Gateway Management Protocol Snooping (IGMP Snooping)
- » Dynamical Host Configuration Protocol (DHCP) client function
- » Simple Network Management Protocol (SNMP)
- » Update, save, and back up the system configuration via TFTP and HTTP
- » PoE+ support at M12 ports

# 1 Table of contents

---

- Legal notice .....2**
  - Intended use .....2
  - Personnel requirements .....2
  - Voltage supply .....2
  - Laser equipment safety.....3
- Foreword .....4**
  - Overview of the *pe-light-S-switch* product family.....4
  - Properties .....4
- 1 Table of contents.....5**
- 2 Hardware Description.....9**
  - 2.1 LED displays .....9
  - 2.2 Ports .....11
    - 2.2.1 M12 ports ..... 11
    - 2.2.2 Optical ports ..... 11
    - 2.2.3 Wiring..... 11
- 3 Network topologies/redundancy ..... 12**
  - 3.1 Star structure .....12

3.2	Meshed networks .....	13
3.3	Ring structure .....	14
<b>4</b>	<b>PoE .....</b>	<b>15</b>
4.1	Supported PoE Standards .....	15
4.2	Derating .....	15
4.3	Port prioritization.....	15
<b>5</b>	<b>Web application.....</b>	<b>16</b>
5.1	Preparations .....	16
5.2	System login.....	17
5.3	Web interface .....	18
5.3.1	Menu bar.....	18
5.3.2	Information bar .....	18
5.4	System information .....	19
5.4.1	Status and diagnosis .....	19
5.4.2	Alarms/Notifications.....	19
5.4.3	Port statistics.....	22
5.4.4	Syslog messages .....	24
5.4.5	Link Layer Discovery protocol – topology .....	25
5.5	Basic settings .....	28

5.5.1	IP configuration .....	28
5.5.2	Password .....	30
5.5.3	Time setting.....	31
5.6	Port configuration.....	34
5.6.1	Port Mirroring.....	36
5.7	Redundancy .....	37
5.7.1	Media Redundancy Protocol (MRP).....	37
5.7.2	Rapid Spanning Tree Protocol (RSTP).....	38
5.8	Switching .....	43
5.8.1	IGMP Snooping.....	43
5.8.2	VLAN 802.1Q .....	44
5.8.3	Quality of Service (QoS).....	47
	Rate Control.....	49
5.9	Access .....	51
5.9.1	Simple Network Management Protocol (SNMP).....	52
5.10	Maintenance .....	54
5.10.1	Backup .....	54
5.10.2	Restore .....	54
5.10.3	Firmware update .....	55
5.10.4	Factory settings.....	56

5.10.5 Reboot.....	57
5.10.6 Licenses .....	57
<b>6 Instructions for troubleshooting.....</b>	<b>58</b>
<b>7 Technical specifications.....</b>	<b>59</b>
<b>8 GPL/LGPL guarantee and liability exclusion .....</b>	<b>60</b>
<b>9 Table of figures .....</b>	<b>61</b>



## 2 Hardware Description

---

### 2.1 LED displays

The front panel of the switch features 3 diagnosis LEDs. Furthermore, each of the Ethernet ports features one status LED.



The LED displays offer real-time information regarding the status of the *pe-light-S-switch*, see Table 1: LED-Description.

LED	State	Meaning
VDC	Green	Sufficient voltage is connected
	Off	No sufficient voltage is provided
Door Contact	Red	Door contact opened
	Off	Door contact closed

<b>Fail</b>	Red	Configured alert active
	Off	No Alert active
<b>LNK/ACT</b>	Yellow	Connected
	Yellow (Flash)	Data received / sent
	Off	No connection

**Table 1: LED-Description**

## 2.2 Ports

### 2.2.1 M12 ports

The *pe-light-S-switch* features four M12 ports, each with transfer rates of 10 mbps, 100 mbps or 1000 mbps. The ports detect the data rate automatically. Sending and receiving lines are crossed appropriately via MDI/MDI-X auto-crossover so that connections are able to be established with other devices, independent of the cable type used (1:1 or crossed).

### 2.2.2 Optical ports

The *pe-light-S-switch* is equipped with two 1000Base-FX ports. The LWL ports have LC plug connectors and are available for different fiber types (multi-mode, single-mode).

Please make sure that the transceivers of the *pe-light-S-switch* are always connected with transceivers of other devices that are suitable for the same wavelength and the same fiber type.

The transmitters of a device must always be connected with the receiver of the opposite device and vice-versa.

### 2.2.3 Wiring

- » Use twisted-pair cable of category 5e or better to connect the M12 ports. The electrical connection cable between the switch and the connection partner (switch, hub, workstation, etc.) may not be longer than 100 meters. Use metal shielded connectors on the cables.
- » Connect the multi-mode transceiver with 50/125 µm or 62.5/125 µm multi-mode optical fiber cables.
- » Connect the single-mode transceiver with 9/125 µm single-mode optical fiber cables.

#### Warning!

Do not mount *pe-light-S-switches* directly beside devices that produce strong electromagnetic interference fields, e.g. transformers, contactors, frequency inverters, etc.

#### Warning!

Do not mount *pe-light-S-switches* directly next to heat producing devices and protect the switch against direct sunlight in order to prevent unwanted heating.

## 3 Network topologies/redundancy

The devices in the *pe-light-S-switch* product family can be used with various protocols in addition to use in star-shaped switched-Ethernet networks and in redundant networks such as meshed networks or rings.

### 3.1 Star structure

Classic Ethernet star structures, see Figure 1, can be networked using devices in the *pe-light-S-switch* product family without additional configuration. The devices are immediately ready to function.

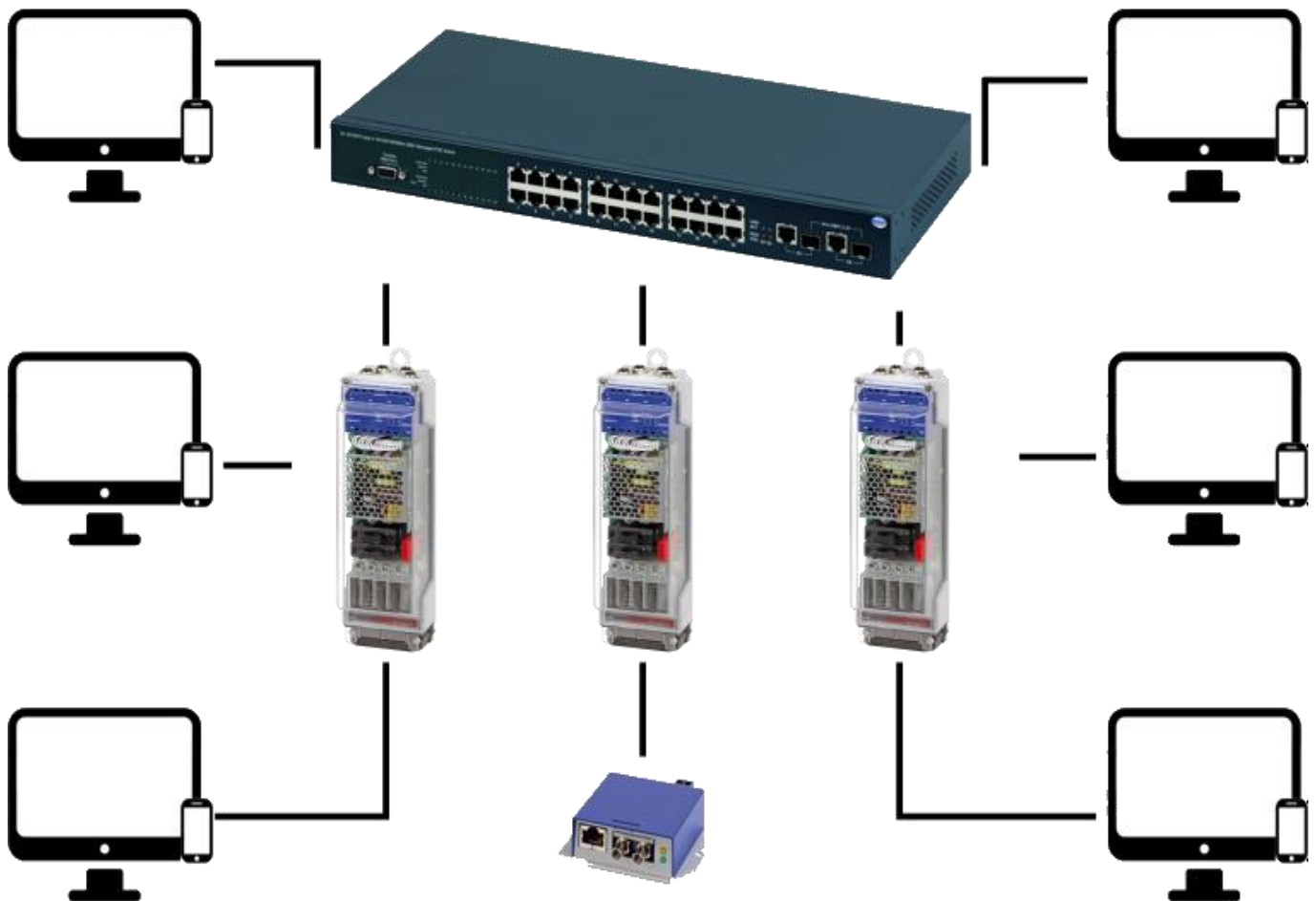


Figure 1: *pe-light-2* in a star-shaped network

### 3.2 Meshed networks

Use of the Rapid Spanning Tree protocol (RSTP) enables any Ethernet structures to be built, for example, as displayed in Figure 2. STP and RSTP break these structures up into a tree structure and reconfigure this tree structure in case of changes to the topology. The reconfiguration time is typically less than 1 s for Rapid Spanning Tree.

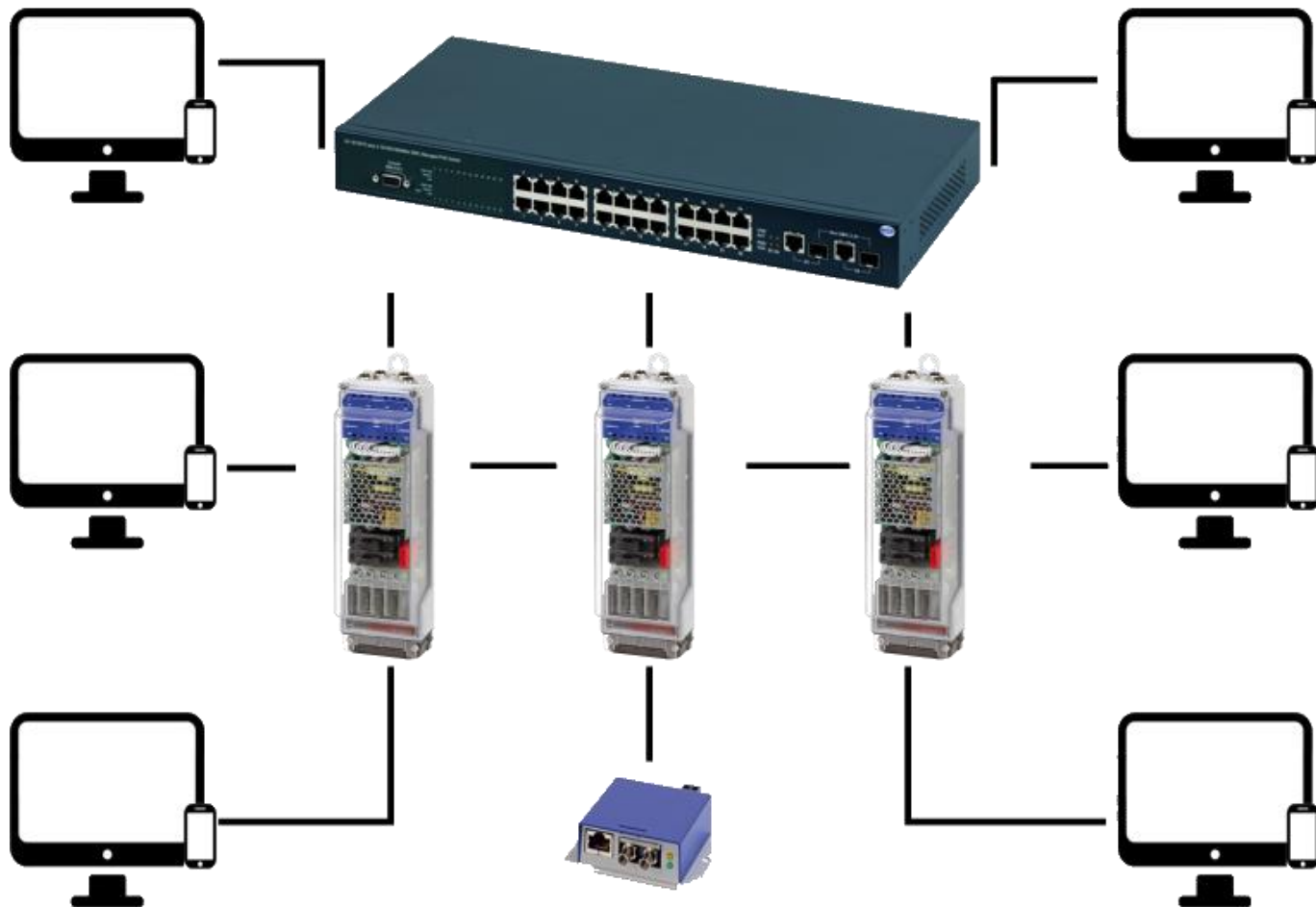


Figure 2: *pe-light-2* in a meshed network

### 3.3 Ring structure

The *pe-light-S-switch* supports the Media Redundancy Protocol as per IEC 62439 (MRP ring), which enables the system to recover from network failures within 200 ms or less. The MRP ring increases the reliability of the network in this way. Figure 3 shows an example for use with ring functionality. The switch can be configured as Manager or Client.

