pe-light-S-switch

Art.-Nr.: 0685 F412 4110 XXXX / 0686 F412 4110 XXXX

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**
Internet: **www.eks-engel.de**

Rechtliche Hinweise

Diese Anleitung enthält wichtige Anmerkungen und Warnungen, deren Nichtbeachtung zu ernsthaften Personen- oder Anlagenschäden führen kann. Bitte lesen Sie die Anleitung vor Inbetriebnahme der ***pe-light-S-switches*** aufmerksam durch. Ordnungsgemäßer Transport, korrekte Lagerung und Installation sowie sorgfältige Bedienung und Instandhaltung der ***pe-light-S-switches*** sind entscheidend für den sicheren Betrieb.

Bestimmungsgemäße Verwendung

Die Geräte der ***pe-light-S-switch*** Produktfamilie dürfen nur wie in der Anleitung beschrieben verwendet werden. Sie dürfen nur unbeschädigt und unter den angegebenen Umweltbedingungen eingesetzt werden. Die Gehäuse der ***pe-light-S-switches*** dürfen nur durch Es-Techniker geöffnet werden - in den Geräten befinden sich keine durch den Benutzer wartbaren Komponenten.

Personalanforderungen

Die Installation und Inbetriebnahme der ***pe-light-S-switch*** darf nur durch technisch geschultes Personal erfolgen, das sich mit dieser Bedienungsanleitung vertraut gemacht hat. Alle Arbeiten an elektrischen Anlagen dürfen außerdem nur durch eine Elektrofachkraft oder unter deren Leitung und Aufsicht durchgeführt werden. Anzuwendende lokale und nationale Sicherheitsbedingungen müssen jederzeit eingehalten werden.

Spannungsversorgung

Die Geräte der ***pe-light-S-switch*** Produktfamilie wurden für den Betrieb mit SELV-Spannungen durch eine LPS (Limited Power Source) designed. Sie dürfen nur durch SELV/LPS konform mit IEC 60950-1 / EN60950-1 / VDE0805-1 versorgt werden, die wiederum durch NEC Class 2 konforme Spannungsversorgungen mit Spannung versorgt werden.

Der Schirm der M12-Buchsen ist zur Ableitung von Störungen mit dem Gehäuse des ***pe-light-S-switch*** verbunden. Beachten Sie mögliche Kurzschlüsse bei Verwendung geschirmter Kabel.

Sicherheit von Lasereinrichtungen

Die Geräte der ***pe-light-S-switch*** Familie enthalten LED- oder LASER-Komponenten nach IEC 60825-1:2014: Klasse 1 Laser/LED-Produkt.

Warnung!

Nicht mit optischen Instrumenten (z.B. Linsen, Mikroskop) in den Strahl der optischen Transceiver sehen! Missachtung dieser Warnung kann zu Augenschäden führen.

Entsorgungshinweis

Die Geräte dürfen nicht über den normalen Hausmüll entsorgt werden, sondern können bei eke Engel FOS GmbH & Co. KG entsorgt werden.

WEEE-Kennzeichnung: DE 900 53 255

Vorwort

Übersicht über die *pe-light-S-switch* Produktfamillie

Die Geräte der ***pe-light-S-switch*** Produktfamilie enthalten industrielle Ethernetswitches mit Management, die über eine Web-Applikation einfach und komfortabel konfiguriert werden können. Sie ermöglichen eine kostengünstige Installation von industriellen Ethernet Bus-, Stern- und Ringstrukturen mit Switching-Funktionalität.

Merkmale

- Web Applikation zur Konfiguration
- 10BASE-T/100BASE-TX/1000BASE-TX (M12) und 1000BASE-FX (MM oder SM)
- PHY und MAC vollständig kompatibel zu IEEE 802.3, IEEE802.3u und IEEE 802.3x
- Auto MDI/MDI-X Crossover-Funktion für 10BASE-T, 100BASE-T und 1000BASE-T-Ports
- Store-and-Forward Switching Architektur mit 2048 MAC Adresstabelle
- Quality of Service (QoS) mit vier Prioritätswarteschlangen
  Priorisierung über IEEE 802.1p Class of Service (COS), Type of Service (TOS)/DiffServ oder Portpriorität
  Limitierung eingehender und ausgehender Pakete
- Port Mirror für TX oder (TX und RX) Pakete
- Port basiertes VLAN / 802.1Q Tagged VLAN
- Simple Network Time Protocol (SNTP)
- Simple Mail Transfer Protocol (SMTP) für Signalisierung von Alarmen
- Internet Gateway Management Protocol-Snooping (IGMP-Snooping)
- Dynamical Host Configuration Protocol (DHCP) Clientfunktion
- Simple Network Management Protocol (SNMP)
- Updaten, Speichern und Sichern der Systemkonfiguration über TFTP oder http
- PoE+ Unterstützung an den M12 Ports

Anmerkung:

Abhängig von der Version der programmierten Software können Geräte mit anderer Funktionalität ausgeliefert werden.

1 Inhaltsverzeichnis

Rechtliche Hinweise 2

Bestimmungsgemäße Verwendung 2

Personalanforderungen 2

Spannungsversorgung 2

Sicherheit von Lasereinrichtungen 3

Vorwort 4

Übersicht über die *pe-light-S-switch* Produktfamillie 4

Merkmale 4

1 Inhaltsverzeichnis 5

2 Hardwarebeschreibung 9

2.1 Frontansicht 9

2.2 LED Anzeigen 9

2.3 Ports 10

2.3.1 M12 Ports 10

2.3.2 Optische Ports 10

2.3.3 Verkabelung 10

3 Netzwerktopologien / Redundanz 12

3.1 Stern-Struktur 12

3.2 Vermaschte Netze 13

3.3 Ring-Struktur 14

4 Web Applikation 15

4.1 Vorbereitungen 15

4.2 System Login 16

4.3 Web-Interface 16

4.3.1 Menüleiste 17

4.3.2 Informationsleiste 17

4.4 Systeminformationen 17

4.5 Diagnose 18

4.5.1 Alarme / Meldungen 18

4.5.2 Port Statistiken 21

4.5.3 Syslog Meldungen 23

4.5.4 Link Layer Discovery Protocol – Topologie 24

4.6 Grundeinstellungen 26

4.6.1 IP-Konfiguration 26

4.6.2 Passwort 28

4.6.3 Zeiteinstellung 29

4.7 Port-Konfiguration 31

4.7.1 Port Mirroring 33

4.8 Redundanz 34

4.8.1 Media Redundancy Protocol (MRP) 34

4.8.2 Rapid Spanning Tree Protocol (RSTP) 35

4.9 Sicherheit ..... **Fehler! Textmarke nicht definiert.**

4.9.1 Radius/802.1x ..... **Fehler! Textmarke nicht definiert.**

4.10 Switching 40

4.10.1 IGMP Snooping 40

4.10.2 VLAN 802.1Q 42

4.10.3 Quality of Service (QoS) 45

4.10.4 Bandbreitenkontrolle 47

4.10.5 Forwarding Database 48

4.11 Zugriff 49

4.11.1 Simple Network Management Protocol (SNMP) 50

4.12 PoE (Power over Ethernet) 53

4.12.1 PoE Guard 55

4.12.2 PoE technische Spezifikationen 56

4.13 Wartung 56

4.13.1 Sicherung 57

4.13.2 Wiederherstellung 58

4.13.3 Firmwareupdate 59

4.13.4 Werkseinstellungen 61

4.13.5 Werksreset über den Türkontakt 61

4.13.6 Neustart 62

4.13.7 Lizenzen 62

5 Hinweise zur Fehlerbehebung 63

6 Technische Spezifikation 64

7 GPL/LGPL Garantie und Haftungsausschluss 65

8 Abbildungsverzeichnis 67

9 Tabellenverzeichnis 69

2 Hardwarebeschreibung

2.1 Frontansicht

Auf dem Frontpaneel des Switches befinden sich 3 Diagnose-LEDs. Darüber hinaus verfügt jeder der Ethernet-Ports über eine Status LED.

Abbildung 1: Frontansicht des *pe-light-S-switches*

2.2 LED Anzeigen

Die LED-Anzeigen bieten Echtzeit-Informationen über den Zustand des ***pe-light-S-switches***.

LED	Status	Bedeutung
PWR	Grün	Am Anschluss VDC liegt eine ausreichende Spannung an (48VDC)
	Aus	Es liegt keine ausreichende Spannung am Anschluss VDC an
Door Contact	Rot	Der Türkontakt ist unterbrochen
	Aus	Der Türkontakt ist geschlossen
Fail	Rot	Konfigurierter Alarm aktiv
	Aus	Keine Alarmbedingung erfüllt
LNK/ACT	Leuchten	Verbindung vorhanden
	Blinken	Senden bzw. Empfang von Paketen

LED	Status	Bedeutung
	Aus	Keine Verbindung

Tabelle 1: LED Beschreibung

2.3 Ports

2.3.1 M12 Ports

Der ***pe-light-S-switch*** verfügt über vier M12 Ports mit Übertragungsraten von jeweils 10MBit/s, 100MBit/s oder 1000MBit/s. Die Ports erkennen die Datenrate automatisch. Sende- und Empfangsleitungen werden per MDI/MDI-X Autocrossover passend gekreuzt, so dass unabhängig vom eingesetzten Kabeltyp (1:1 oder gekreuzt) Verbindungen zu anderen Geräten aufgebaut werden können.

2.3.2 Optische Ports

Der ***pe-light-S-switch*** ist mit zwei 1000Base-FX Ports ausgestattet. Je nach bestellter Variante können die LWL-Ports für verschiedene Fasertypen geeignet sein (Multimode oder Singlemode).

Bitte achten Sie darauf, dass Sie die Transceiver des ***pe-light-S-switch*** immer mit Transceivern anderer Geräte verbinden, die für die gleiche Wellenlänge und den gleichen Fasertyp geeignet sind.

Der Sender eines Gerätes muss immer mit dem Empfänger des gegenüberliegenden Gerätes verbunden werden und umgekehrt.