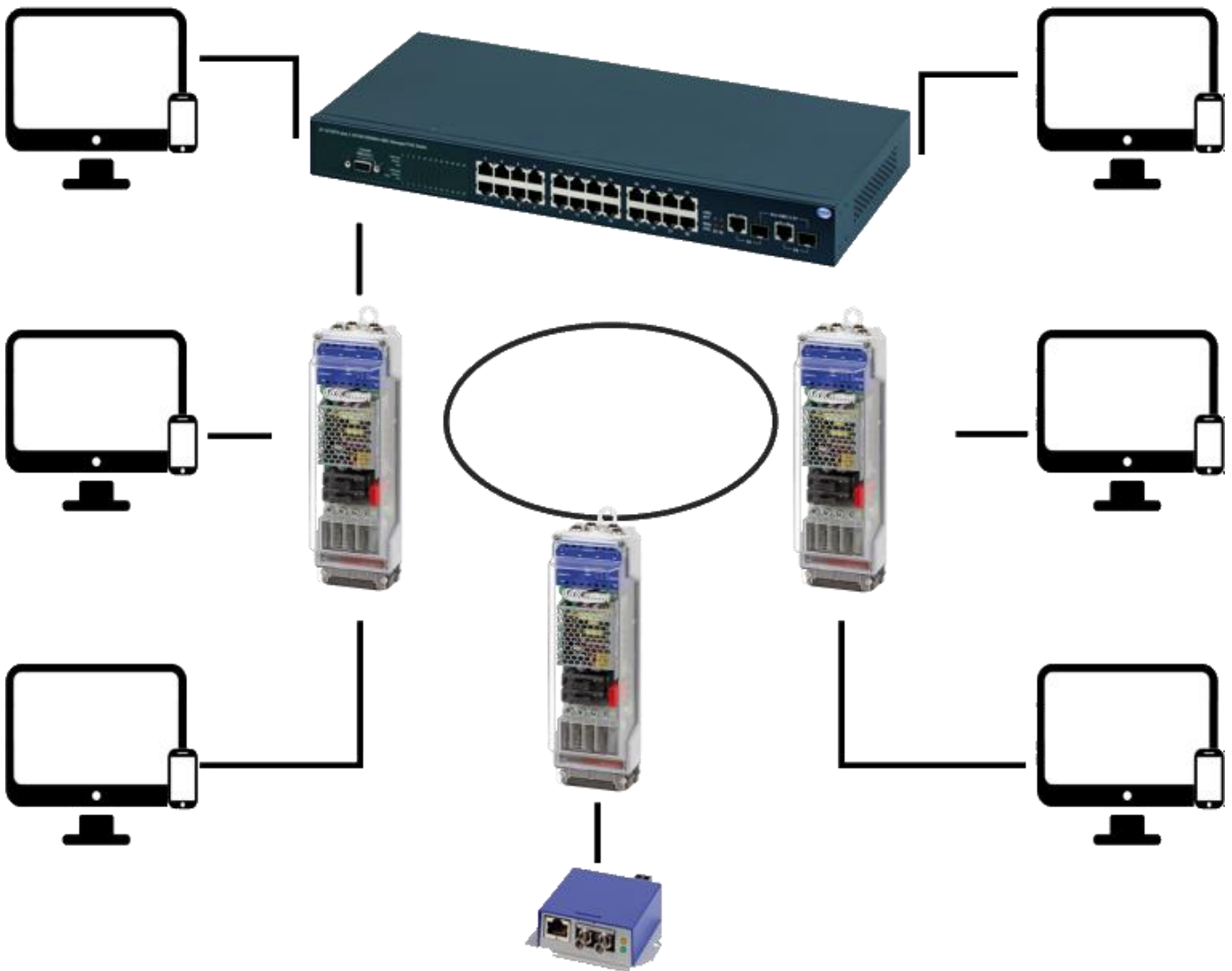


Figure 3: *pe-light-2* in a ring-shaped network

## 4 PoE

The *pe-light-S-switch* supports the PoE+ Standard up to a system performance of 120W. Each port supports up to 60W. To calculate the system’s total power, the maximum allowed power for each port’s class is used, even if the port does not currently use the full power.

### 4.1 Supported PoE Standards

The *pe-light-S-switch* supports the following standards:

- » ieee 802.3 af, class 1 to 3, type 1 (4W, 7W, 15.4W)
- » ieee 802.3 at, class 4, type 2 (30W)
- » ieee 802.3 bt, class 1 to 6, type 3 (4W, 7W, 15.4W, 30W, 60W)

### 4.2 Derating

Starting on a system temperature of 70°C, the system performance of the *pe-light-S-switch* is gradually reduced based on port priorities in a timely cycle of 5 minutes. Once the critical temperature of 70°C is exceeded, the port with the lowest priority is disabled. If, after a waiting period of 5 minutes, the temperature still exceeds the critical limit, further ports are disabled one by one until the temperature no longer exceeds the critical limit of 70°C.

### 4.3 Port prioritization

The current control software of the *pe-light-S-switch* sets the M12 ports to fixed priorities.

Port	Priority
Port 1	High
Port 2	High
Port 3	Medium
Port 4	Low

Table 2: *pe-light-switch* default port priority

## 5 Web application

---

*pe-light-S-switches* are equipped with a modern web interface so that they can be configured conveniently using any web browser. With factory settings the device's IP-Address is set to 192.168.10.1.

### 5.1 Preparations

Before you use the web management feature, install the *pe-light-S-switch* in the network and ensure that the PC intended for configuration of the switch is in the same subnet to be able to access the switch via the web browser. The device credentials set upon delivery are available here:

» User name: **admin**

» Password: **admin**

Alternatively to administrator access, guest access with fewer permissions and adjusted menu guidance is also available. The guest user does not have access to the switching and maintenance functions and their sub-items. The access data are:

» User name: **guest**

» Password: **guest**

**Note:**

Please change the passwords of the admin and guest users, before you use the device in your network. See 5.5.2.



## 5.2 System login

1. Start a web browser on your computer.
2. Enter the configured IP address of the *pe-light-S-switch* and then press the “Enter” key. With factory settings the device’s IP-Address is set to 192.168.10.1. See section 5.5.1 for information about the IP-Address configuration.
3. The login mask of the device now appears on the screen.

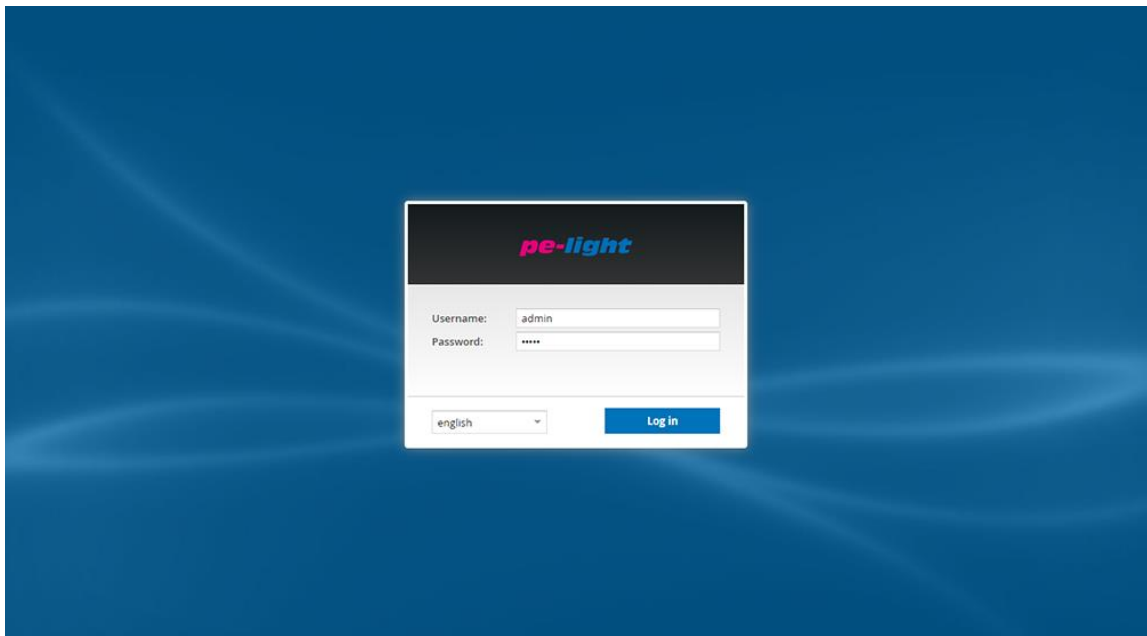


Figure 4: Login Window

4. Select the desired menu language.
5. Now enter the user name and password.
6. Press the “Enter” key or click “Login”. You will now enter the web interface of the switch.

## 5.3 Web interface

The web interface of the *pe-light-S-switch* comprises the menu bar on the left edge, the information bar in the top area, the actual configuration in the center, and the help on the right edge, see Figure 5.

### 5.3.1 Menu bar

The menu guide enables you to access the individual screens and complete settings there. The menu items displayed are divided into additional sub-items.

### 5.3.2 Information bar

The information bar shows you the device type, location and the IP address. The current user is shown under the logout button on the right end of the bar. By pressing the button, you can log out and lock the webgui of the device. The help button shows instructions and explanations for the individual screens.

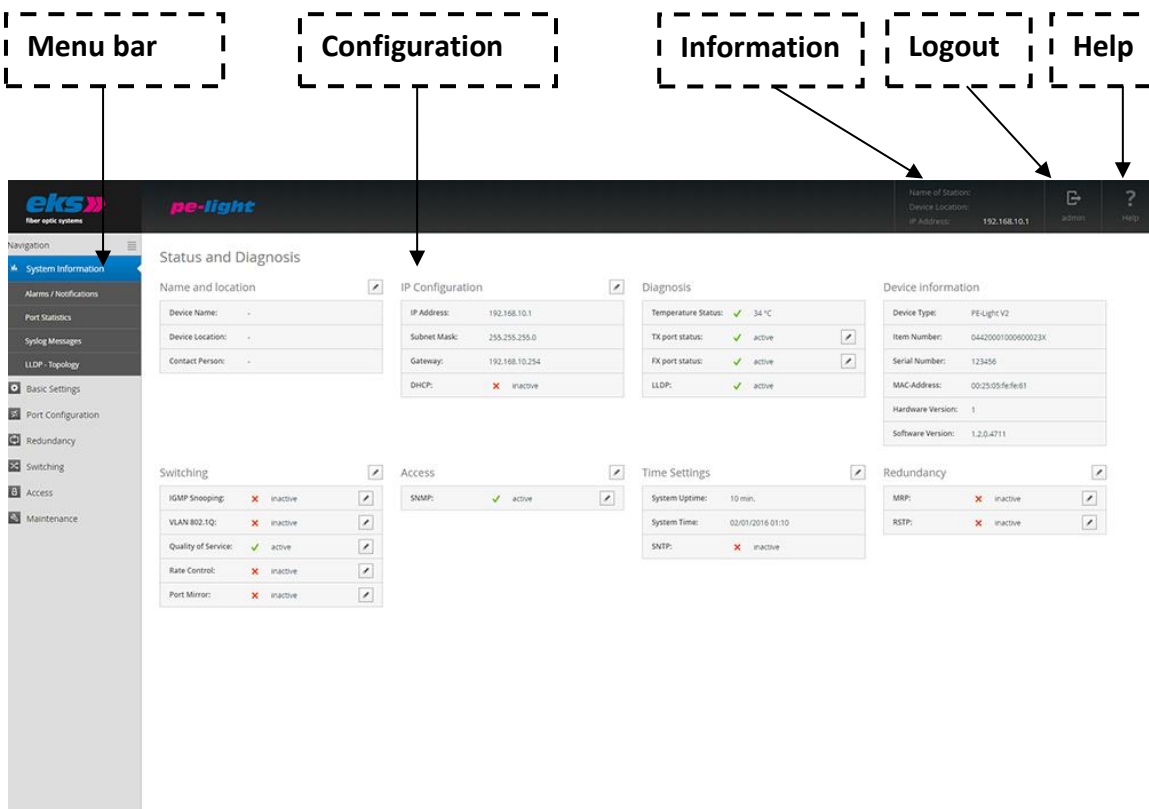



Figure 5: Status and diagnosis

	<h1>Software Operating Manual</h1>	MAN_pe-light-S-switch
		Version: 2021-09-13
		Authorized by: T.W.
		Page 19 of 61

## 5.4 System information

The system information screen offers you a complete overview of the status and current configuration of the *pe-light-S-switch*.

### 5.4.1 Status and diagnosis

On the actual status and diagnosis screen, an overview displays the currently activated and deactivated protocols and functions in addition to the serial number, hard and software version of the device. With the help of the editing buttons, you can directly change to the corresponding protocols and functions to change the settings there.

### 5.4.2 Alarms/Notifications

The menu item alarms/notifications is used to define alarm triggers and alarm receivers. Alarm triggers indicate which alarms of the software should be observed. If alarms occur for which an alarm trigger is defined, then a log entry will be created and the Fail LED will be activated. In turn, alarm receivers connected with the alarm trigger are informed or activated. Alarm triggers include, for example:

- » a status change at a port
- » temperature that is too high or too low
- » Media Redundancy Protocol Error
- » opening the door contact
- » PoE Power that is too high or too low

Alarm receivers are:

- » SNMP traps
- » E-mail addresses

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

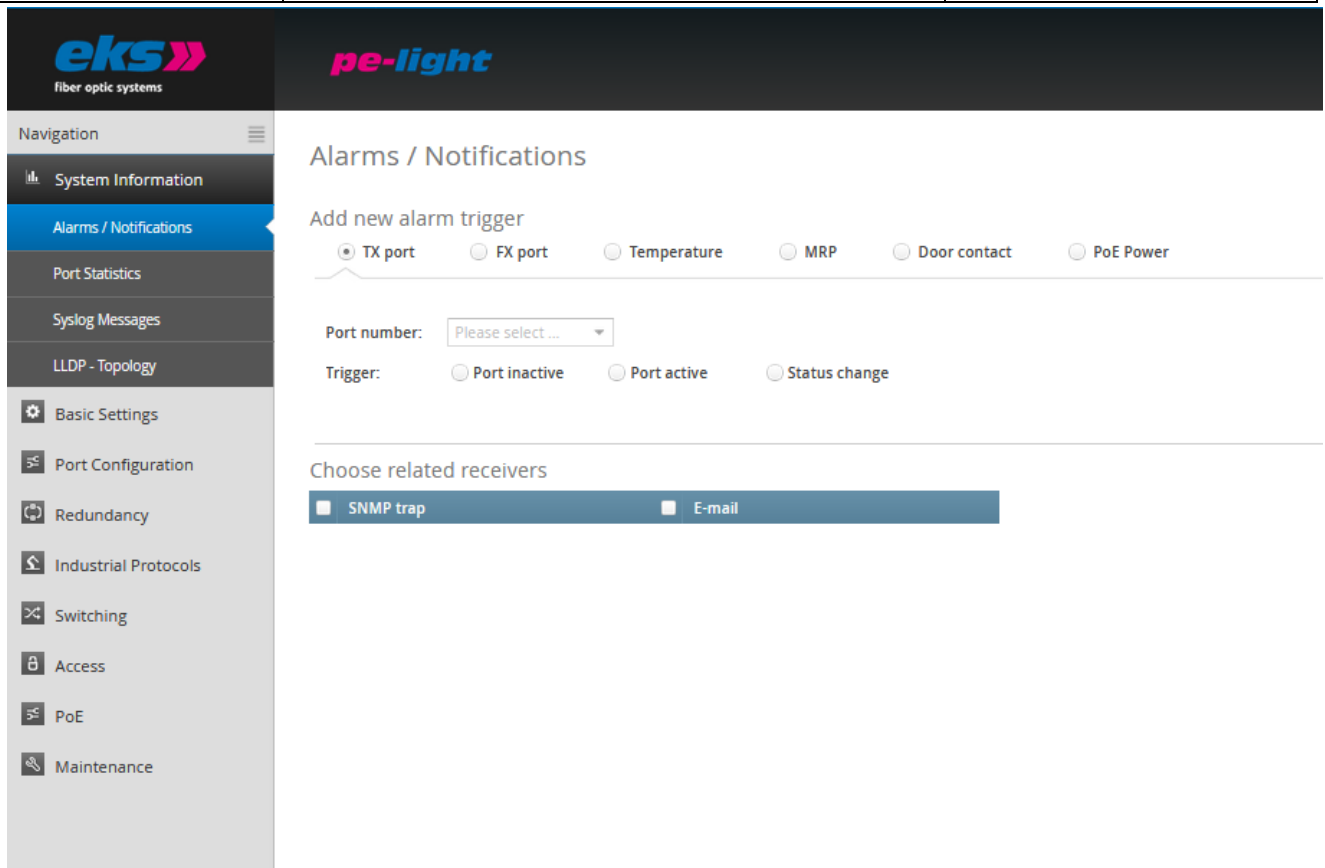
With the help of the alarm trigger and alarm receiver screen tabs, the view can be switched between:

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

### Add and edit alarm trigger

The alarm trigger screen tab (Figure 6) enables new alarms to be added by clicking the "+" button. If alarms are already present, they can be edited or deleted using the button on the right in the table. When adding and editing alarms, the associated receiver can be selected in the lower part of the screen and linked to the alarm trigger in this way. The following alarm triggers are possible:

- » The Ethernet ports can trigger an alarm in case of activity, inactivity, and status change.
- » Alarms can be configured to be raised if the device's temperature rises above an upper limit or if it sinks below a lower limit.
- » MRP events (ring interruption, ring connected again, generic warning) may create an alarm.
- » Alarms can be configured to be raised if the door contact is opened.
- » Alarms can be configured to be raised if a Port's PoE Power rises above an upper limit or if it sinks below a lower limit.



**Figure 6: Alarms/notifications: Adding an alarm trigger**

### Add and edit alarm receiver

By clicking the "+" buttons below the alarm receiver screen tab (Figure 7), new receivers can be added. SNMP traps and e-mail in-boxes can be added as new alarm receivers.

#### Alarm receiver: SNMP trap

With the simple network management protocol (SNMP), the generated error messages of the device (which acts as agent) are sent to the management station whose IP-address is specified in the field "Trap receiver IP". The receiver will not send acknowledgement messages. So, there is no guarantee that the trap receiver received the information. Furthermore, you have to define a community string to ensure the communication between the management station and the agent. The settings will be confirmed by clicking the Create button.

#### Alarm receiver: E-mail

With the email notification, administrators can be notified about errors. Enter an email address and a SMTP-server IP (simple mail transfer protocol) to configure receivers. The device will send email messages if a configured alarm is triggered. If required, set up authentication credentials according to your needs. For this you have to select the checkbox “Authentication needed:” and define a SMTP password. Optionally, the encryption can be activated by selecting the checkbox. Subsequently, the port and the type of encryption can be defined.

The setting will be confirmed by clicking the Create button.

With the Button “Send test email” you can verify if the email setup works before the alarm receiver is created.

In the lower part of the screen, the alarm receivers can be assigned to previously added alarm triggers.

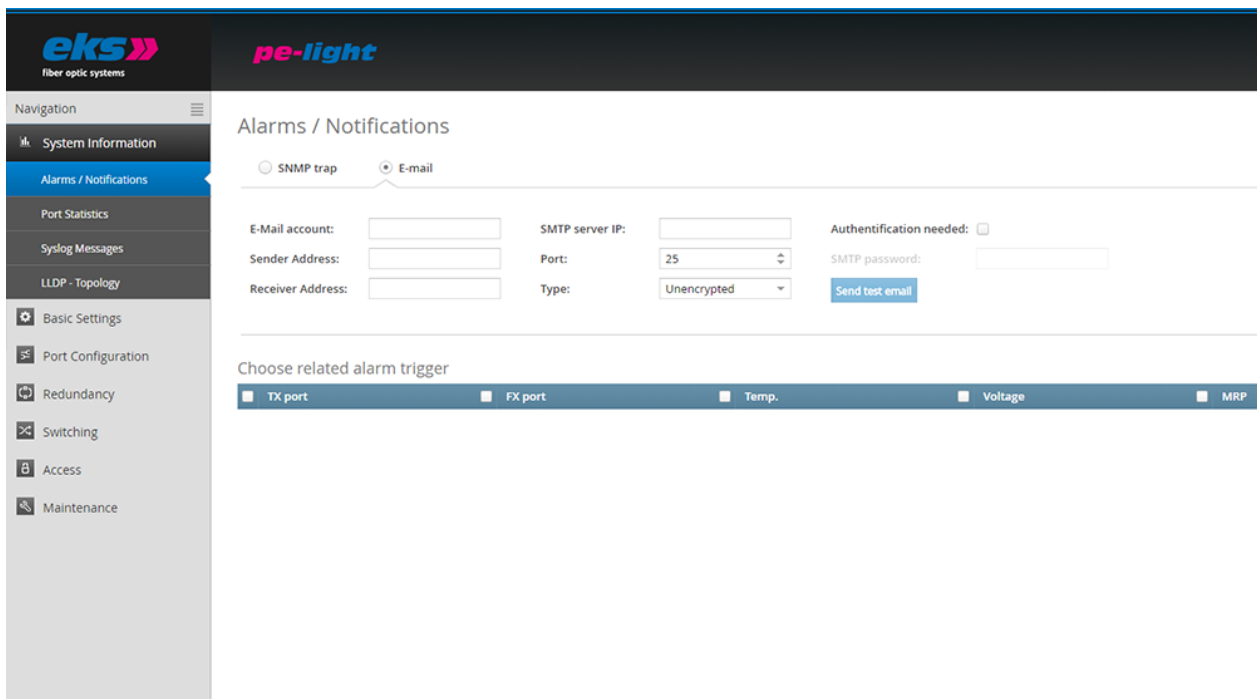


Figure 7: Adding an alarm receiver

### 5.4.3 Port statistics

The port statistics screen (Figure 8) provides information about the data traffic on the individual ports, which is helpful for diagnosis purposes in case of network problems. The complete number of sent, received, faulty, and colliding packets is displayed. Furthermore, the size of the individual packets is recorded statistically up to a variety of threshold values.

Sent packets are differentiated in terms of:

- » Number of packets
- » Number of Unicast packets (packets to one receiver)
- » Number of non-Unicast packets (packets to multiple receivers)

Received packets are differentiated in terms of:

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

The CRC errors column provides information about the number of faulty received data packets. The cyclical redundancy test, CRC (Cyclic Redundancy Check), specifies a test value using the transferred data. This value is sent together with the data and evaluated by the receiver. Faulty packets are detected and discarded in this way.

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

The packets up to bytes column provides information about the number of packets in diverse sizes. In this case, the number of packets received up to 63, 127, 255, 511, 1023, or 1518 bytes in size is recorded.

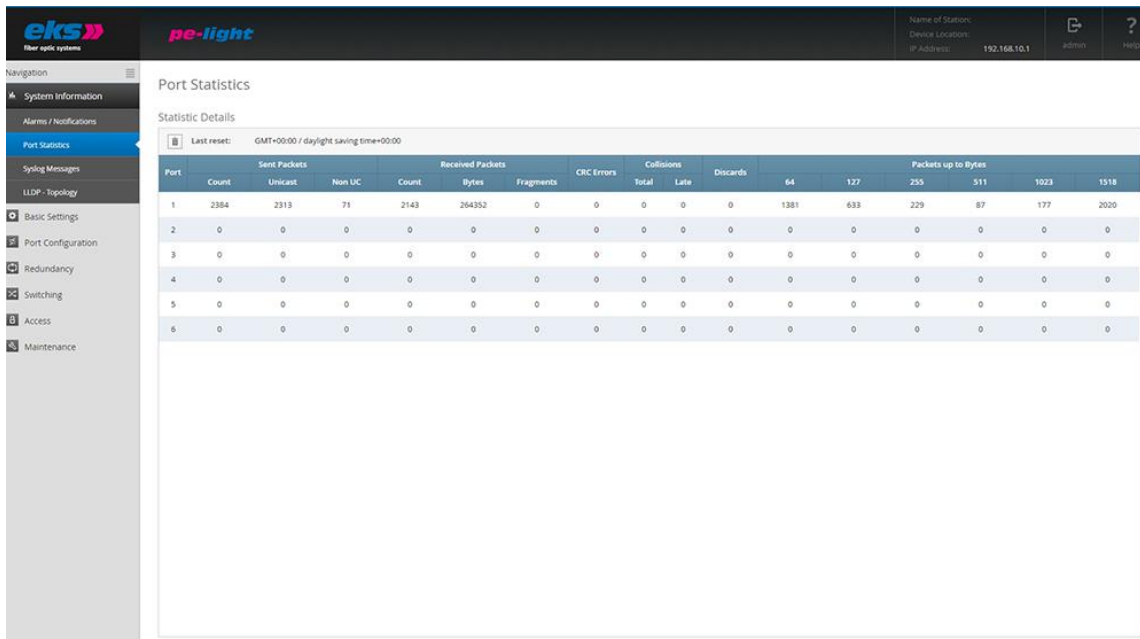
### Update and reset the values

The button above the table's header can be used to reset all values to 0. Using a second button, the option is available to reset the counters of all ports and start a new evaluation in this way. The time at which the evaluation was started is displayed in the status bar as the last reset.

### Sort and hide the entries

The port statistics offer valuable information about the network diagnosis. In order to simplify the diagnosis, the option is available to limit the display to the important columns.

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



Port Statistics

Statistic Details

Last reset: GMT+00:00 / daylight saving time+00:00

Port	Sent Packets			Received Packets			CRC Errors		Collisions		Discards	Packets up to Bytes					
	Count	Unicast	Non UC	Count	Bytes	Fragments	Total	Late	64	127		255	511	1023	1518		
1	2384	2313	71	2143	264352	0	0	0	0	0	0	1381	633	229	87	177	2020
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	9	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 8: Port statistics

## 5.4.4 Syslog messages

The Syslog messages (Figure 9) provide help for receiving status and error messages about the various functions and protocols. The messages are displayed in the overview including date and time, plus a code, a description, and a reference. Because the log entries are not saved in the device, they are no longer available after the device is restarted or if the voltage is interrupted. In order to archive the messages permanently, the option is available to use an external Syslog server or USB flash drive.

### Using the Syslog server

In order to archive the messages on a Syslog server or to save them, activate this function via the selection field in the top bar. Enter the IP address of the Syslog server and save the settings using the apply button that appears below. Please check if the server is available and if the messages are being saved in a file.



## Update, export, and reset the entries

The following buttons are available for this:

- Using the update button in the status bar arranged above the table, the table can be reloaded.
- The CSV export button creates a CSV file (Comma-Separated Values) including all entries from the table and saves these in the download folder of the browser. The messages are written in a file separated into rows by comma.
- The button for deleting the log file removes all entries from the table. After that all messages that occurred after this time are shown. The time that the entries were deleted is visible via the first log entry that appears.

## Sort and hide the entries

The individual columns of the Syslog messages can be hidden or sorted for using pull-down menus in the table labels.

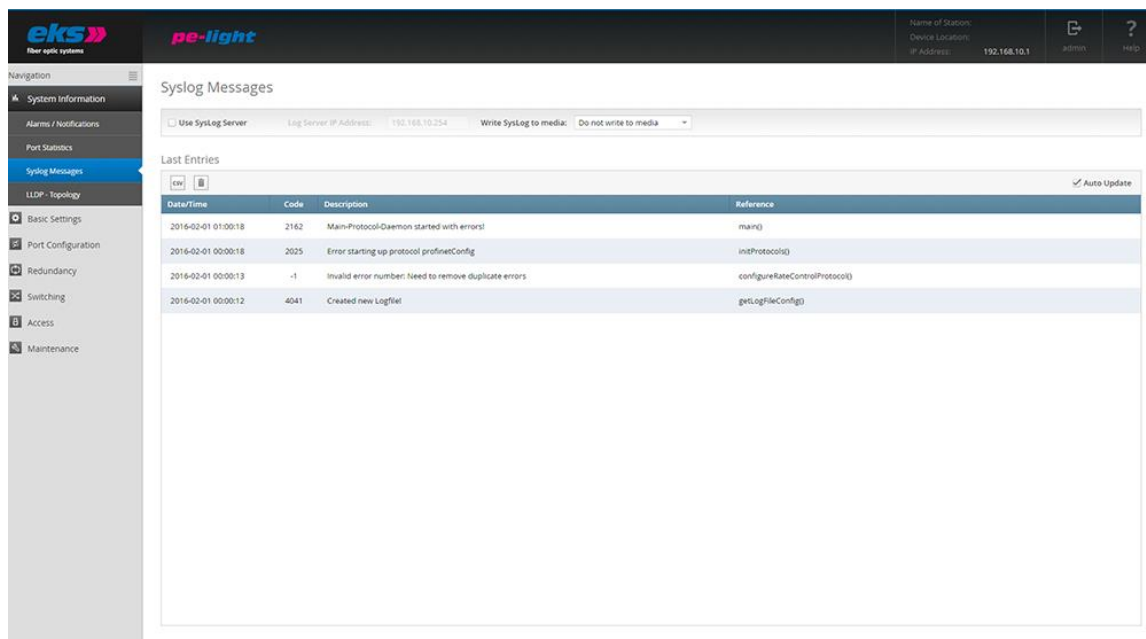


Figure 9: Syslog messages

## 5.4.5 Link Layer Discovery protocol – topology

The Link Layer Discovery protocol (menu see Figure 10) is a manufacturer-independent Layer-2 protocol, which is defined as per the IEEE-802.1AB[1] standard and offers the option to exchange information between neighboring devices. On every device that supports the LLDP, a software

component operates as the so-called LLDP agent. This sends information in periodic intervals concerning the actual status and receives information from neighboring devices permanently. Because this occurs independently of each other, the LLDP is also referred to as a one-way protocol. Before sending the information, no connection to the other devices is established.