2.3.3 Verkabelung

- Benutzen Sie Twisted-Pair Kabel der Kategorie 5e oder besser zur Verbindung der M12 Ports. Das elektrische Verbindungskabel zwischen dem Switch und dem Verbindungspartner (Switch, Hub, Workstation, etc.) darf nicht länger als 100 Meter sein.
- Verbinden Sie Multimode-Transceiver mit 50/125µm bzw. 62,5/125µm Multimode-Lichtwellenleitern.
- Verbinden Sie Singlemode-Transceiver mit 9/125µm Singlemode-Lichtwellenleitern.

Warnung!

Montieren Sie die ***pe-light-S-switches*** nicht direkt neben Geräten, die starke elektromagnetische Störfelder erzeugen, wie z.B. Trafos, Schütze, Frequenzumrichter, etc.

Warnung!

Montieren Sie die ***pe-light-S-switches*** nicht direkt neben stark wärmeerzeugenden Geräten und schützen Sie den Switch vor direkter Sonneneinstrahlung, um eine unerwünschte Erwärmung zu vermeiden.

3 Netzwerktopologien / Redundanz

Die Geräte der ***pe-light-S-switch*** Produktfamilie können durch Verwendung verschiedener Protokolle neben dem Einsatz in sternförmigen Switched-Ethernet-Netzen auch in redundanten Netzen sowie vermaschten Netzen oder Ringen verwendet werden.

3.1 Stern-Struktur

Klassische Ethernet-Stern-Strukturen, siehe Abbildung 2, können mit den Geräten der ***pe-light-S-switch*** Produktfamilie ohne weitere Konfiguration vernetzt werden. Die Geräte sind sofort funktionsbereit.

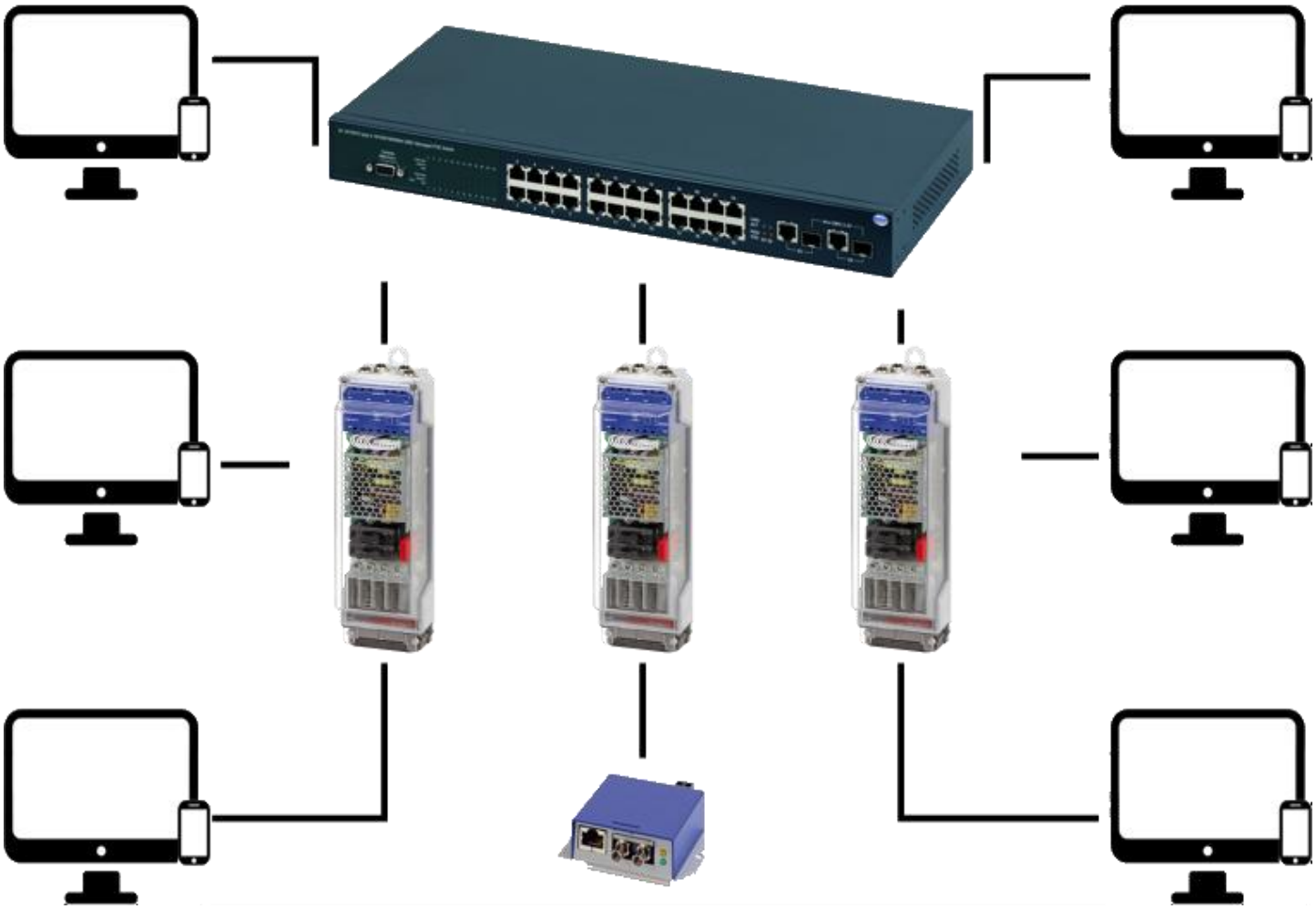


Abbildung 2: *pe-light-S* in einem sternförmigen Netzwerk

3.2 Vermaschte Netze

Durch den Einsatz des Rapid Spanning Tree Protokolls (RSTP) können beliebige Ethernet-Strukturen aufgebaut werden, beispielsweise wie in Abbildung 3, gezeigt. STP und RSTP brechen diese Strukturen in eine Baum-Struktur auf und rekonfigurieren diese Baum-Struktur bei Änderungen der Topologie. Die Rekonfigurationszeit beträgt beim Rapid Spanning Tree typisch weniger als 1s.

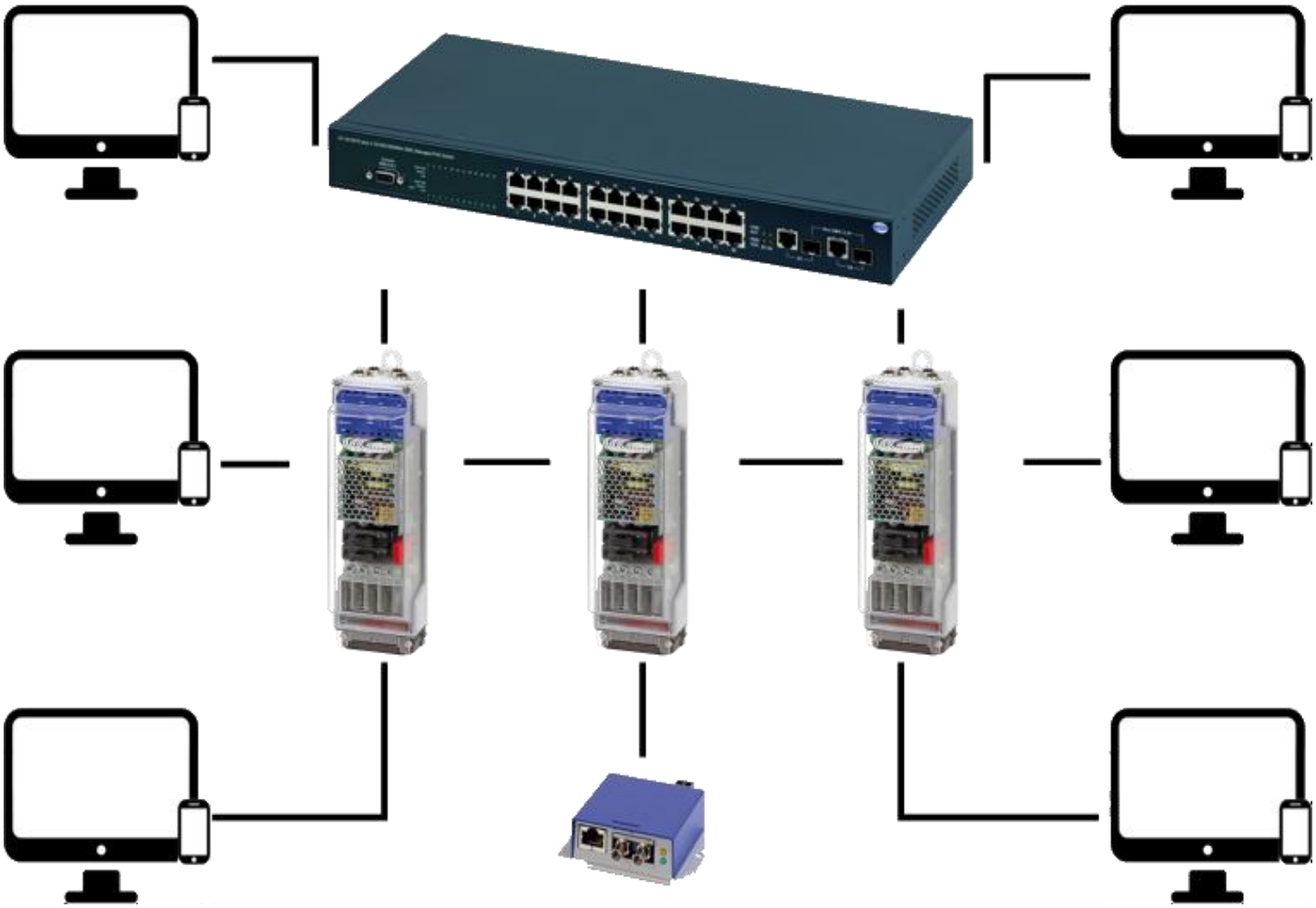


Abbildung 3: *pe-light-S* in einem vermaschten Netzwerk

3.3 Ring-Struktur

Der ***pe-light-S-switch*** unterstützt das Media Redundancy Protocol nach IEC 62439 (MRP-Ring), das es dem System ermöglicht, sich von Netzwerkausfällen innerhalb von 200ms oder weniger zu erholen. Der MRP-Ring erhöht auf diese Weise die Zuverlässigkeit im Netzwerk. Abbildung 4 zeigt ein Beispiel für eine Anwendung mit Ring-Funktionalität.