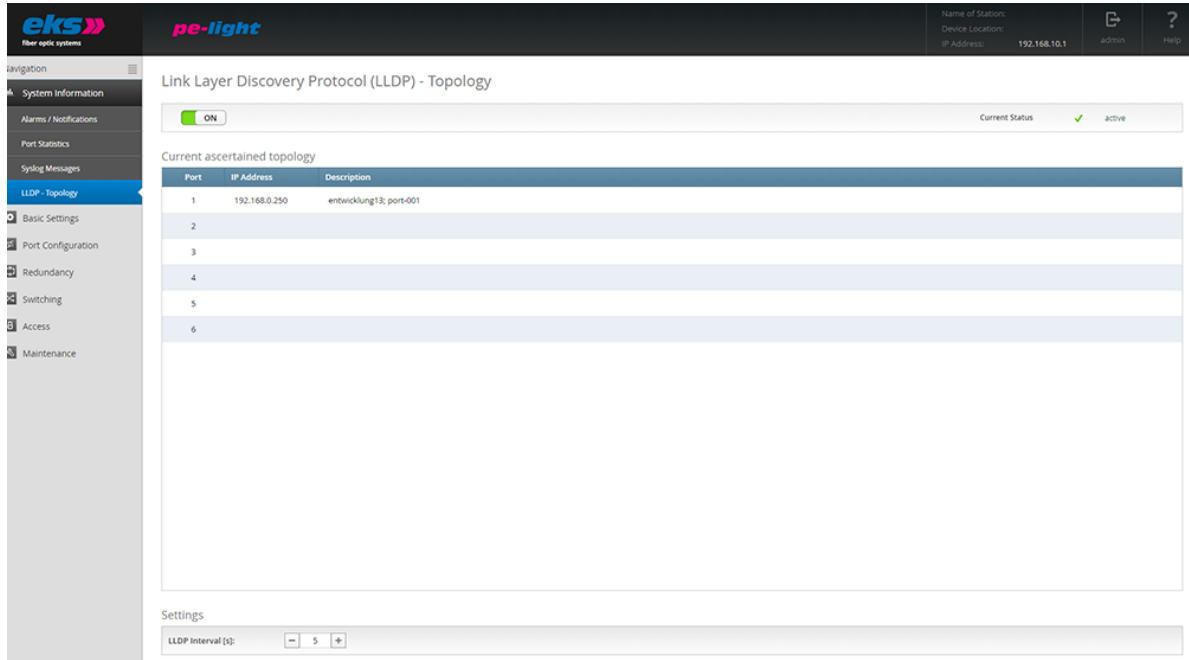
The following information is compiled by the LLDP and sent:

- » System name
- » System description
- » Port description
- » Chassis ID
- » IP-Address

System name, System description and Port description are set according to the values given in SNMP-MIB2. These values are read-only. The Chassis ID is the assigned device Name. In case no device name is assigned the MAC-Address is transmitted. The IP-Address is automatically set to the current device IP

### LLDP interval

The LLDP interval parameter can be used to specify the time intervals (in seconds) in which the device sends its own LLDP telegram to the neighboring devices.



**Figure 10: Link Layer Discovery protocol (LLDP)**

## 5.5 Basic settings

The basic settings screen (Figure 11) offers you the option to assign the device an individual name, a location, and a contact partner.

- » Device name: Assign a name to the *pe-light-S-switch* to clearly identify the device.
- » Location: The location provides you an additional option for identifying the device.
- » Contact partner: A contact partner responsible for the device can be saved in the third field.

The input fields allow a maximum amount of 50 characters. At least one character has to be set. The use of special characters is possible. The location is displayed in the information bar in the upper right and helps you to assign the web interface to a device.

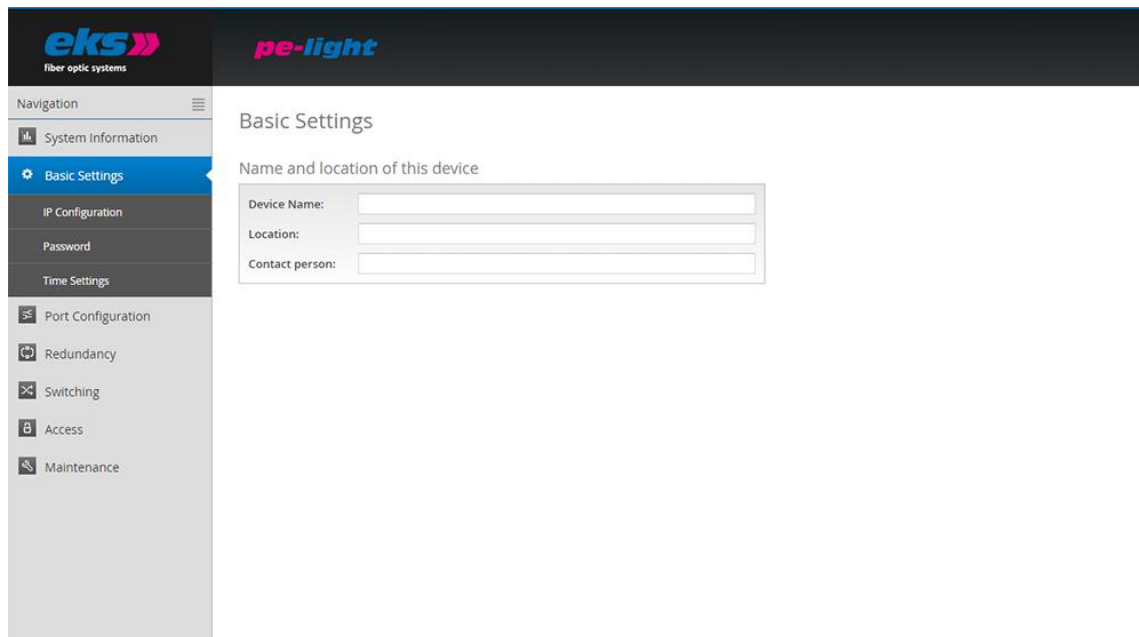



Figure 11: The basic settings of the *pe-light-S-switch*

### 5.5.1 IP configuration

You can either execute the IP configuration (see Figure 12) automatically with the help of the Dynamic Host Configuration Protocol (DHCP) or adjust the settings manually.

	<h1>Software Operating Manual</h1>	MAN_pe-light-S-switch
		Version: 2021-09-13
		Authorized by: T.W.
		Page 29 of 61

## Automatic

In order to receive a configuration for the IP-Address, the subnet mask and the standard gateway from a server working in the network with the corresponding functionality, activate the DHCP client function.

After you have saved the settings by clicking the apply button, the device sends a query to the network and accepts the configuration received by the DHCP server. Because the device has now received a new IP address, it can no longer be reached via the previously configured IP. Please contact your network administrator to receive the new IP address.

## Manual

If your network does not offer DHCP service, or if the settings should be made by hand, then select the manual IP configuration via the top area of the screen. Please check exactly which settings you change to avoid errors such as duplicate IP addresses, as these could have a negative influence on the entire network. The format of the IP address, the subnet mask, and the gateway must be entered in decimal point format. The following settings are required:

- » IP address: Please note that the set IP address must valid and reachable from your PC so that you can connect again with the device in order to make additional settings.
- » Subnet mask: Enter the subnet mask; this separates the IP address into a network component and a device component. This specifies which IP addresses are able to be reached in the network and which addresses are located in other subnets and only accessible via routers.
- » Gateway: Specify the standard gateway of the switch. The gateway is used to communicate with devices beyond the subnet.

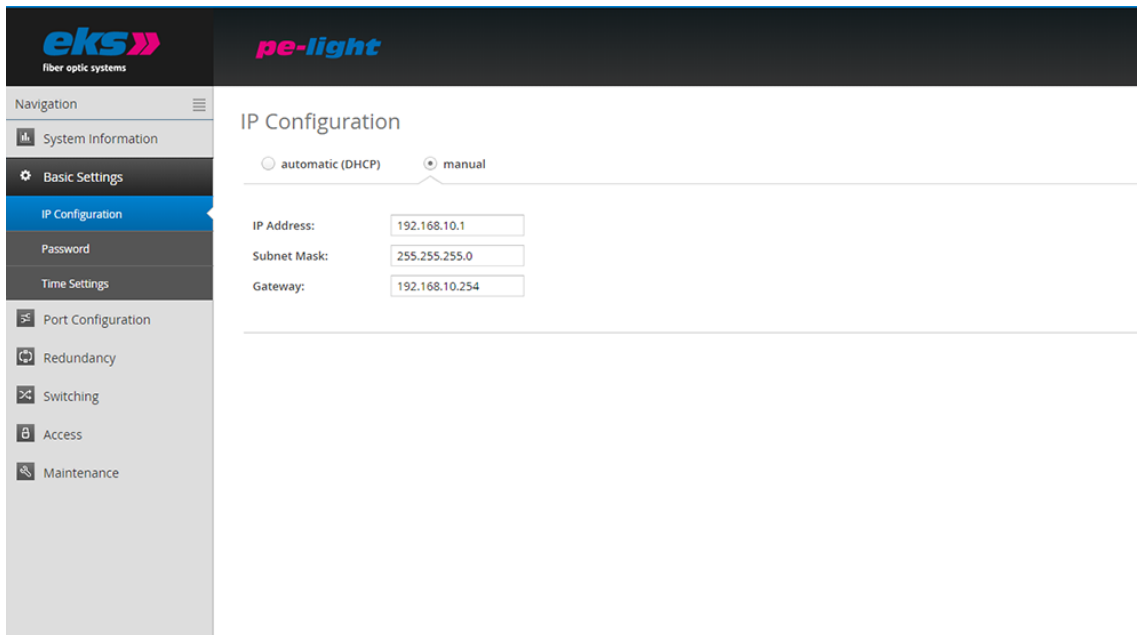


Figure 12: Changes to the IP configuration

## 5.5.2 Password

On the password screen (Figure 13), the pre-set standard password for administrator and guest user can be changed. The current or former password must be known and entered. The user names and rights of the administrator and guest are specified permanently and cannot be changed.

**The following form fields are available:**

- » New password: Please enter the password specified by you in this field for the previously selected user. Please also note the instructions for providing passwords in the section below.
- » Confirm the password: To ensure that you have entered your password correctly, repeat the input in this field.
- » Current password: Please enter the password used until now, which should now be changed.

## Instructions concerning passwords

The safety of your system depends significantly on the security of your passwords. For passwords, we therefore generally recommend:

- » Do not use dictionary entries
- » Please use passwords that are as complex as possible
- » Combine letters, numbers, and special characters
- » Use lower case and capital letters
- » Your password should consist of at least eight characters
- » Do not write down the passwords

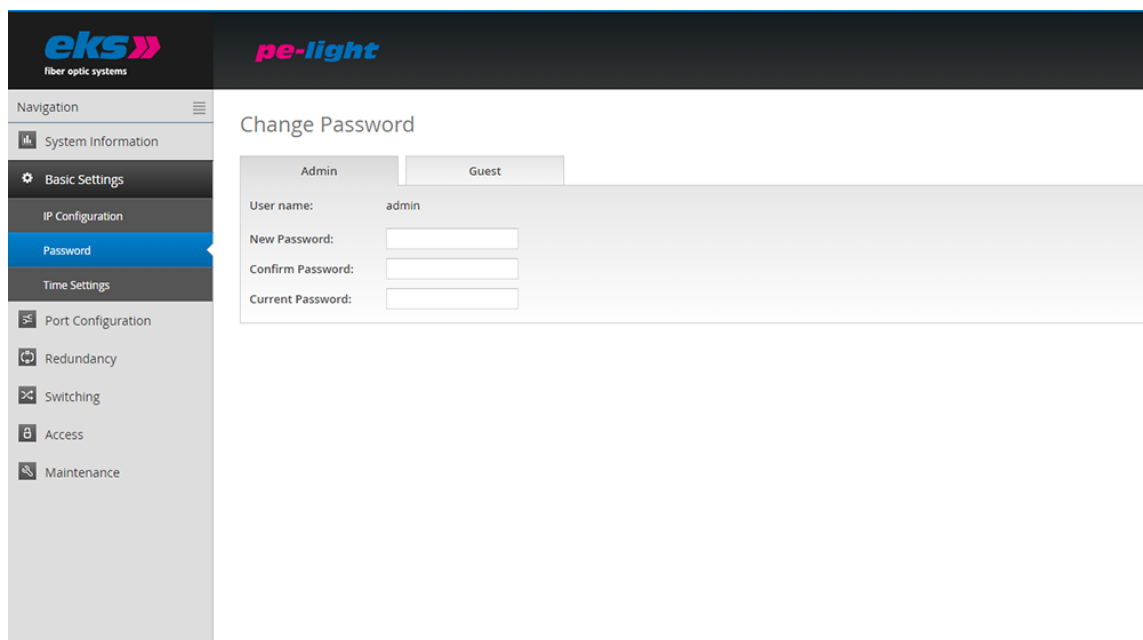


Figure 13: Change the password for administrator and guest access

### 5.5.3 Time setting

The status bar in the top area of the screen for setting the time (Figure 14) displays the system time and the date. The device running time is featured in the center. The far right features the currently applied settings for the time zone and any possible offset due to daylight savings.

When setting the date and time, select between the use of a time server and manual configuration.

The automatic configuration of the system time via Simple Network Time protocol (SNTP) has the advantage that the time setting is updated in regular intervals. An exact system time is especially important if the log file should be evaluated in case of a fault.

## Set system time automatically via SNTP

In order to set the system time via SNTP, a connection to an SNTP server on the Internet is necessary. The following settings are required when using SNTP:

- » SNTP server IP address: Enter the IP address of a time server that can be reached on the Internet or locally. Please use the decimal point format.
- » SNTP server IP address (redundancy): In this field, you may enter the IP address of a second, redundant time server. If the first server is not available, then the time will be synchronized via this SNTP server.
- » Update interval: Please enter the time intervals at which the device should synchronize with the time server. Note that the system time may possibly deviate severely from the real time in case of large time spans.
- » Time zone: Please enter the time zone where the device is located.

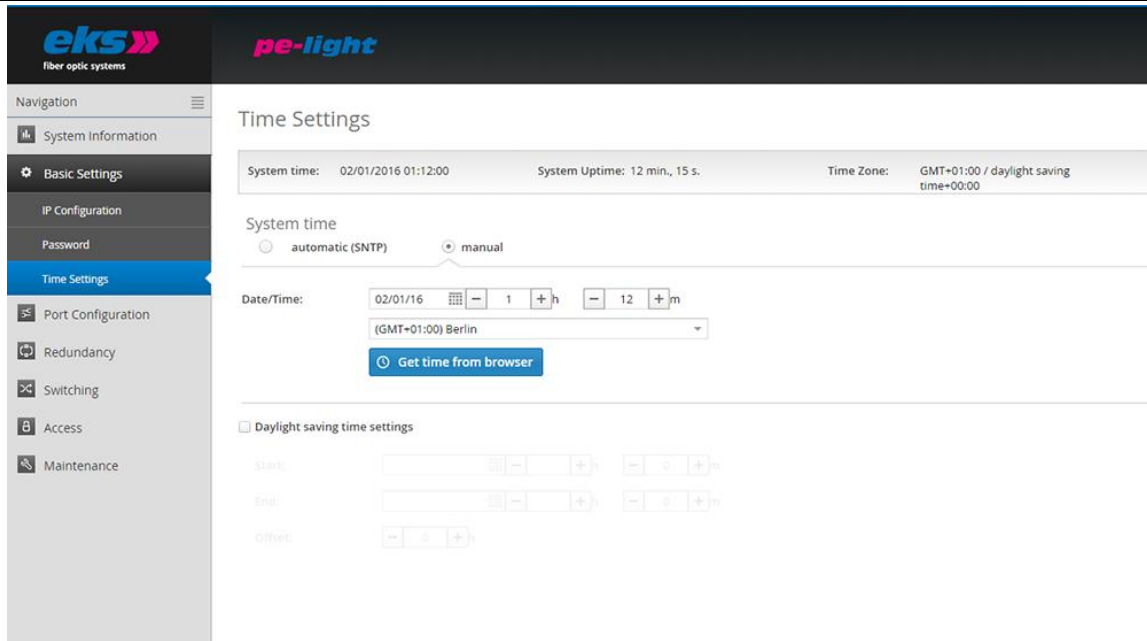
## Set the system time by hand

If the system time is set by hand, then you have the option of using the browser time or entering the time and the date by hand and saving this.

To use the browser time, press the use browser time button, check the correct date/time, save the correct date/time and save the values with the apply button.

If you want to set the date by hand, select the current date first via the input field. You can also enter the date with the help of the keyboard: first two digits for the month, then two for the day, and finally two or four digits for the year. Enter the time and the corresponding time zone and check if everything has been accepted correctly. Save the settings using the apply button.





**Figure 14: Time settings configuration**

### Daylight savings settings

If you would like to use the automatic changeover between winter and daylight savings time, activate the daylight savings time option.

- Beginning: Define the date and time when summer daylight savings should start.
- End: Define the date and time that summer daylight savings should end and the time to change to normal time again.
- Offset: Please enter the time offset between summer daylight savings and the standard time.

## 5.6 Port configuration

The table for the port configuration (Figure 15) provides an overview of the current configuration of the individual ports. The columns Enabled, Auto Negotiation, and Flow Control may also be configured. The remaining fields are partially changed by configuring the ports and updated by reloading the screen.

Port	Type	Enabled	Status	Auto Negotiation			MDI(X)	Flow control	Description
				Enabled	Speed	Duplex			
1	M12	<input checked="" type="checkbox"/>	Green	<input checked="" type="checkbox"/>	1000 mbps	full	AUTO ...	<input type="checkbox"/>	TX-Port 1
2	M12	<input checked="" type="checkbox"/>	Red	<input checked="" type="checkbox"/>	10 mbps	half	AUTO ...	<input type="checkbox"/>	TX-Port 2
3	M12	<input checked="" type="checkbox"/>	Red	<input checked="" type="checkbox"/>	1000 mbps	half	MDI	<input type="checkbox"/>	TX-Port 3
4	M12	<input checked="" type="checkbox"/>	Red	<input checked="" type="checkbox"/>	1000 mbps	half	MDI	<input type="checkbox"/>	TX-Port 4
5	Optical	<input checked="" type="checkbox"/>	Grey		1000 mbps	full		<input type="checkbox"/>	FX-Port 5
6	Optical	<input checked="" type="checkbox"/>	Grey		1000 mbps	full		<input type="checkbox"/>	FX-Port 6

Figure 15: Overview of the port configuration table

The following columns are displayed:

- » Port: Indicates the port number, which is also labeled on the enclosure (P1 to P6).
- » Type: Indicates via the symbol, if the port is a M12 port or an optical port.
- » Enabled: The individual ports can be activated or deactivated here. This specifies whether a port is able to be used or not.
- » Status: Status signals the current status of the ports:
  - Green: The port is activated and a connection is present.
  - Red: The port is activated, but there is no connection.
  - Grey: The port is deactivated. A connection is not possible.
  - Green/yellow: The LWL port is active and a connection is present. The Fiber connection should be checked.
- » Auto Negotiation: If this function is activated, the configuration of transfer speed and duplex

mode via the *pe-light-S-switch* and the connected recipient will take place automatically. If Auto Negotiation is deactivated, then the settings can be set manually, and the communicating devices must work with these settings:

- Speed: The data rate of the ports can be assigned permanently. The option of setting a data rate 10 mbps, 100mbps or 1000 mbps is possible.
- Duplex: Duplex modus can be switched between half and full duplex. This setting is therefore specified permanently for a connection and can only be applied to M12 sockets.

**Note:** If both link partners use Auto Negotiation, then it cannot be guaranteed that the link partners will settle on 1000 mbps full duplex. There will also be a duplex mismatch with output impairment if one link partner uses Auto Negotiation and the other is set permanently to 1000 mbps. We recommend setting link partners permanently to one speed and one duplex mode.

- MDI(X): The *pe-light-S-switch* can complete an auto-crossover by default. This means that the switch independently recognizes whether a subscriber is connected via a crossed or uncrossed cable.
- Flow control: The flow control ensures that overloading at a port signals to the opposite subscriber that it should send slower. If QoS (Quality of Service) is used, then the flow control should be deactivated.
- Description: You can give the ports a name in this column. The names are displayed during the complete configuration and are used for selection of the correct settings and diagnosis in case of an error. The port descriptions can be edited directly in the row where they are displayed.

### 5.6.1 Port Mirroring

Port Mirroring (Figure 16) is a method for mirroring the data traffic of one port in a network (source) on a second port (target) in order to analyze it. Either only sent or sent and received packets can be mirrored. The following settings are possible:

- Port and port name: All of the ports are displayed here in order to select a target and one or multiple source ports.
- Target port: If port mirroring is active, then the port can be selected here to which the data should be duplicated.
- The source port indicates from which ports sent (TX) or sent and received (TX and RX) data packets should be forwarded to the target port.

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

**Note:**

Deactivate port mirroring in normal mode and only apply it for problem analysis.

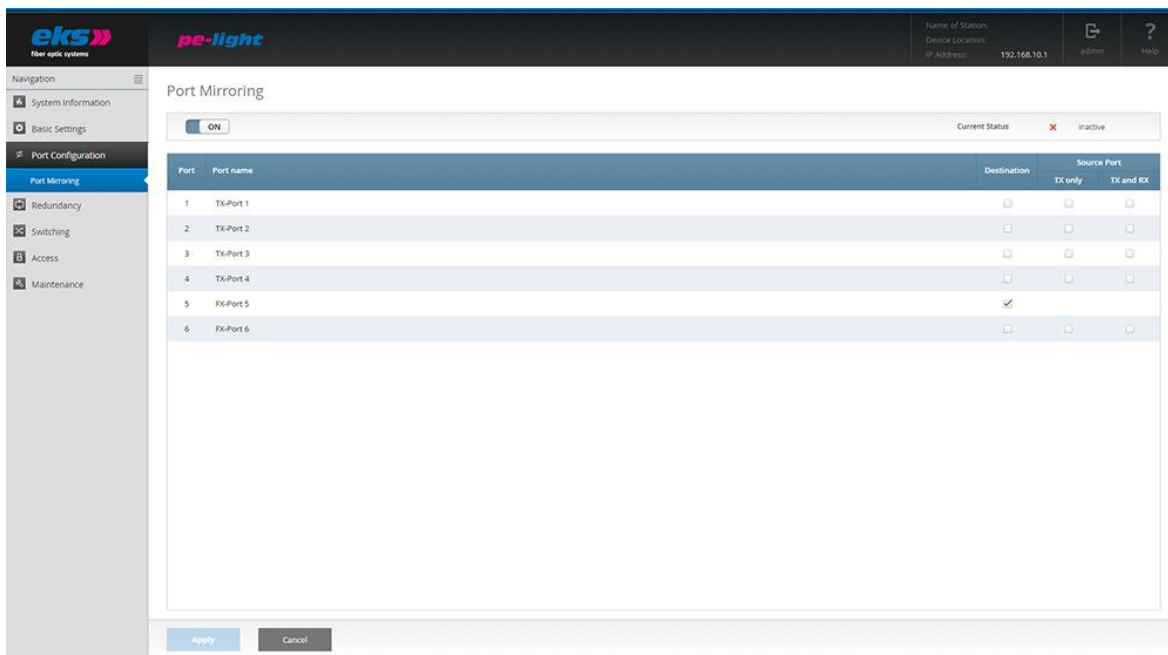


Figure 16: Port Mirroring

## 5.7 Redundancy

The redundancy screen offers an overview of the available redundancy protocols and their status. It isn't possible to activate multiple redundancy protocols at the same time. The edit button can be used to access the protocols, where the configuration can be made.

The following protocols are available:

- » MRP: Media Redundancy Protocol
- » RSTP: Rapid Spanning Tree Protocol

Use of the redundancy protocols guarantees your network increased failure security and availability in case of faults.

### 5.7.1 Media Redundancy Protocol (MRP)

The Media Redundancy Protocol (Figure 17) is a ring protocol for highly available networks. The MRP switches form a ring via the two respective dedicated ports. Exactly one switch in the ring is configured as a redundancy manager. This redundancy manager uses special test packets to test the flow capacity of the ring and establishes a redundant connection if the ring is interrupted by a fault.

The guaranteed reconfiguration time for up to 50 devices in the ring is 200 ms. In a typical application, the reconfiguration time normally is less than 50 ms.

**Attention!** The ring may only physically be closed if MRP is configured completely.

#### Ring configuration

The following settings are required for MRP:

- First ring port: Please select a port that should work as the primary ring port.
- Second ring port: Specify a second port that should work as the secondary ring port. Please note that the secondary ring port cannot simultaneously function as the primary ring port.
- Ring Settings: Please specify whether the *pe-light-S-switch* should act as manager or client. Please note that only one manager can be used for each ring.

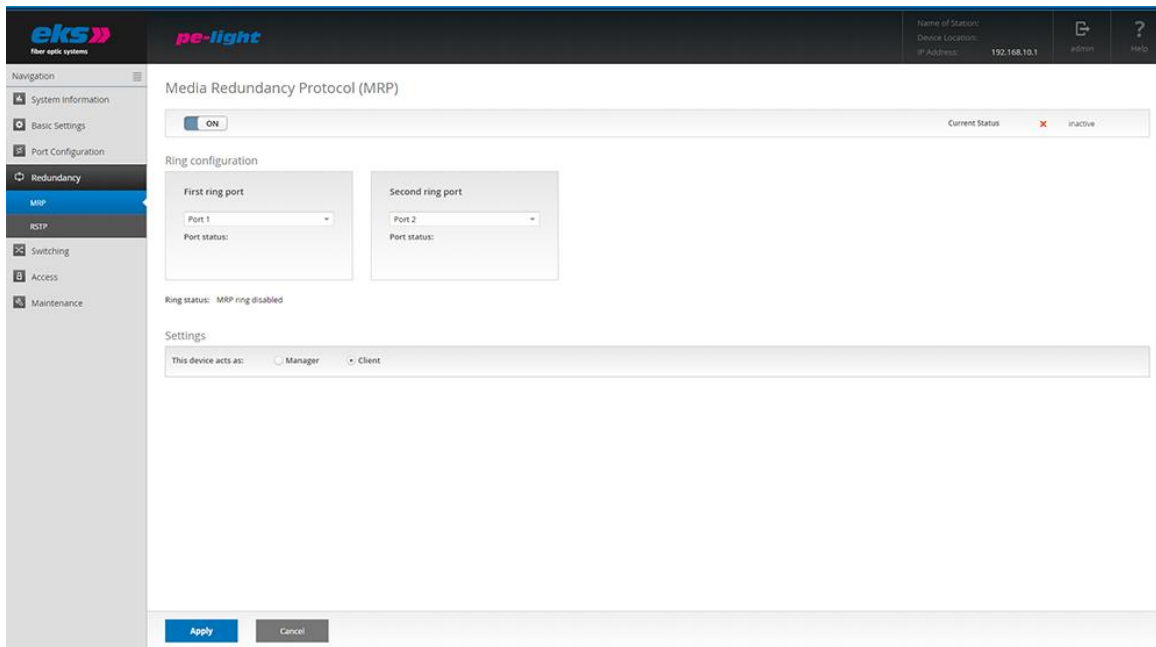
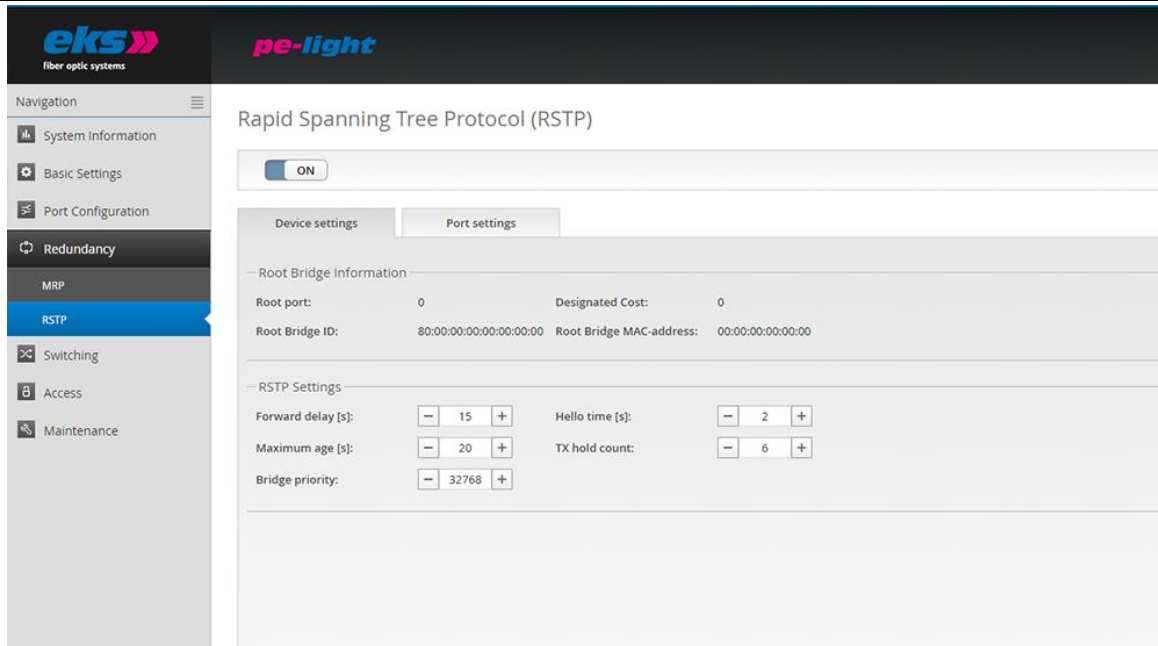


Figure 17: Media Redundancy protocol (MRP)

## 5.7.2 Rapid Spanning Tree Protocol (RSTP)

The Rapid Spanning Tree Protocol (RSTP) (Figure 18 and Figure 19) is a standardized method that can be used to establish network structures including a ring. The protocol breaks the network into a logical tree and deactivates redundant paths or activates them as required. The first step is to select a root bridge, which depicts the root of the tree to be created. Starting from the root bridge, the path to all of the other bridges in the network is specified. The paths that can be used for communication are detected via the path costs of the individual bridges.