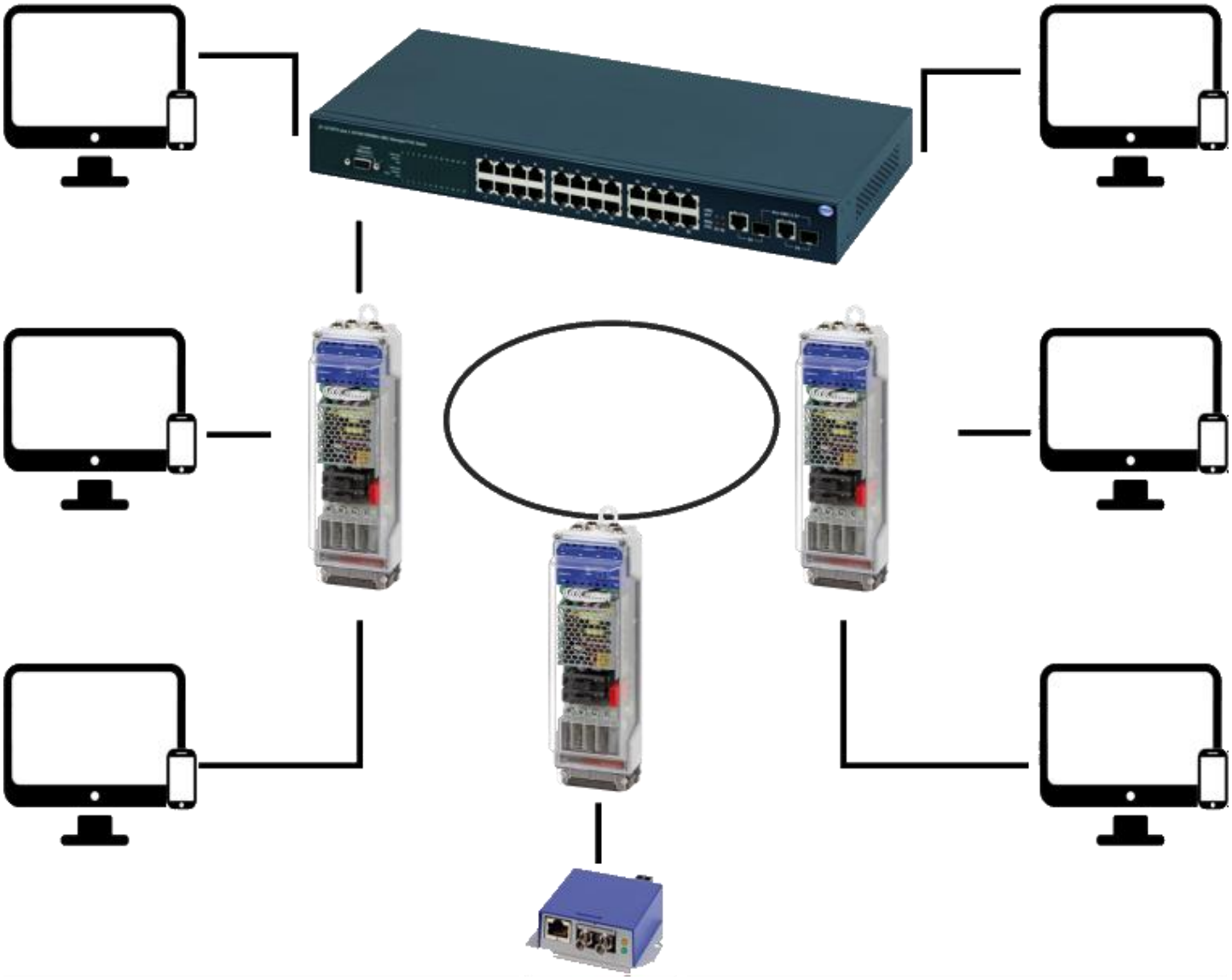


Abbildung 4: *pe-light-S* in einem ringförmigen Netzwerk

4 Web Applikation

Die ***pe-light-S-switches*** sind mit einem modernen Web-Interface ausgestattet, durch das sie von jedem Webbrowser aus komfortabel konfiguriert werden können.

Im Auslieferungszustand hat das Gerät die fest eingestellte IP Adresse 192.168.10.1.

4.1 Vorbereitungen

Bevor Sie das Web-Management verwenden, installieren Sie den ***pe-light-S-switch*** im Netzwerk und vergewissern Sie sich, dass der zur Konfiguration des Switches vorgesehene PC sich im gleichen Subnetz befindet damit er über den Webbrowser auf den Switch zugreifen kann. Die bei Auslieferung Zugangsdaten finden Sie hier:

- Benutzername: **admin**
- Passwort: **admin**

Alternativ zum Administratorzugriff steht ein Gastzugang mit geringeren Berechtigungen und angepasster Menüführung zur Verfügung. Der Gastbenutzer hat keinen Zugriff auf die Funktionen Switching und Wartung sowie deren Unterpunkte. Die Zugangsdaten lauten:

- Benutzername: **guest**
- Passwort: **guest**

Hinweis:

Bitte ändern Sie die Passwörter der Benutzer admin und guest, bevor Sie das Gerät in ihrem Netzwerk einsetzen. Siehe Abschnitt 4.6.2.

4.2 System Login

1. Starten Sie einen Webbrowser auf Ihrem Computer.
2. Geben Sie die von Ihnen konfigurierte IP-Adresse des ***pe-light-S-switches*** ein, und drücken Sie die Taste “**Enter**”. Im Auslieferungszustand hat das Gerät die IP-Adresse 192.168.10.1 Siehe Abschnitt 4.6.1 für die Konfiguration der IP-Adresse.
3. Auf dem Bildschirm erscheint nun die Login Maske des Gerätes

Abbildung 5: Login-Maske

4. Wählen Sie die gewünschte Menüsprache aus.
5. Geben Sie nun den Benutzernamen und das Passwort ein.
6. Drücken Sie die Taste “**Enter**” oder klicken Sie auf ”**Anmelden**”. Sie gelangen jetzt zum Web-Interface des Switches.

4.3 Web-Interface

Das Web-Interface des ***pe-light-S-switches*** setzt sich zusammen aus der Menüleiste am linken Rand, der Informationsleiste im oberen Bereich, der eigentlichen Konfiguration in der Mitte und der Hilfe am rechten Rand, siehe Abbildung 6.

4.3.1 Menüleiste

Die Menüführung ermöglicht es Ihnen die einzelnen Seiten aufzurufen und dort Einstellungen vorzunehmen. Die angezeigten Menüpunkte untergliedern sich in weitere Unterpunkte.

4.3.2 Informationsleiste

Die Informationsleiste zeigt Ihnen den Gerätetyp, Einbauort und die IP-Adresse an. Unter dem Logout-Button am rechten Ende der Leiste wird der aktuelle Benutzer angezeigt. Durch Betätigen des Buttons können Sie sich ausloggen und die Weboberfläche sperren. Der Hilfe Button blendet Ihnen für die einzelnen Seiten Hinweise und Erläuterungen ein.

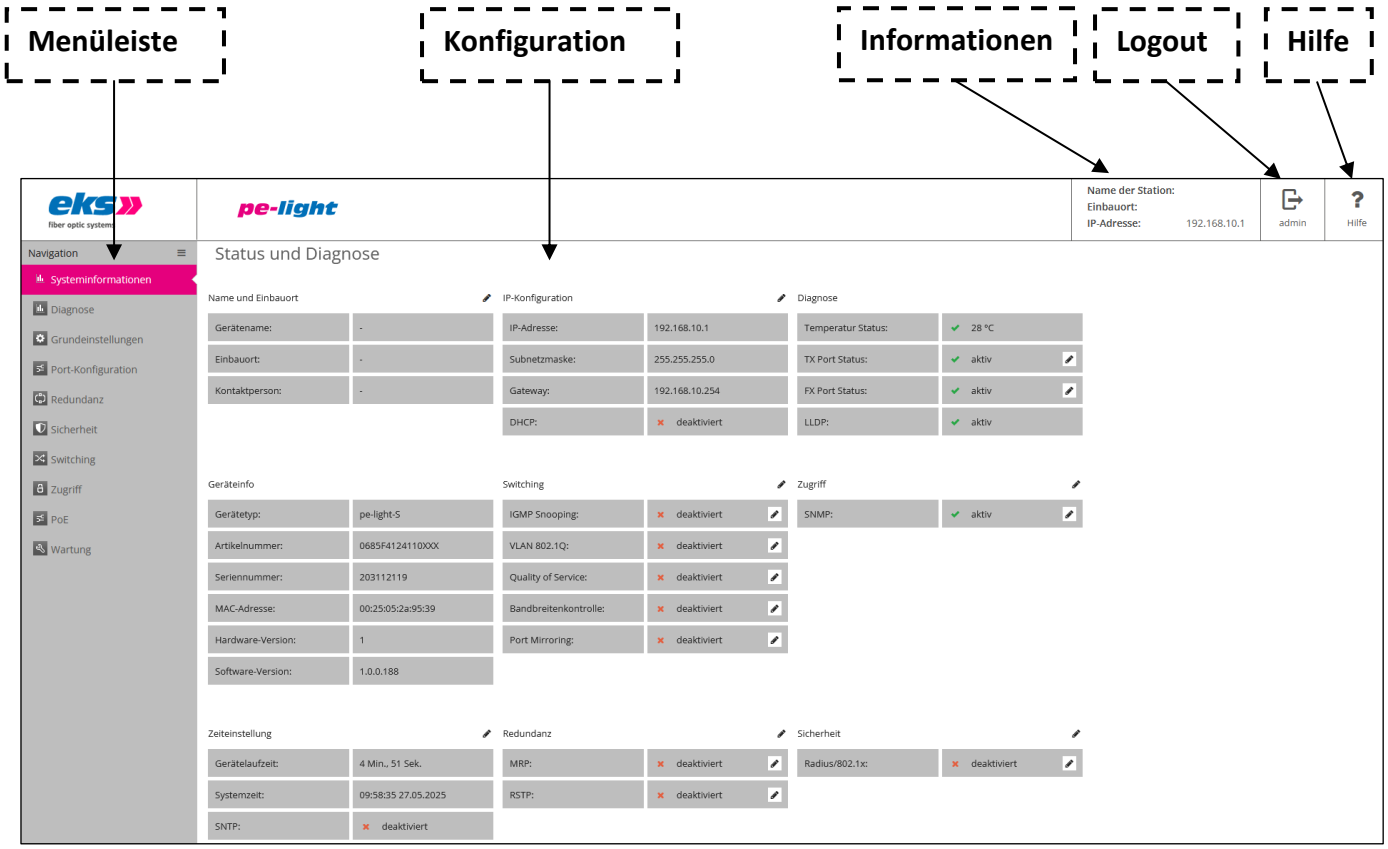


Abbildung 6: Status und Diagnose

4.4 Systeminformationen

Die Seite Systeminformationen bietet Ihnen einen kompletten Überblick über den Status und die aktuelle Konfiguration des ***pe-light-S-switches***.