### Device settings



**Figure 18: Rapid Spanning Tree Protocol – device settings**

## Root Bridge Information

The following parameters are displayed in this field:

- Root port: Shows which port works as the root port, i.e. the connection with the lowest path costs to the root bridge.
- Root bridge ID: The bridge ID is a combination of bridge priority and MAC address of a bridge. The bridge with the lowest bridge ID is selected as the root bridge. The Root bridge ID is the bridge ID of the selected root bridge.
- Designated cost: Path costs for root bridge
- Root bridge MAC address: Displays the MAC address of the root bridge.

## RSTP settings

In order to discover the RSTP tree, every port of the switch completes a process involving the port states before the ports transfer useful data. The time span that the ports remain in the individual states are specified by timers. Under RSTP settings, the following can be adjusted:

- » Forward Delay: The waiting time before a port switches from the status Learning/Listening (still no transfer of useful data) to Forwarding (transfer of useful data). A time between 4 s and 30 s can be entered. The basic setting features a forward delay of 15 s.
- » Maximum Age: The time that a bridge waits before attempting a new configuration if it does not receive messages from the Spanning Tree configuration protocol. A time between 6 s and 40 s can be entered. In the basic setting, the Maximum Age is equal to 20 seconds.
- » Bridge Priority: This value is used to specify the root bridge. The bridge with the lowest value is selected as the root bridge. The value must be between 0 and 61440 and a multiple of 4096. Changes to this value require a switch restart.
- » Hello Time: The time in which the switch sends a BPDU packet (Bridge Protocol Data Unit) to check the current status of the RSTP. A time between 1 s and 10 s can be entered. The basic setting for the Hello Time is 2 s.
- » TX Hold Count: The maximum number of hello packets of an interval transferred. Between 1 and 10 packets can be selected. In the basic setting, the TX Hold Count is set to 3.

**Note:** Observe the following rules to configure the forward delay, maximum age, and hello time:

$$2 * (\text{Forward Delay Time} - 1) \geq \text{Maximum age} \geq 2 * (\text{Hello Time} + 1).$$

Recommended approach: Select a value for the "Hello Time" and calculate using the formula  $2 * (\text{Hello Time} + 1)$  according to the rule indicated above to determine the lower limit for the Maximum Age. Select a value for the "Forward Delay Time" and calculate using the formula  $2 * (\text{Forward Delay Time} - 1)$  according to the rule indicated above to determine the upper limit for the Maximum Age. Select a maximum age between 6 and 40 seconds between the calculated limits.

After clicking apply, the RSTP protocol reconfigures itself and indicates any possibly changed root bridge parameters in the top part of the screen.



## 5.7.2.1.1 Port settings

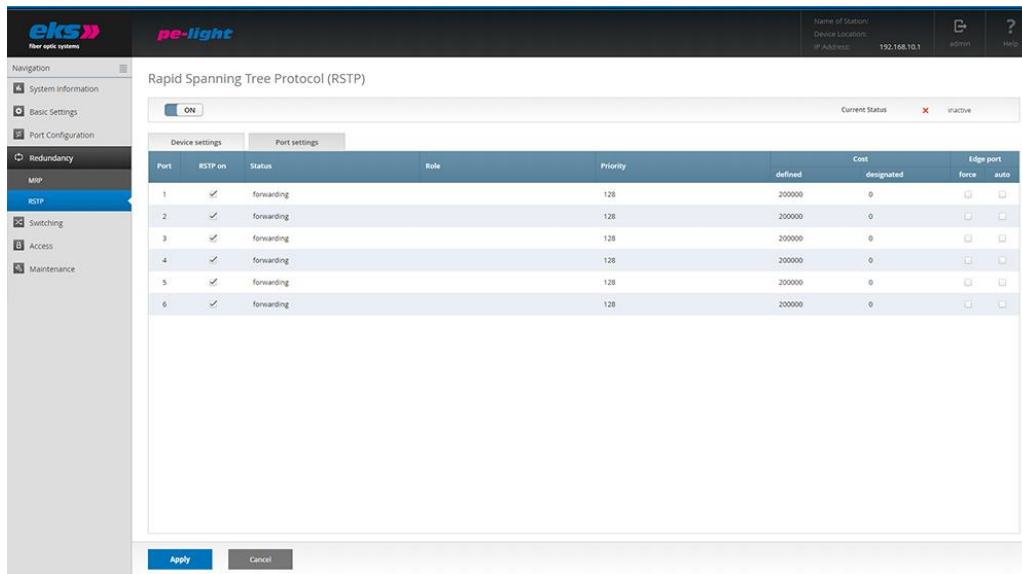


Figure 19: Rapid Spanning Tree Protocol – port settings

The port settings screen tab enables the following settings to be made:

- Port: Displays the port number.
- RSTP on: RSTP can be activated or deactivated for each port.
- Status: This column displays the status of the individual ports. This is differentiated between:
  - Blocking: Discards packets; does not learn addresses; does not receive and processes BPDUs (Bridge Protocol Data Units = RSTP protocol packets)
  - Listening: Discards packets; does not learn addresses; receives, processes, and transfers BPDUs
  - Learning: Discards packets; learns addresses; receives, processes, and transfers BPDUs
  - Forwarding: Forwards packets; learns addresses; receives, processes, and transfers BPDUs
  - Disabled: Discards packets; does not learn addresses; does not receive and process BPDUs
- Role: Each port is able to run in one of the following modes:
  - Root Port: A port in the forwarding state that was selected for the best tree structure.
  - Designated Port: A port in the forwarding state that has been selected for any switched LAN segment.

- Alternative Port: An alternative port to the root bridge that is also available in addition to the current root port.
- Backup Port: A reserve path that is provided via a designated port in the direction of the branches of the tree structure.
- Deactivated Port: A port that does not have any operating function in the tree structure.
- » Priority: Decides which port is treated with priority if the path costs to multiple ports are the same. Priority must be a multiple of 16 between 0 and 240.
- » Costs: The path costs from this bridge to the opposite bridge. The costs can be between 1 and 200,000,000.
  - Defined: The costs of the connection to the root bridge can be specified to include cable lengths or maximum data rates.
  - Designed: Calculated path costs.
- » Edge port: Indicates a port that is connected directly with an end station. These ports cannot cause loops and therefore immediately change to forwarding mode. The status change of an edge port will not lead to a change in the topology.
  - Force: The port is configured by default as an edge port.
  - Auto: The configuration as edge port takes place automatically.

After setting the RSTP parameters, these must be saved by clicking the apply button.

## 5.8 Switching

The switching screen offers an overview of activated and deactivated functions in the switching area.

**Aging Time:** This indicates the period of time during which a MAC address remains after removal from the port or switching of the device. You can select values between 16 and 4080 seconds in steps of 16 seconds. The default value is 304 seconds.

### 5.8.1 IGMP Snooping

The Internet Group Management Protocol (IGMP) is used by switches, routers, and hosts to set up multi-cast groups. If IGMP is activated, multi-cast data traffic does not need to be sent to every individual multi-cast receiver, but rather only to each group. This severely reduces the network load.

IGMP snooping works on Layer 3 of the OSI model and is extended by the Layer 2 protocol IGMP snooping (Figure 20). IGMP snooping listens to the IGMP data traffic and learns via which ports the multi-cast data must be sent.

#### IGMP snooping settings

The following settings are displayed and can be adjusted:

- » VLAN ID: IGMP snooping operates on VLAN basis and can be activated for each individual VLAN ID.
- » Fast Leaver: If a multi-cast group should be removed, then there usually is a query, whether no subscriber is really available in the group (query message). Fast Leaver is a port that removes a multi-cast group without any additional query. This setting is interesting for ports that are only connected with one multi-cast receiver.
- » Learned Ports: Shows which ports are connected with multi-cast receivers and which ports should be forwarded to the corresponding multi-cast data.
- » Static Ports: Freely configurable ports that should always receive multi-cast data independent of IGMP messages.
- » VLAN name: The name of VLANs.

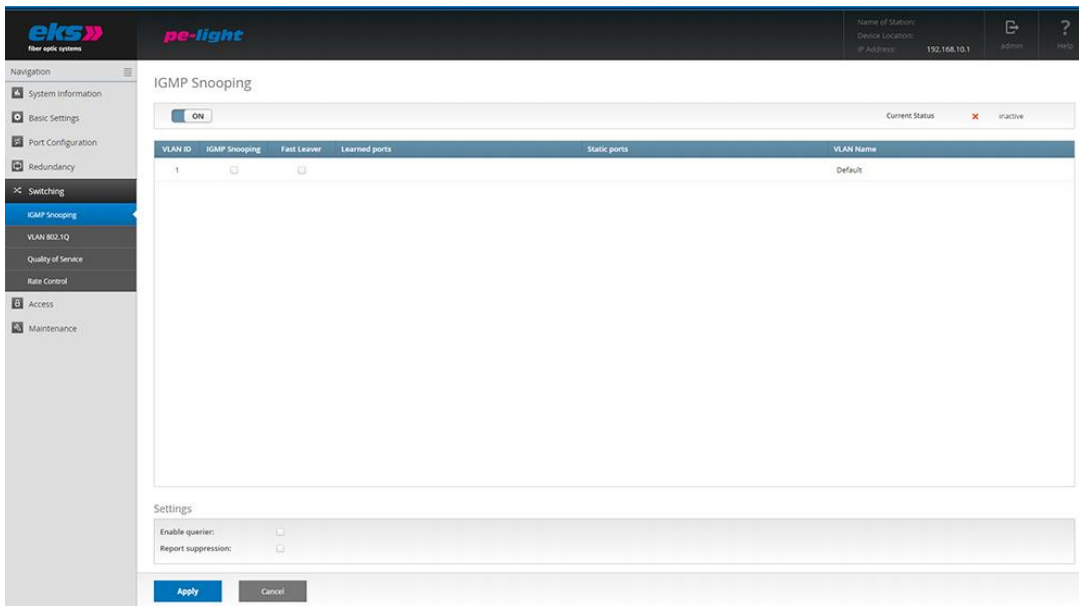


Figure 20: IGMP Snooping

### Additional Settings

- ▶ Activate querier: If no multi-cast router is present in the VLAN and the IGMP queries are sent, you can configure here that query packets should be created from this switch.
- ▶ Suppress report: If receivers join multi-cast groups or leave them, then they transfer status reports to the IGMP protocol. This status data can be bundled by the IGMP snooping protocol by activating "suppress report". By limiting the necessary reports, the network load is reduced.

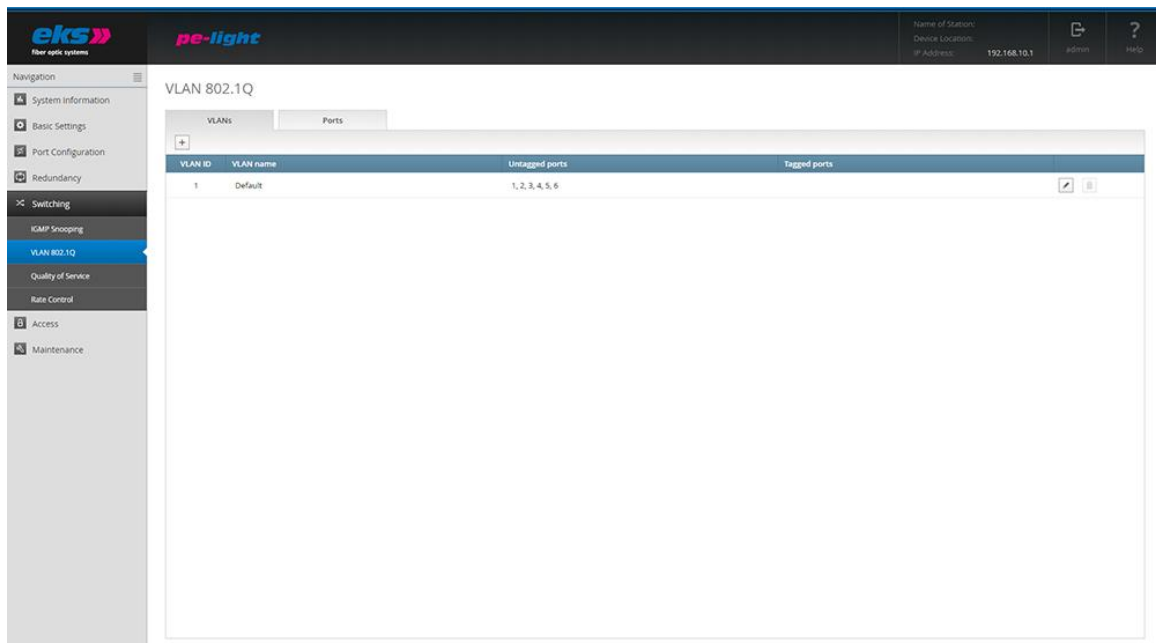
### 5.8.2 VLAN 802.1Q

A virtual LAN (VLAN) is a group of ports that may be somewhere in the network, but communicate as if they were in the same area. VLANs can be used to separate departments (R&D, marketing), applications (e.g. E-mail), or multi-cast groups for video transfers, which thereby simplifies network management.

In case of VLAN as per 802.1Q, Ethernet-data packet feature a VLAN tag, an extension, that includes a VLAN-ID, a clear number for the VLAN that the data packet belongs to. Which ports should send data Packets of VLAN with a VLAN tag and which ports should send data packets of a VLAN without a VLAN tag can be configured comfortably in the VLAN web interface menu (Figure 21). In addition

to this, VLANs are added using the “+” buttons or the following settings can be changed via editing with the edit button:

- VLAN ID: This identification number is clearly assigned to a VLAN. VLAN IDs between 1 and 4094 are possible.
- VLAN name: Any name for the VLAN.
- VLAN packets are sent to untagged ports without a VLAN tag.
- VLAN packets are sent to tagged ports with a VLAN tag.



**Figure 21: VLAN 802.1Q**

Use the delete button to remove any VLANs except for the default VLAN (VLAN ID 1).

## Use of VLANs as per VLAN 802.1Q

If data packets that do not include a VLAN tag are received by a port, then they receive the VLAN-ID of the VLAN for internal processing that is configured as the untagged receiver port. Each port may therefore be configured as untagged for a VLAN. If data packets are received that contain a VLAN tag, then these are discarded if their VLAN-ID does not correspond with the default VLAN-ID or the VLAN-ID of a VLAN that is assigned to the receiving location tagged or untagged.

All incoming data packets therefore possess a VLAN-ID internally. This internal VLAN-ID determines which ports the data packets are exported on. The data of the default VLAN is sent to all ports, while the data of other VLANs are only sent to ports that are assigned to the VLAN with the VLAN-ID of the data packets.

If the data packets are sent with or without a VLAN tag is decided by the type of port assignment to the VLAN. If a port is assigned to a VLAN tagged, then data packets are sent with the VLAN-ID of the VLAN on the corresponding port with a VLAN tag. If the VLAN is assigned untagged, then the packets are sent on the port without a VLAN tag.

**Attention!** Packets of the default VLAN are sent to all ports. The default VLAN should therefore be used for management packets. Ports without a VLAN assignment must be assigned to a VLAN that is not used so that packets that are received on these ports are not able to enter the default VLAN.

**Attention!** Packets with the VLAN tag 1 are received on all ports and output to all ports.

### 5.8.3 Quality of Service (QoS)

Quality of Service (Figure 22) influences the data traffic in the switch so that services are available to the receiver with a specified quality. In addition to this, data packets are sorted depending on different priority processes (port-based, class of service, type of service) into four priority queues, which are emptied at the exit corresponding with a priority mode (strictly and weighted).

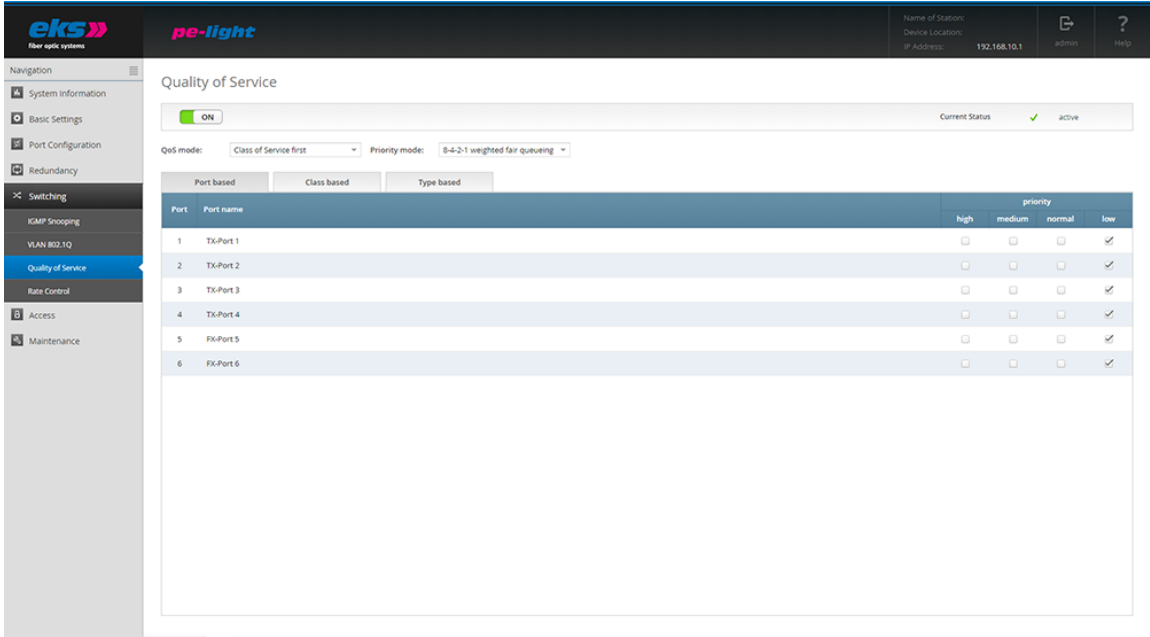


Figure 22: Quality of Service

## Priority process

The following priority processes can be selected:

- » Port-based only: The priority takes place exclusively based on the port priority.
- » Class of Service (CoS) only: The priority takes place based on the CoS fields in the VLAN tag of the data packets. Non VLAN packets are guided to the priority queue with the lowest priority.
- » Type of Service (ToS) only: The priority takes place based on the ToS fields in the IP header of the IP data packets. Packets without ToS field or non-IP packets are guided into the priority queue with the lowest priority.
- » Class of Service first: Packets with COS information in the VLAN tag are prioritized after this. Packets without CoS information are prioritized according to the ToS field in the IP header or according to port priority in case of a missing ToS field.
- » Type of Service first: Packets with ToS field in the IP header are prioritized after this. Packets without ToS information are prioritized according to the CoS field in the VLAN tag or according to port priority in case of a missing VLAN tag.

## Output: Priority mode

- » Strict priority diagram: In case of a strict priority diagram, all of the packets from the higher priority queue are sent first, and then packets from the next lower priority queue are sent.
- » 8-4-2-1 weighted sequence: After 8 packets in the highest priority queue have been sent, 4 packets in the second-highest, 2 packets in the third-highest, and 1 packet in the lowest priority queue will be sent. This approach avoids extreme waiting times for packets with the lowest priority.

<p><b>Note:</b> If Quality of Service is used, the flow control must be switched off, since activated flow control will transfer data packets throttled and independent of the priority (see section 5.6).</p>
--



## Rate Control

The rate control feature (Figure 23) can be used to limit different types of packets to an adjustable data rate. This can be used, for example, to ensure that an excessive number of broadcast packets (packets that are sent to all subscribers) do not disturb the normal Unicast data traffic (packets that are only sent to one subscriber).

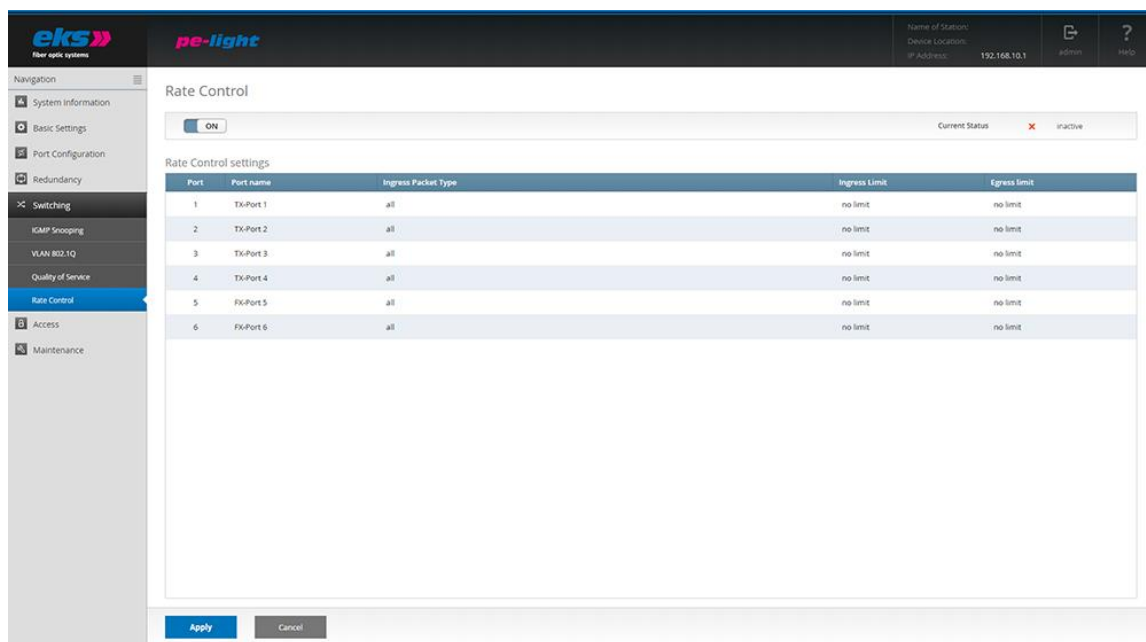


Figure 23: Rate Control settings

The following settings can be made:

- Port: Indicates the port number.
- Type of incoming packets: Indicates which types of data packets should be limited:
  - All: All packets are limited.
  - Broadcasts: Only broadcast packets are limited.
  - Multi-casts: Only multi-cast packets (packets to receiver groups) are limited.
  - Unknown Unicasts: Only Unicast packets from unknown receivers are limited.
- Limit incoming packets: The data rate limits of incoming data. 128 kbps, 256 kbps, 512 kbps, 1 mbps, 2 mbps, 4 mbps and 8 mbps are possible. "No limit" is defined as a standard value.
- Limit outgoing packets: The data rates limits for outgoing packets. These always relate to all

packet types. 128 kbps, 256 kbps, 512 kbps, 1 mbps, 2 mbps, 4 mbps and 8 mbps are possible.

"No limit" is defined as a standard value.

The desired settings can be saved by pressing the apply button.

## 5.9 Access

The access menu item (Figure 24) is used to specify the paths that will be used to access the *pe-light-S-switch*.

- **Ping:** In order to check if the device is available in your network, you can send queries to the device, which will send a response. The responses to these ping packets are suppressed if you deactivate ping under access.
- **Device Identifier:** To identify a specific device in a network, the status LEDs of the device (PWR, Fail, Door Contact) will flash with a frequency of 1 Hz for 30 seconds.

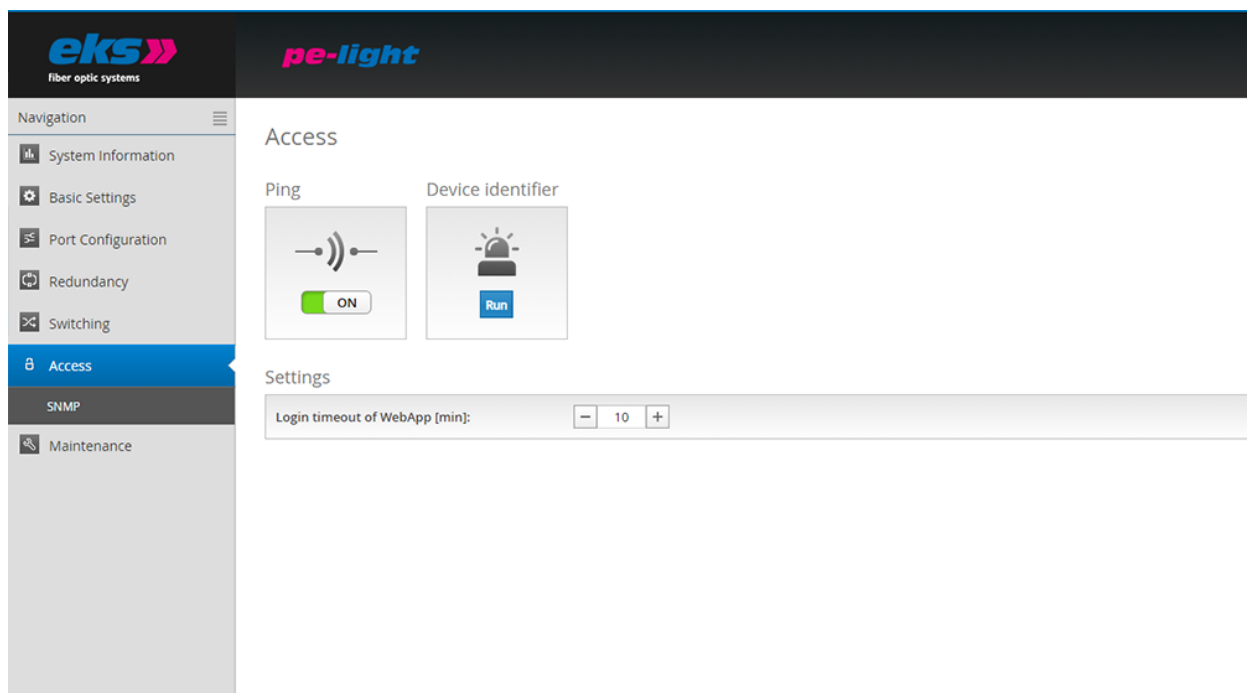


Figure 24: Selection of access options

### Settings

The time until automatic logout specifies how long a session remains in the web management without activity until an automatic logout takes place. The time can be configured between 3 minutes and 30 minutes.

The apply button can be used to save the settings.

### 5.9.1 Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) is used to monitor and control network elements via a central station. Which settings in a network element can be changed and which values can be queried is not defined in the SNMP, but rather in the so-called MIBs (Management Information Base). In addition to several generally applicable MIBs, most of the devices also feature manufacturer-specific MIBs with device-specific information.

SNMP queries are sent from the management station with a so-called community string, which represents a simple access limit. Responses are only provided for queries featuring a community string that matches a community string that is defined in the switch. Because the community string is sent in plain text via the network, its use does not necessarily increase the security.

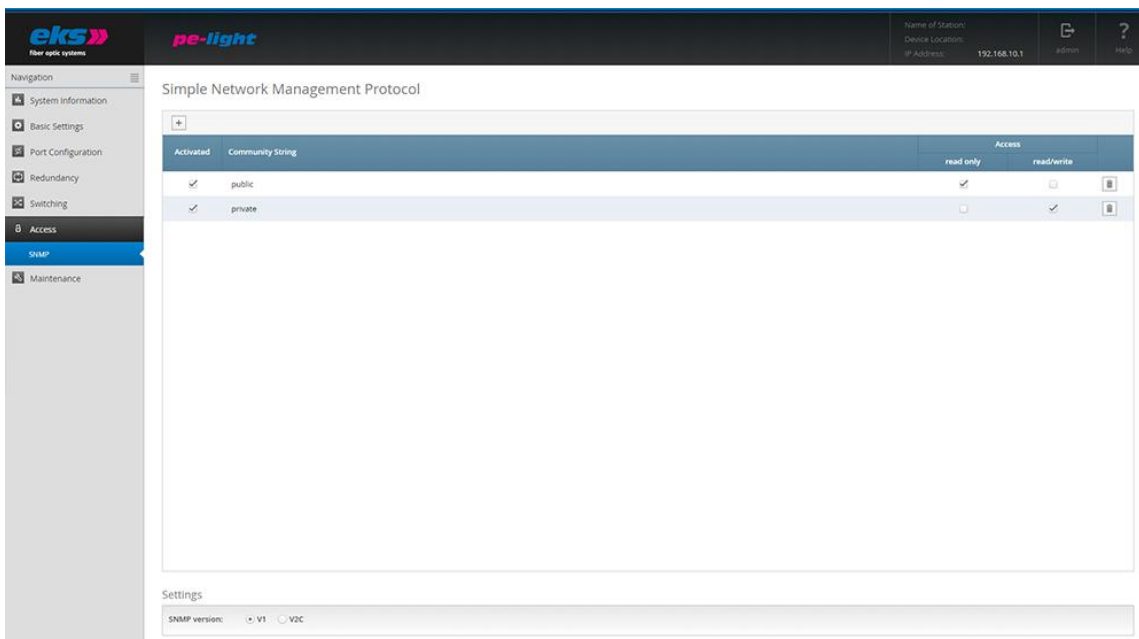



Figure 25: Overview of currently available SNMP accesses

	<h1>Software Operating Manual</h1>	MAN_pe-light-S-switch
		Version: 2021-09-13
		Authorized by: T.W.
		Page 53 of 61

## SNMP accesses

In the SNMP menu (Figure 25) of the *pe-light-S-switch*, community strings can be added, edited, or deleted. The following settings can be configured in this case:

- » Active: Shows which strings are active at which community and which are not
- » Community string: The accesses are defined via a clear name, which can be set here. A name may feature a maximum 32 characters.
- » Read only: Queries with this community string are answered, but they cannot adjust settings at the switch.
- » Read and write: Queries with this community string are answered and may adjust settings at the switch.
- » Remove: Delete the community strings

The *pe-light-S-switch* supports SNMP versions V1 and V2C. Please select the desired version.