Neben Seriennummer, Hard- und Softwareversion des Gerätes finden Sie hier eine Übersicht über die

aktivierten bzw. deaktivierten Protokolle und Funktionen. Mit Hilfe der Editier-Buttons können Sie direkt zu den entsprechenden Protokollen und Funktionen wechseln, um dort Einstellungen vorzunehmen.

4.5 Diagnose

Der Menüpunkt Diagnose ist in mehrere Unterpunkte gegliedert, die umfassende Informationen über den Zustand des ***pe-light-S-switches*** und dessen Netzwerkumgebung bereitstellen.

Die einzelnen Unterpunkte werden im Folgenden näher erläutert.

4.5.1 Alarme / Meldungen

Der Menüpunkt Alarme / Meldungen dient zur Definition von Alarmauslösern und Alarmempfängern. Alarmtrigger geben an, welche Alarme von der Software beachtet werden sollen. Treten Alarme auf, für die ein Alarmtrigger definiert ist, dann wird ein Logeintrag erzeugt und die Fail-LED angesteuert. Ebenso werden mit dem Alarmtrigger verknüpfte Alarmempfänger informiert oder angesteuert.

Alarmtrigger

- Eine Statusänderung eines Ports
- Eine zu hohe oder zu niedrige Temperatur des Switch ICs
- Fehler im MRP Protokoll
- Öffnen des Türkontaktes
- Eine zu hohe oder zu niedrige PoE Leistung

Alarmempfänger

- SNMP-Traps
- E-Mail-Adressen

Übersichtstabelle

Die konfigurierten Alarmzuweisungen werden in einer Tabelle mit fortlaufender ID angezeigt.

Einzelne Spalten der Tabelle können über

Pulldown-Menüs in den Tabellenüberschriften sortiert werden. Wird auf eine Tabellenüberschrift geklickt erscheint rechts daneben ein

kleiner Pfeil nach oben, bei

nochmaligem Klick zeigt der Pfeil nach unten, so kann gewechselt werden zwischen einer auf- oder absteigenden Sortierung der Einträge. Wird das Pulldownmenü ein

drittes Mal betätigt, so verschwindet der Pfeil wieder und die Sortierung entspricht der chronologischen Reihenfolge, in der die Einträge angelegt wurden. (Die Spalten werden entweder nach Zahlen sortiert (ID) oder alphabetisch (Alarmtrigger und zugeordnete Alarmempfänger). Es kann immer nur nach einer Spalte sortiert werden.

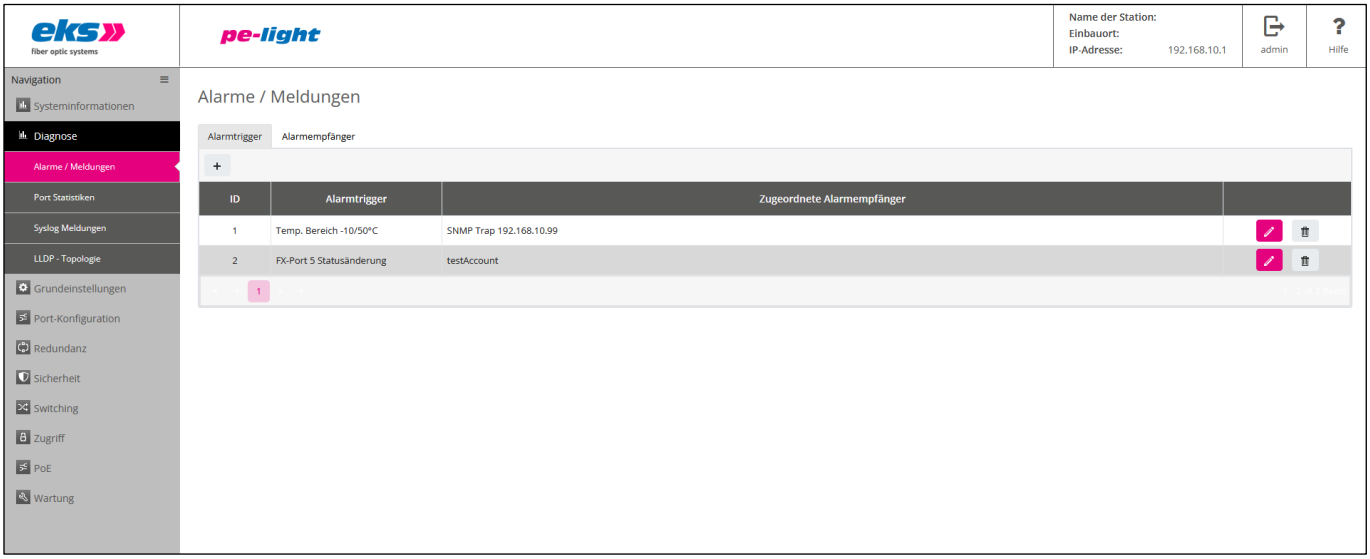


Abbildung 7: Übersicht der Alarmtrigger

Mit Hilfe der Seitenreiter Alarmauslöser und Alarmempfänger kann die Ansicht umgeschaltet werden zwischen:

- Alarmauslöser mit zugeordnetem -empfänger
- Alarmempfänger mit zugeordnetem -auslöser

Alarmtrigger hinzufügen und editieren

Unter dem Seitenreiter Alarmtrigger (Abbildung 8) können durch Anklicken des „+“-Buttons neue Alarme ergänzt werden. Sind bereits Alarme vorhanden, können sie per Button rechts in der Tabelle editiert oder gelöscht werden. Beim Anlegen und Editieren der Alarme können die zugehörigen Empfänger im unteren Teil der Seite ausgewählt und auf diese Weise mit dem Alarmauslöser verknüpft werden. Die folgenden Alarmtrigger sind möglich:

- Die Ethernet Ports können einen Alarm bei Aktivität, Inaktivität und Statusänderung auslösen.
- Die optischen Ports können Aktivität, Inaktivität und eine Statusänderung melden.
- Es können Alarme beim Überschreiten einer oberen oder Unterschreiten einer unteren Temperaturgrenze konfiguriert werden.
- MRP-Ereignisse (Ringunterbrechung, Ring wieder geschlossen, generische Warnung) können Alarme

erzeugen.

- Es können Alarme beim Überschreiten einer oberen oder Unterschreiten einer unteren PoE Leistungsgrenze konfiguriert werden.
- Alarme können durch Öffnen des Türkontaktes auslösen.

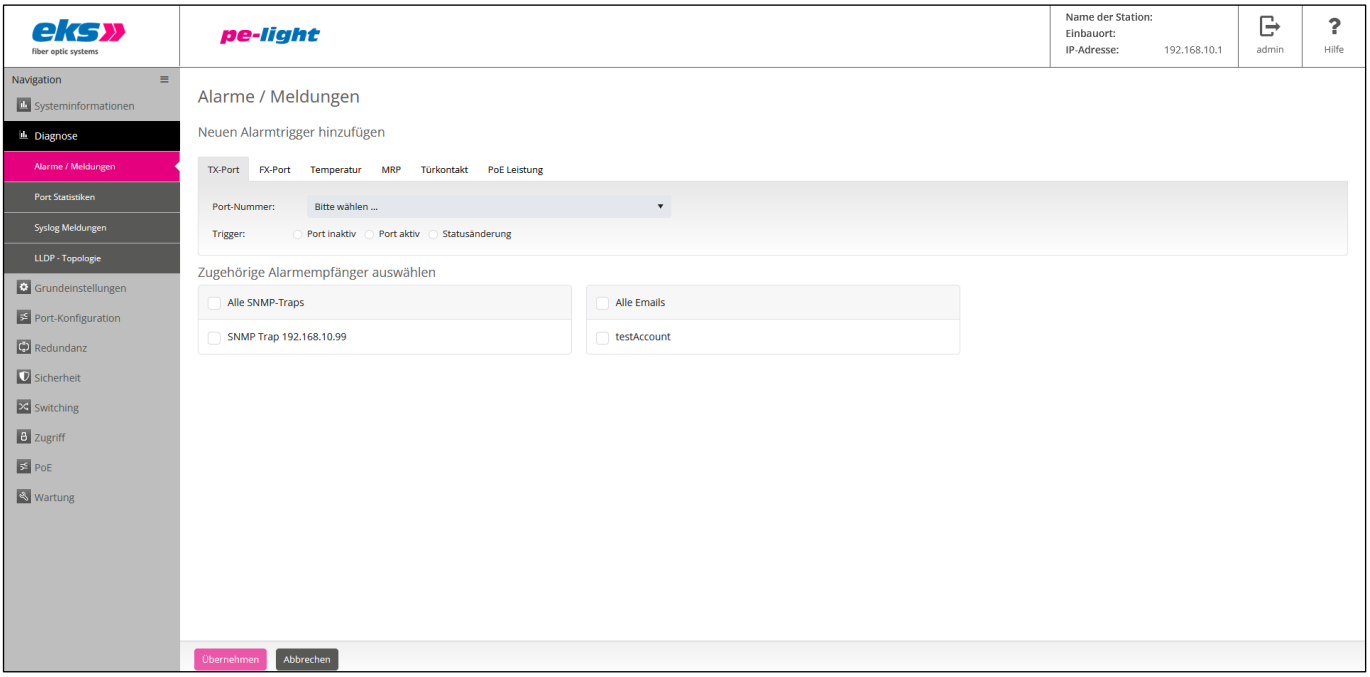


Abbildung 8: Alarme / Meldungen: Hinzufügen eines Alarmauslösers

Alarmempfänger hinzufügen und editieren

Durch Anklicken des „+“-Buttons unter dem Seitenreiter Alarmempfänger (Abbildung 9) können neue Empfänger hinzugefügt werden. Als neue Alarmempfänger können SNMP Traps und E-Mail-Postfächer angelegt werden:

- Beim Simple Network Management Protokoll (SNMP) werden Fehlerbenachrichtigungen vom Gerät (das als Agent arbeitet) erzeugt und unaufgefordert an eine Management Station versendet. Da die Pakete nicht bestätigt werden, kann das Gerät nicht feststellen, ob der Manager die Informationen erhalten hat.
- Beim Verwenden der E-Mail Funktion kann der Anwender seine E-Mail Adresse und einen SMTP-Server (Simple Mail Network Protokoll) angeben und das Gerät versendet bei einem Alarm eine E-Mail an den Benutzer. Optional kann die Authentifizierung aktiviert und das E-Mail Passwort eingegeben werden.

  Mit dem Button „Test Mail senden“ können die Einstellungen überprüft werden, bevor der

Alarmempfänger angelegt wird.

Im unteren Teil der Seite können die Alarmempfänger bereits angelegten Alarmauslösern zugeordnet werden.

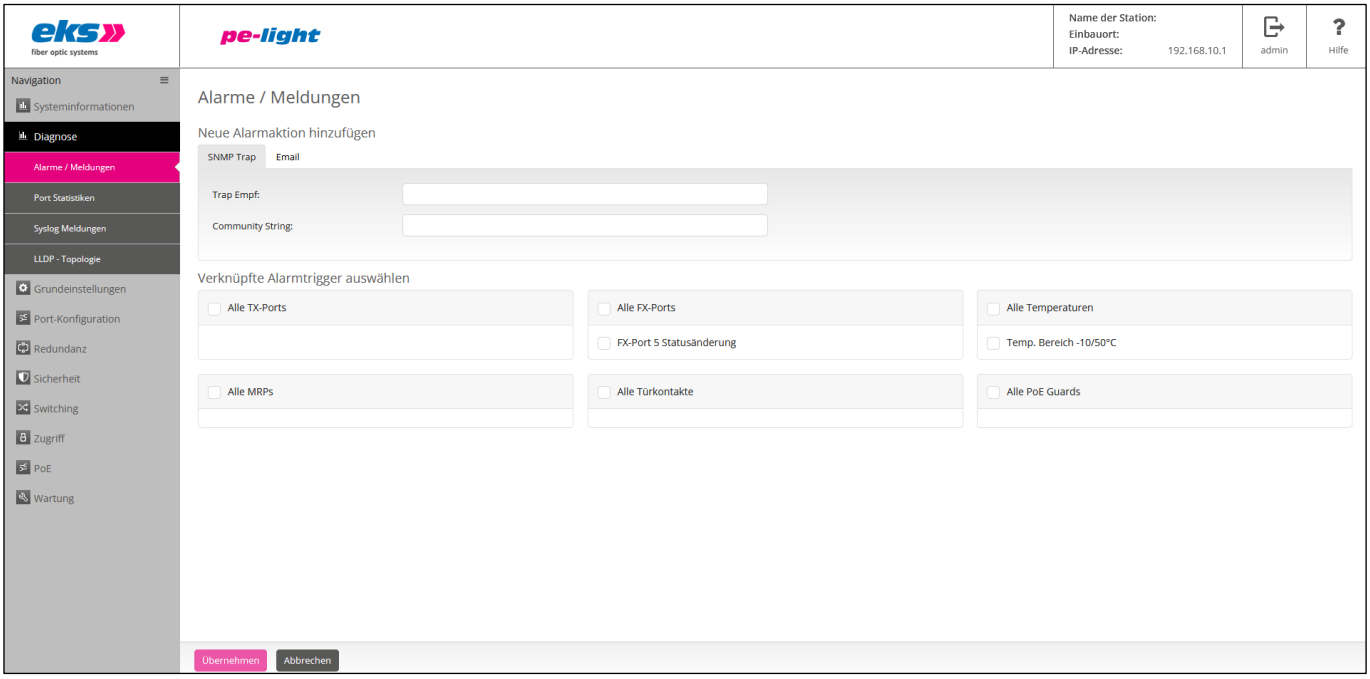


Abbildung 9: Hinzufügen eines Alarmempfängers

4.5.2 Port Statistiken

Die Seite Port Statistiken (Abbildung 10) gibt Auskunft über den Datenverkehr auf den einzelnen Ports, die für Diagnosezwecke bei Netzwerkproblemen hilfreich ist. Die gesamte Anzahl der versendeten, empfangenen, fehlerbehafteten und kollidierten Pakete wird angezeigt. Außerdem wird die Größe der einzelnen Pakete statistisch bis zu verschiedenen Grenzwerten erfasst.

Bei den versendeten Paketen wird unterschieden zwischen:

- Anzahl aller Pakete
- Anzahl der Unicast Pakete (Pakete an einen Empfänger)
- Anzahl der nicht Unicast Pakete (Pakete an mehrere Empfänger)

Bei den empfangenen Paketen wird unterschieden zwischen:

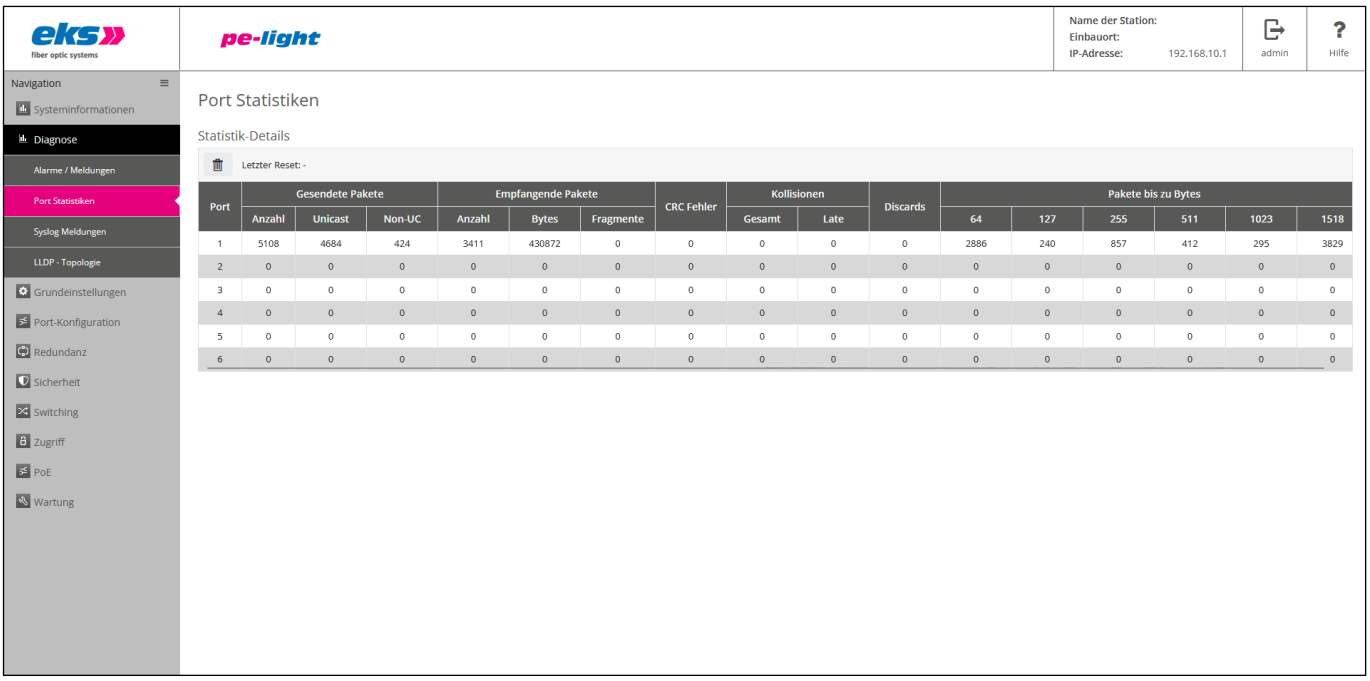
- Anzahl aller Pakete
- Insgesamt empfangene Bytes

- Insgesamt empfangene Fragmente

Die Spalte CRC-Fehler gibt Auskunft über die Anzahl der fehlerhaft empfangenen Datenpakete. Die zyklische Redundanzprüfung CRC (Englisch: Cyclic Redundancy Check) berechnet einen Prüfwert anhand der übertragenen Daten. Dieser Wert wird zusammen mit den Daten versendet und vom Empfänger ausgewertet. Fehlerhafte Pakete werden so erkannt und verworfen.

Die Gesamtzahl aller Kollisionen und die der späten Kollisionen (Late Collisions) wird in der Spalte Kollisionen angezeigt.

Die Spalte „Pakete bis zu Bytes“ gibt Auskunft über die Anzahl der Pakete in verschiedenen Größen. Hier wird die Zahl der empfangenen Pakete bis zu 64, 127, 255, 511, 1023 und 1518 Byte Größe erfasst.



Port	Gesendete Pakete			Empfangende Pakete			CRC Fehler	Kollisionen		Discards	Pakete bis zu Bytes					
	Anzahl	Unicast	Non-UC	Anzahl	Bytes	Fragmente		Gesamt	Late		64	127	255	511	1023	1518
1	5108	4684	424	3411	430872	0	0	0	0	0	2886	240	857	412	295	3829
2	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	0	0	0	0	0	0
4	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
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Abbildung 10: Port Statistiken

Zurücksetzen der Werte

In der, oberhalb der Tabelle angeordneten, Statusleiste können, mit Hilfe eines Buttons, die Zähler aller Ports zurückgesetzt und auf diese Weise eine neue Auswertung gestartet werden. Der Zeitpunkt, an dem mit der Auswertung begonnen wurde, wird in der Statuszeile als letzter Reset angezeigt.