Save the settings by clicking the "create" button.

## 5.10 Maintenance

The maintenance menu item is divided into the items backup, restore, firmware update, factory settings, and restart, which are described in the following.

### 5.10.1 Backup

This menu item offers you the option to save the current configuration of the *pe-light-S-switch* as a file. The backup can be stored via TFTP-server (Trivial File Transfer Protocol) or as download. In connection with restoring, the backup function enables you to save all settings and reload them later to the device or use the current configuration in other devices.

The device creates a file with all settings. You have to store this file and can load it again to the device with the restore function.

In order to save the configuration via TFTP, a TFTP server must be set up on a computer in the network. Various TFTP server programs are available for download as freeware on the Internet.

#### Settings TFTP

» TFTP Server IP address: IP address of the TFTP server available in the network in decimal point notation.

#### Settings TFTP or HTTP

» File name: File name of the switch configuration file to be saved.

If the parameters have been entered correctly, the backup can be executed by clicking on "Start backup".

### 5.10.2 Restore

This menu item is used to import a configuration that was previously saved as a backup file. It can be loaded via tftp-server or as an upload.

#### TFTP Settings

» TFTP Server IP address: IP address of the TFTP server available in the network in decimal point notation.

## Settings TFTP, or HTTP

- » Filename: The filename of the switch configuration file stored on the TFTP server.
- » Password: Specifies whether the current password settings should be retained when restoring the configuration or whether they should be overwritten with the settings from the configuration file.
- » IP configuration: Specifies whether the currently set IP address, subnet mask and gate way should be retained or overwritten with the settings from the configuration file.

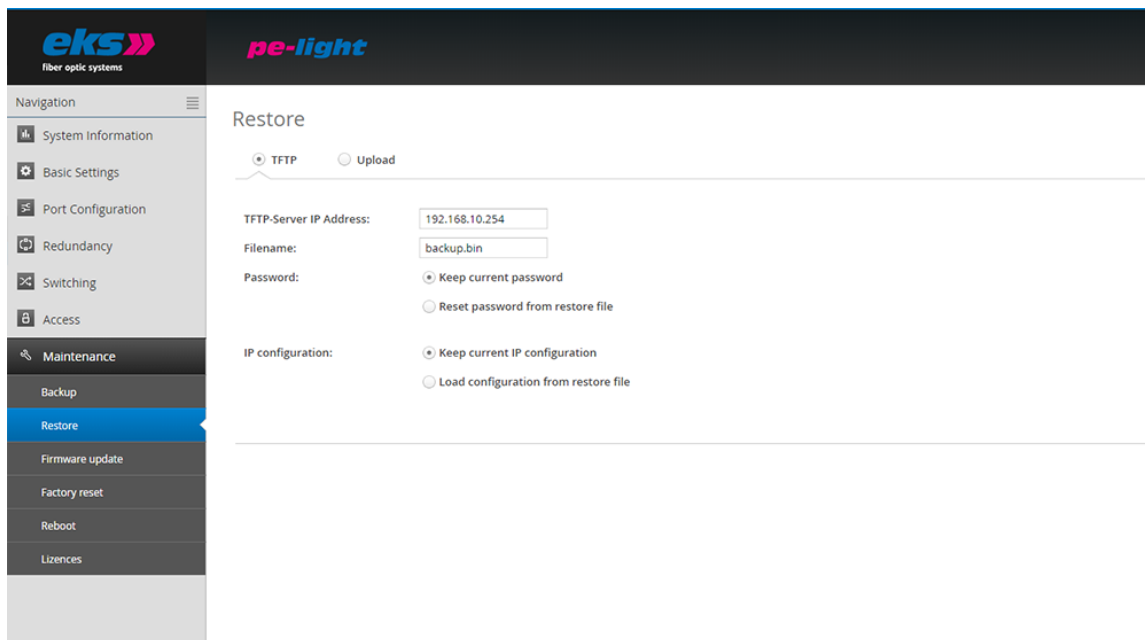


Figure 26: Settings for restoring a configuration

Press the button "Start restore" to start the restore process. Doublecheck the settings in the popup window and confirm to reload the settings. After the process is done the device will reboot.

### 5.10.3 Firmware update

The menu item firmware update can be used to update the firmware of the *pe-light-S-switch*. Please only use firmware versions that are released by eks Engel FOS GmbH & Co. KG and have been developed for the devices of the *pe-light-S-switch* series. Before starting the update process, it is important to stop the redundancy protocols and to open the MRP ring. The device can get the new firmware by downloading it from a TFTP-Server, which is accessible in the network. With the option upload it is possible to use a firmware which is stored on the computer or server in your network and store it on the *pe-light-S-switch*.

**Attention!** Please do not complete this action if you have not been authorized to do so by the manufacturer beforehand. This function should only be used if problems occur that can only be corrected by changing the device software. For this reason, you will only receive new or changed firmware if the manufacturer considers it to be necessary.

### Update via TFTP-Server

To update the firmware by using a TFTP-Server, the new firmware file has to be stored in the TFTP-Server root directory. Please write down the name of the file or remember it. Now open the web interface of the *pe-light-S-switch* and choose Firmware update over TFTP. Insert the IP-Address (Version 4) of the TFTP-Server in the field "TFTP-Server IP Address" and the name of the firmware file in the field filename. Press the button "Start Firmware update" to install the new firmware on the device.

### Update via Upload

Press the button "select file" and a new window will open and show you the content of your computer. Select the firmware file and press the button open, to upload the file to the *pe-light-S-switch*. The upload of the firmware file will start and you can see the progress status. When the upload has finished the progress window will close and you can check the name of the uploaded file in the field Filename. Press the button "Start Firmware update" to install the new firmware on the device.

**Attention.** Please follow these rules during the firmware update:


- » Do not disconnect the device from the supply voltage.
- » Do not disconnect or replace any network connections.

During the update, a progress display appears in the web interface. As soon as the update is completed, the *pe-light-S-switch* will restart.

## 5.10.4 Factory settings

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



	<h1>Software Operating Manual</h1>	MAN_pe-light-S-switch
		Version: 2021-09-13
		Authorized by: T.W.
		Page 57 of 61

### Settings:

- » Password: Specifies whether the password settings should be maintained if the configuration is reset or if they should be overwritten with the factory settings.
- » IP configuration: Specifies whether the IP address, subnet mask, and gateway should be maintained or if they should be overwritten with the factory settings.

By clicking the "Set factory settings" button, the *pe-light-S-switch* is reset.

### 5.10.5 Reboot

A reboot or software reset can be executed here. By clicking the reboot button, the switch's program is stopped and the device is rebooted.

### 5.10.6 Licenses

#### Manufacturer information

Get in contact with the eks Engel FOS GmbH & Co. KG as manufacturer of the *pe-light-S-switch* if you have serious problems during the configuration of the switch, or if you have questions to which you don't get an answer in the data sheet or in the manual. Read the chapter in the help text of the device and the manual before you get in contact with our support.

#### User manual

With this link you can download or open the manual of the *pe-light-S-switch* in the portable document format (\*.pdf). To read the manual a pdf-viewer is necessary which you can download in the internet for free. For example, you can use the adobe acrobat reader.

#### SNMP - Management Information Base

To configure the *pe-light-S-switch*, the parameters have to be defined. The description of these parameters is done in a file called the management information base.

#### License information

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

## 6 Instructions for troubleshooting

---

- » Check the correct voltage supply. The VDC LED must be glowing green.
- » Check the link/act LEDs of the wired M12 sockets and the optical fiber cable transceiver. If the connection is established, the link LEDs will light up, and they will flash in case data is being transmitted.
- » Check the wiring of the M12 sockets. Select the correct network cable. Use "unshielded twisted pair" (UTP) or "shielded twisted pair" (STP) for M12 connections to establish the network: 100Ω category 3, 4, 5 or better cables for connections with 10 mbps or 100Ω category 5e or better cables for connections with 100 mbps or 1000 mbps. Make sure that the cables are not longer than 100 meters.
- » In case of doubt, disconnect redundant network structures and set the *pe-light-S-switch* to the factory settings. If the communication is working, enter your settings gradually and observe which settings result in the error.

## 7 Technical specifications

<b>LED display</b>	Status LEDs / port LEDs (yellow) / voltage supply (green)
<b>IEEE</b>	IEEE 802.3 10Base-T Ethernet / IEEE 802.3u 100Base-TX and 100Base-FX Fast Ethernet / IEEE802.1d spanning tree / IEEE802.1w rapid spanning tree / IEEE 802.1p class of service / IEEE802.1Q VLAN Tag
<b>Protocol</b>	CSMA/CD
<b>Management</b>	SNMP management, Web interface management
<b>SNMP MIB</b>	RFC 1213 MIBII / RFC 1493 Bridge MIB / RMON RFC 1757 / RFC 2674 VLAN MIB / RFC 1643 EtherLike-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
<b>Technology</b>	Store and forward switching architecture, Netload Class III
<b>SNMP trap</b>	Trap receiver / cold start / port link up / port link down / authentication fault / private trap for power status / port alarm configuration / fault alarm ring
<b>Transfer rate</b>	14,880 pps for 10 Base-T Ethernet port 148,800 pps for 100 Base-TX Fast Ethernet port 148,800,000 pps for 1000 Base-TX/FX Gigabit Ethernet port
<b>MAC address table</b>	2K MAC address table
<b>Packet filters</b>	4 types of packet filter rules with different packet combinations
<b>Ring</b>	2 ports for the ring in order to guarantee a recovery time below 200 ms
<b>VLAN</b>	Port-based VLAN Tagged VLAN IEEE 802.1Q
<b>Class of Service</b>	IEEE802.1p Class of Service with 4 priority queues per port
<b>Spanning Tree</b>	IEEE802.1d Spanning Tree and IEEE802.1w Rapid Spanning Tree
<b>IGMP</b>	IGMP v1 and query mode with up to 256 groups
<b>SNTP</b>	SNTP for time synchronization
<b>SMTP</b>	SMTP server and e-mail accounts for event messages
<b>Port Mirror</b>	Only TX packets or TX and RX packets
<b>Firmware Update</b>	Firmware update, TFTP backup and restore via TFTP, USB; HTTP
<b>Bandwidth control</b>	Ingress and egress with combination options
<b>DHCP Client</b>	DHCP client function to receive an IP address from the DHCP server

## 8 GPL/LGPL guarantee and liability exclusion

---

The *pe-light-S-switches* from eks Engel GmbH & Co. KG (referred to as eks in the following) also include open source software components in addition to proprietary software. The open source software is provided to you according to the conditions of the GNU General Public License (GPL) and the GNU Lesser General Public License (LGPL) free of license fees. It was written by third parties and is subject to copyright. You are entitled to use open source software according to the conditions of the GPL or LGPL. In case of a conflict between eks license conditions and the conditions of the GPL or the LGPL, the GPL and LGPL shall apply to the open source components of the software.

The GPL and LGPL licenses and additional license information are available via the following URL on the device (IP address upon delivery): <http://device-ip/download/license.txt>

If the source code of the open source software is not delivered with the *pe-light-S-switch*, then you may request it via the following e-mail address (together with the associated copyright instructions): [info@eks-engel.de](mailto:info@eks-engel.de). The source code will be sent to you for the price the of copying and delivery costs.

All source code queries must be submitted within three years after purchasing the *pe-light-S-switch*. Please include a copy of the purchase receipt with your request. Please also include the exact name of the device and the version number of the installed software.

Use of the open source software delivered with *pe-light-S-switches* in any other way with the *pe-light-S-switch* hardware shall take place at your own risk without any liability claims against eks. For more information about guarantee claims involving the authors of the open source software delivered with the *pe-light-S-switch*, we refer to the GPL and the LGPL.

We exclude all liability for damage that results from any changes completed by third parties other than eks on parts of the software or the configuration. We exclude all liability on behalf of eks if the open source software violates copyrights of third parties. In case of changes that were not made to the software by eks, we shall not provide any technical support.

## 9 Table of figures

Figure 1: <i>pe-light-2</i> in a star-shaped network	12
Figure 2: <i>pe-light-2</i> in a meshed network	13
Figure 3: <i>pe-light-2</i> in a ring-shaped network	14
Figure 4: Login Window	17
Figure 5: Status and diagnosis	18
Figure 6: Alarms/notifications: Adding an alarm trigger	21
Figure 7: Adding an alarm receiver	22
Figure 8: Port statistics	24
Figure 9: Syslog messages	25
Figure 10: Link Layer Discovery protocol (LLDP)	27
Figure 11: The basic settings of the <i>pe-light-S-switch</i>	28
Figure 12: Changes to the IP configuration	30
Figure 13: Change the password for administrator and guest access	31
Figure 14: Time settings configuration	33
Figure 15: Overview of the port configuration table	34
Figure 16: Port Mirroring	36
Figure 17: Media Redundancy protocol (MRP)	38
Figure 18: Rapid Spanning Tree Protocol – device settings	39
Figure 19: Rapid Spanning Tree Protocol – port settings	41
Figure 20: IGMP Snooping	44
Figure 21: VLAN 802.1Q	45
Figure 22: Quality of Service	47
Figure 23: Rate Control settings	49
Figure 24: Selection of access options	51
Figure 25: Overview of currently available SNMP accesses	52
Figure 26: Settings for restoring a configuration	55