4.5.3 Syslog Meldungen

Die Syslog Meldungen (Abbildung 11) dienen dem Benutzer als Hilfestellung, um Status- und Fehlermeldungen der verschiedenen Funktionen und Protokolle zu erhalten. Die Meldungen werden in der Übersicht mit Datum und Uhrzeit, sowie einem Code, einer Beschreibung und einer Referenz angezeigt. Da die Log-Einträge nicht im Gerät gespeichert werden, sind sie nach einem Geräteneustart bzw. einer Spannungsunterbrechung nicht mehr verfügbar. Um die Meldungen dauerhaft zu archivieren, besteht die Möglichkeit einen externen Syslog-Server zu verwenden.

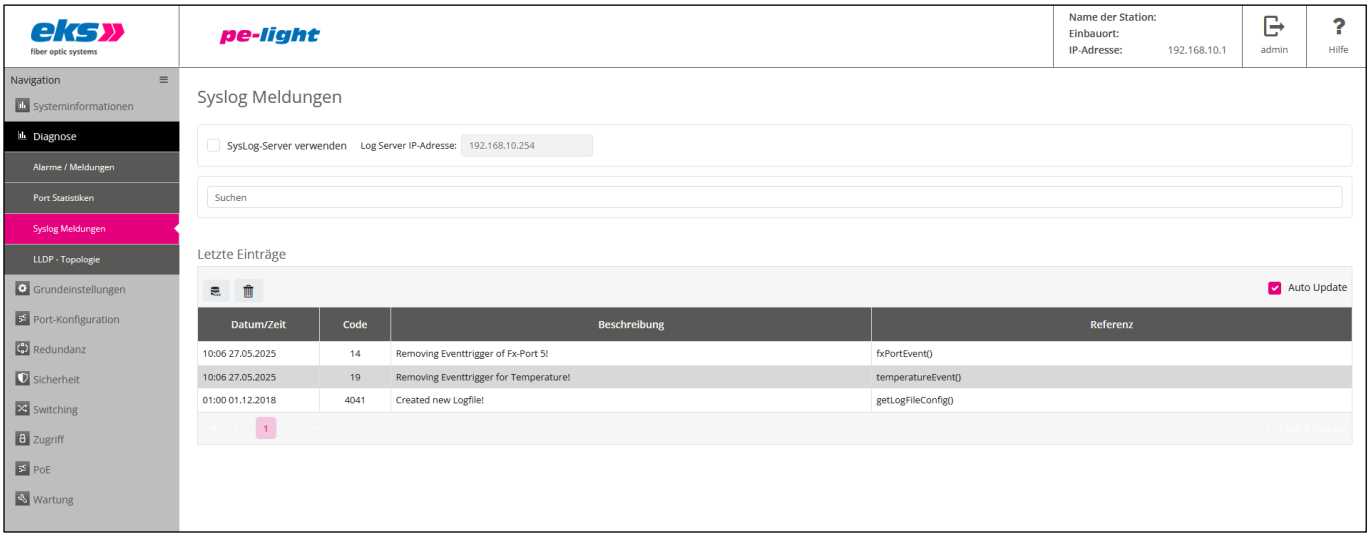


Abbildung 11: Syslog Meldungen

Verwendung des Syslog-Servers

Um die Meldungen auf einem Syslog-Server zu archivieren bzw. zu speichern, aktivieren Sie diese Funktion über die Checkbox in der oberen Leiste. Geben Sie die IP-Adresse des Syslog-Servers in Dezimalpunktschreibweise an und speichern Sie die Einstellungen mit Hilfe des unten erscheinenden Übernehmen Buttons. Bitte überprüfen Sie, ob der Server erreichbar ist und die Meldungen in einer Datei abspeichert.

Exportieren und Zurücksetzen der Einträge

Folgende Buttons stehen hier zur Verfügung:

- Der Button CSV-Export erstellt eine CSV-Datei (Comma-Seperated Values) mit allen Einträgen aus der Tabelle und speichert diese im Download-Ordner des Browsers. Die Meldungen werden zeilenweise durch ein Komma getrennt in eine Datei geschrieben.
- Der Button zum Löschen der Log-Datei entfernt alle Einträge aus der Tabelle. In der Folge werden alle

ab diesem Zeitpunkt aufgetretenen Meldungen angezeigt. Der Zeitpunkt des Löschens der Einträge ist am neu erscheinenden ersten Logeintrag erkennbar.

Suche nach Einträgen

Mit der Suchleiste können Sie gezielt in der Liste der Syslog-Meldungen nach bestimmten Einträgen suchen. Dies ist besonders nützlich, wenn die Liste umfangreich ist und Sie herausfinden möchten, ob ein bestimmtes Ereignis aufgetreten ist, wie oft es vorkam oder welche Ereignisse an einem bestimmten Tag verzeichnet wurden. Die Suche kann auf alle Spalten der Tabelle angewendet werden (Datum/Zeit, Code, Beschreibung und Referenz). Es werden Ihnen nur noch die Einträge angezeigt, die mit Ihrer Suchanfrage übereinstimmen, wobei die Groß- und Kleinschreibung nicht berücksichtigt wird. Um wieder alle Einträge anzuzeigen, müssen Sie die Suchleiste leeren.

Sortieren der Einträge

Die Einträge der Syslog-Meldungen lassen sich über Pulldown-Menüs in den Spaltenüberschriften sortieren. Durch einen Klick auf eine Spaltenüberschrift erscheint rechts daneben ein kleiner Pfeil nach oben. Ein weiterer Klick kehrt die Sortierreihenfolge um und der Pfeil zeigt nach unten. Beim dritten Klick wird die ursprüngliche Reihenfolge der Einträge wiederhergestellt und der Pfeil verschwindet.

Sortierung innerhalb der Spalten:

- „Datum/Zeit“: die Sortierung erfolgt chronologisch in auf- oder absteigender Reihenfolge
- „Code“: die Sortierung erfolgt auf- bzw. absteigend anhand der ersten Ziffer des Fehlercodes.
- „Beschreibung“ und „Referenz“: die Sortierung erfolgt alphabetisch, basierend auf dem Anfangsbuchstaben

4.5.4 Link Layer Discovery Protocol – Topologie

Das Link Layer Discovery Protokoll (Abbildung 12) ist ein herstellerunabhängiges Layer-2-Protokoll, das nach der IEEE-802.1AB-Norm[1] definiert ist und die Möglichkeit bietet, Informationen zwischen Nachbargeräten auszutauschen. Auf jedem Gerät, das LLDP unterstützt, arbeitet eine Softwarekomponente, der sogenannte LLDP-Agent. Dieser versendet in periodischen Abständen Informationen über den eigenen Zustand und empfängt permanent Informationen der Nachbargeräte. Da dies unabhängig voneinander geschieht, wird das LLDP auch als Ein-Weg-Protokoll bezeichnet. Vor dem Versenden der Informationen wird keine Verbindung zu anderen Geräten aufgebaut.

Die folgenden Informationen werden von LLDP zusammengestellt und versendet:

- Systemname
- Systembeschreibung
- Portbeschreibung
- Chassis-ID
- IP-Adresse

Systemname, Systembeschreibung und Portbeschreibung entsprechen den Einträgen der sysObjektID und der sysDescription sowie der ifDescr (Interface Description) aus der SNMP-MIB2. Diese Werte sind nicht anpassbar. Die IP-Adresse wird automatisch auf die aktuelle Einstellung angepasst. Die Chassis ID entspricht dem vergebenen Gerätenamen. Wenn kein Gerätename vergeben ist, wird die MAC-Adresse übertragen.

LLDP Intervall

Mit dem Parameter LLDP Intervall kann festgelegt werden, in welchen Zeitabständen (in Sekunden) das Geräteeigene LLDP-Telegramm an die Nachbargeräte versendet wird.

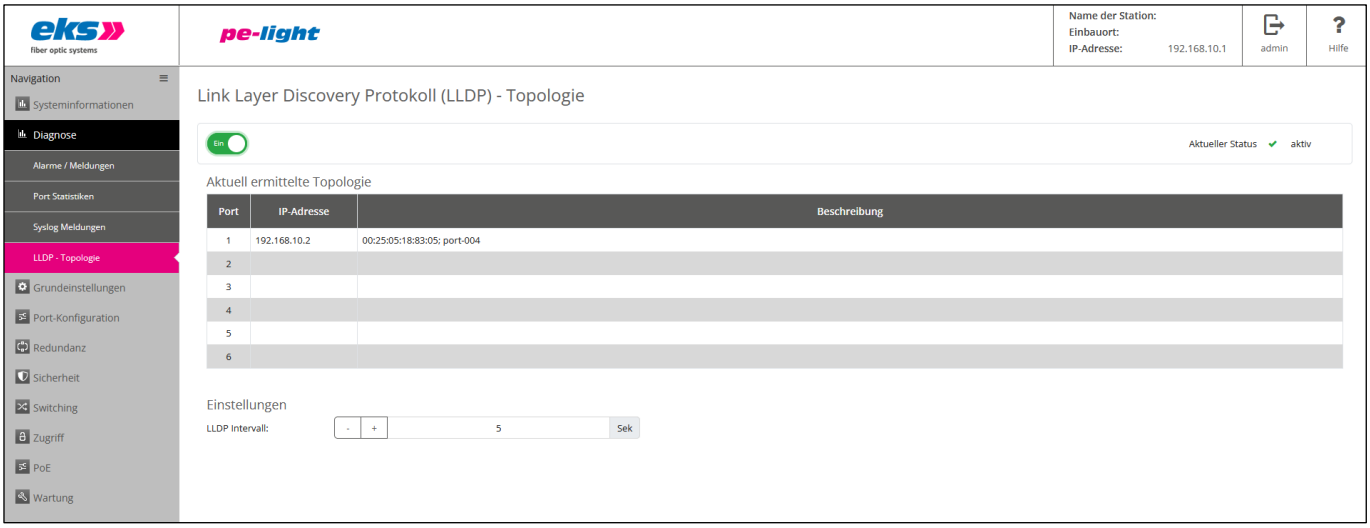


Abbildung 12: Link Layer Discovery Protokoll (LLDP)

- Ein/Aus – Schalter: Mithilfe des Schalter kann LLDP ein oder ausgeschaltet werden.
- Einstellungen speichern: Die Einstellungen können gespeichert werden indem man unter der Einstellung zur LLDP Intervall auf den Button Übernehmen klickt. Wird der Abbrechen Button angeklickt werden die neuen Einstellungen verworfen. Beide Buttons sind erst zu sehen, wenn eine Einstellung auf

der Seite, verändert worden ist.

4.6 Grundeinstellungen

Die Seite Grundeinstellungen (Abbildung 13) bietet ihnen die Möglichkeit, dem Gerät einen eindeutigen Namen, einen Standort und einen Ansprechpartner zuzuweisen.

- Gerätename: Vergeben Sie dem ***pe-light-S-switch*** einen Namen, um das Gerät eindeutig zu identifizieren.
- Einbauort: Mit Hilfe des Einbauortes haben Sie eine weitere Möglichkeit, das Gerät zu identifizieren.
- Kontaktperson: Ein Ansprechpartner, der für das Gerät zuständig ist, kann im dritten Eingabefeld gespeichert werden.

Die Eingabefelder sind so konfiguriert, dass bis zu 50 Zeichen verwendet werden können. Eine leere Eingabe wird nicht akzeptiert. Die Verwendung von Sonderzeichen ist möglich. Nach Übernahme der eingetragenen Daten wird der Einbauort in der Informationsleiste oben rechts angezeigt und hilft Ihnen, das Web-Interface einem Gerät zuzuordnen.

Abbildung 13: Grundeinstellungen des *pe-light-S-switches*

4.6.1 IP-Konfiguration

Sie können die IP-Konfiguration (Abbildung 14) entweder automatisch mit Hilfe des Dynamical Host Configuration Protocol (DHCP) durchführen lassen oder die Einstellungen manuell vornehmen.

Automatisch (DHCP)

Um eine Konfiguration der IP-Adresse, der Subnetzmaske und des Standardgateways von einem im Netzwerk arbeitenden Server mit entsprechender Funktionalität zu erhalten, aktivieren Sie die DHCP - Clientfunktion.

Nachdem Sie die Einstellungen durch Klicken auf den Anwenden Button gespeichert haben, wird das Gerät eine Anfrage ins Netz schicken und die vom DHCP-Server erhaltene Konfiguration übernehmen. Da das Gerät nun eine neue IP-Adresse bekommen hat, ist es nicht mehr über die vorher konfigurierte-IP erreichbar. Bitte kontaktieren Sie ihren Netzwerkadministrator, um die neue IP-Adresse zu erhalten.

Manuell

Sollte Ihr Netzwerk über keinen DHCP-Server verfügen oder sollen die Einstellungen von Hand vorgenommen werden, so wählen Sie im oberen Bereich der Seite die manuelle IP-Konfiguration aus. Bitte überprüfen Sie genau, welche Einstellungen Sie vornehmen, damit es nicht zu Problemen mit doppelten IP-Adressen kommt, die Ihr gesamtes Netzwerk negativ beeinflussen können. Das Format der IP-Adresse, der Subnetzmaske und des Gateways muss in Dezimalpunktschreibweise eingegeben werden. Die folgenden Einstellungen sind erforderlich:

- IP-Adresse: Bitte beachten Sie, dass die von ihnen eingestellte IP-Adresse von ihrem PC aus erreichbar sein muss, damit sie sich erneut mit dem Gerät verbinden können, um die weiteren Einstellungen vorzunehmen.
- Subnetzmaske: Geben Sie die Subnetzmaske der IP-Adresse ein, diese trennt die IP-Adresse in einen Netzwerkteil und einen Geräteteil auf. Somit wird festgelegt, welche IP-Adressen im eigenen Netz erreichbar sind und welche Adressen in anderen Teilnetzen angesiedelt und nur über Router zugänglich sind.
- Gateway: Bestimmen Sie das Standartgateway des Switches. Über das Gateway wird mit Geräten außerhalb Ihres Subnetzes kommuniziert.

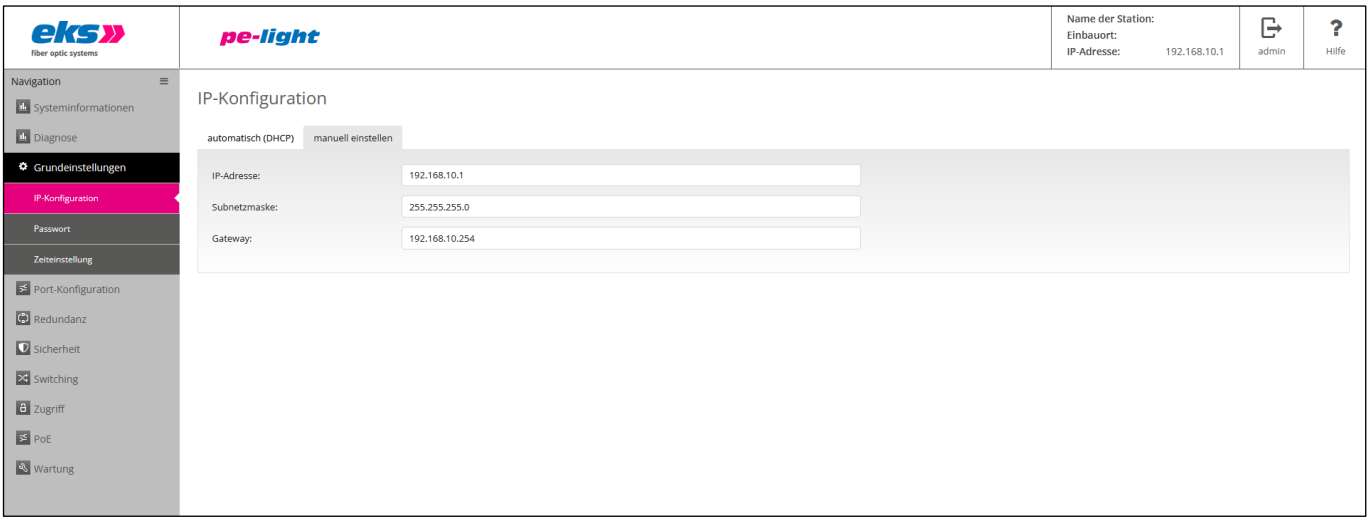


Abbildung 14: Änderung der IP-Konfiguration

4.6.2 Passwort

Auf der Passwort-Seite (Abbildung 15) kann das voreingestellte Standardpasswort für Administrator- und Gastbenutzer verändert werden. Das aktuelle bzw. bisherige Passwort muss dazu bekannt sein und eingegeben werden. Die Benutzernamen und Rechte vom Administrator und Gast sind fest vergeben und können nicht verändert werden.

Abbildung 15: Änderung des Passwortes für Administrator- und Gastzugriff

Folgende Formularfelder sind vorhanden:

- Neues Passwort: Bitte tragen Sie in dieses Feld das von Ihnen festgelegte Passwort für den zuvor ausgewählten Benutzer ein. Beachten Sie dazu auch die Hinweise zur Vergabe von Passwörtern im unteren Abschnitt.
- Passwort bestätigen: Um sicher zu gehen, dass Sie Ihr Passwort korrekt eingegeben haben,

wiederholen Sie die Eingabe in diesem Feld.

- Aktuelles Passwort: Bitte geben Sie hier das bisher verwendete aktuelle Passwort ein, das nun geändert werden soll.

Hinweis:

Die Sicherheit ihres Systems hängt im Wesentlich mit der Sicherheit ihrer Passwörter zusammen. Es wird daher bei Passwörtern generell empfohlen:

- Verwenden Sie keine Wörterbucheinträge
- Benutzen Sie möglichst komplexe Passwörter
- Kombinieren Sie Buchstaben, Zahlen und Sonderzeichen
- Verwenden sie kleine und große Buchstaben
- Ihr Passwort sollte aus mindestens acht Zeichen bestehen
- Notieren Sie sich die Passwörter nicht

4.6.3 **Zeiteinstellung**

In der Statusleiste im oberen Bereich der Seite zur Zeiteinstellung (Abbildung 17 / Abbildung 17) werden links die Systemzeit und das Datum angezeigt. Die Gerätelaufzeit folgt in der Mitte. Ganz rechts stehen die aktuell verwendeten Einstellungen zur Zeitzone und eine eventuelle Verschiebung durch die Sommerzeit.

Beim Setzen von Datum und Zeit können Sie zwischen der Verwendung eines Zeitservers und einer manuellen Konfiguration auswählen. Die automatische Konfiguration der Systemzeit per Simple Network Time Protokoll (SNTP) hat den Vorteil, dass die Zeiteistellung in regelmäßigen Abständen aktualisiert wird. Eine exakte Systemzeit ist insbesondere dann sinnvoll, wenn die Logdatei im Fehlerfall ausgewertet werden soll.

Systemzeit automatisch per SNTP setzen

Um die Systemzeit per SNTP zu setzen, ist eine Verbindung zu einem SNTP-Server im Internet erforderlich. Die folgenden Einstellungen sind bei der Verwendung von SNTP erforderlich:

- SNTP Server IP-Adresse: Geben Sie hier die IP-Adresse eines über das Internet erreichbaren oder

lokalen Zeitservers ein. Bitte verwenden Sie die Dezimalpunktschreibweise.

- SNTP Server IP-Adresse (Redundanz): In diesem Feld können Sie die IP-Adresse eines zweiten, redundanten Zeitservers angeben. Sollte der erste Server nicht erreichbar sein, dann wird die Zeit über diesen SNTP-Server synchronisiert.
- Update-Intervall: Bitte geben Sie hier vor, in welchen Zeitabständen sich das Gerät mit dem Zeitserver synchronisieren soll. Bedenken Sie dabei, dass die Systemzeit bei größeren Zeitspannen eventuell sehr stark von der realen Zeit abweicht.
- Zeitzone: Bitte geben Sie die Zeitzone an, in der sich das Gerät befindet.

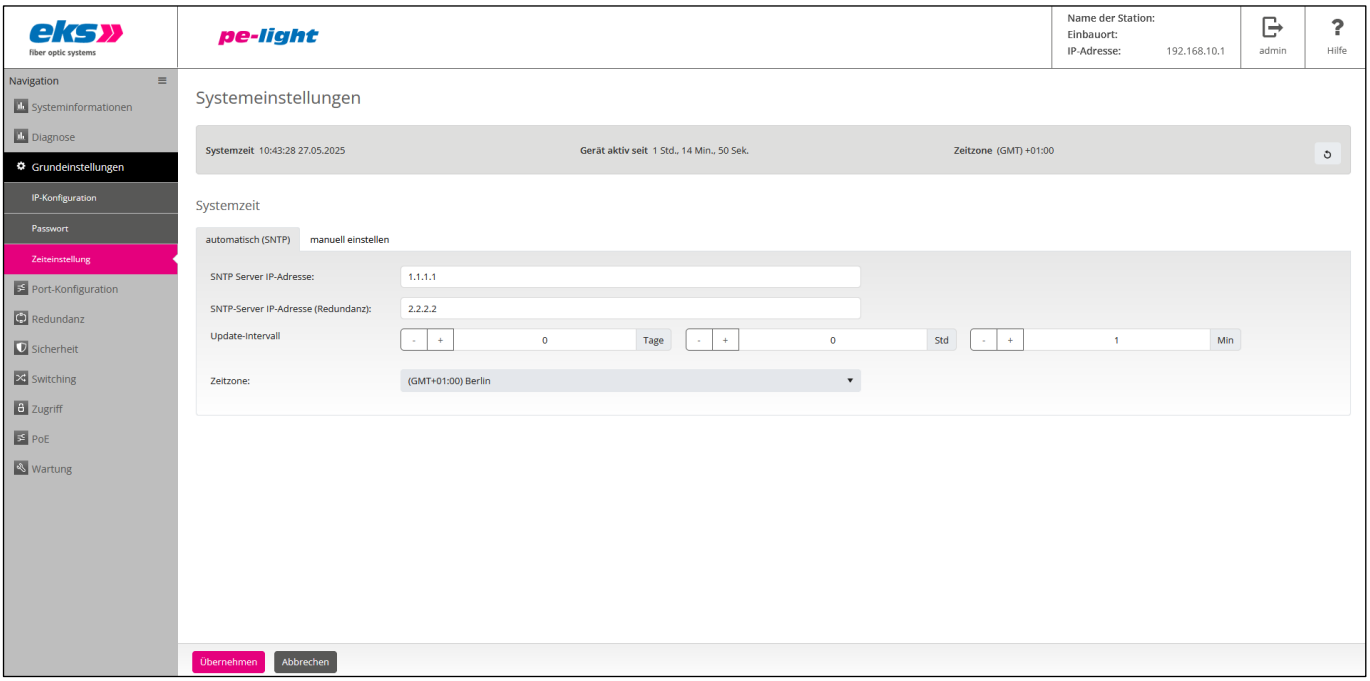


Abbildung 16: Konfiguration der Zeiteinstellung (SNTP)

Systemzeit von Hand setzen

Beim Setzen der Systemzeit von Hand haben Sie die Möglichkeiten, die Zeit des Browsers zu verwenden oder die Zeit und das Datum von Hand einzugeben und zu speichern.

Um die Zeit des Browsers zu verwenden, betätigen Sie den Button „Zeit des Browsers verwenden“, überprüfen Sie ob die korrekte Zeit/das Datum übernommen worden sind und speichern Sie die Werte mit dem Übernehmen Button.

Falls Sie die Einstellungen von Hand vornehmen möchten, wählen Sie zunächst das aktuelle Datum per Eingabefeld aus. Sie können das Datum auch mit Hilfe der Tastatur eingeben, zuerst zwei Stellen für den Monat, dann zwei für den Tag und schließlich zwei oder vier Stellen für das Jahr. Alternativ können Sie neben dem Eingabefeld den kleinen Kalender-Button nutzen und Datum und Zeit grafisch per Mausklick

einstellen. Geben Sie die Zeit und die entsprechende Zeitzone ein. Speichern Sie die Einstellungen mit Hilfe des Übernehmen-Buttons und überprüfen Sie, ob alles korrekt übernommen wurde.

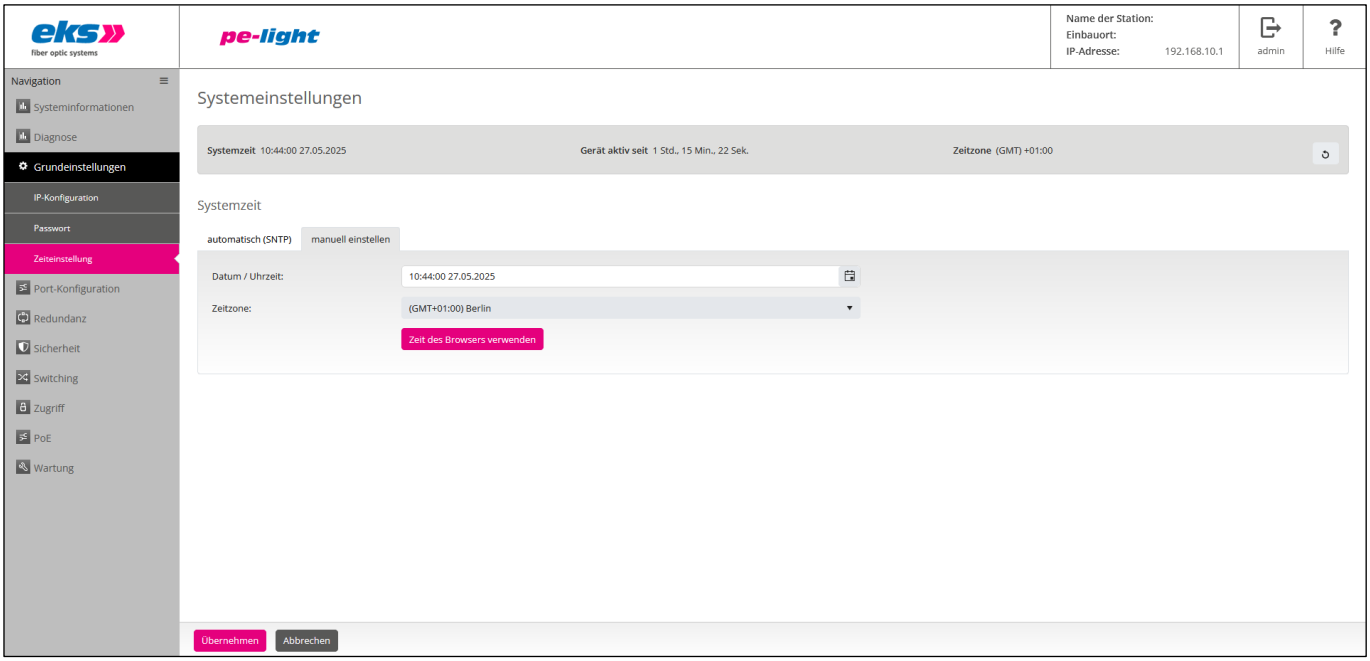


Abbildung 17: Konfiguration der Zeiteinstellungen (manuell)

4.7 Port-Konfiguration

Die Tabelle zur Port-Konfiguration (Abbildung 18) ermöglicht eine Übersicht der aktuellen Konfiguration der einzelnen Ports. Die Spalten Aktiviert, Auto Negotiation, Flusskontrolle und Bezeichnung können darüber hinaus konfiguriert werden. Die restlichen Felder werden durch Belegung der Ports verändert und durch neu laden der Seite aktualisiert.

Folgende Spalten werden angezeigt:

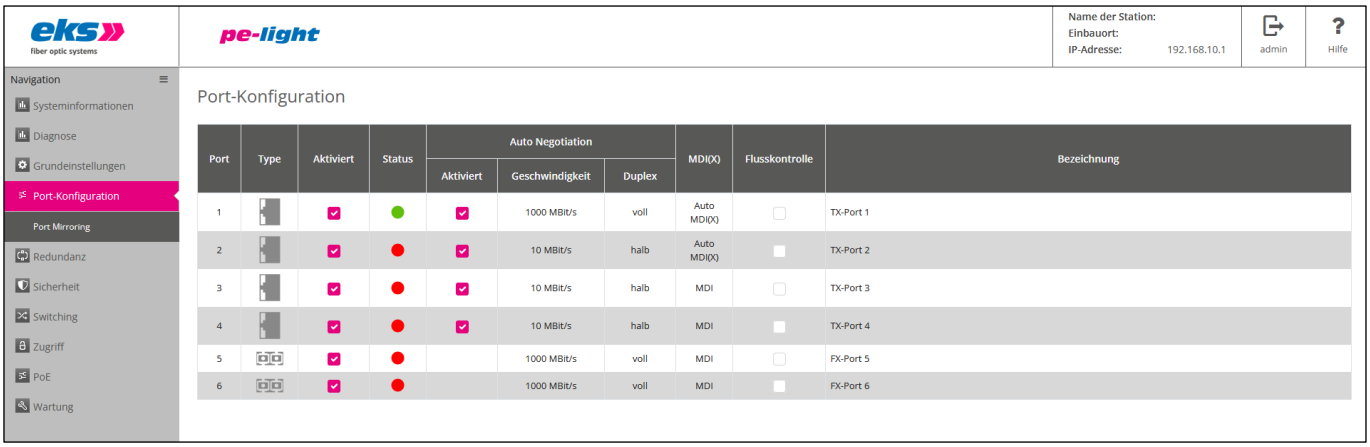
- Port: Gibt die Portnummer an, die auch auf dem Gehäuse (als P1 bis P8) gekennzeichnet ist.
- Typ: Zeigt mit Hilfe eines Symboles an, ob der Port ein RJ45-Port oder ein optischer Port ist.
- Aktiviert: Die einzelnen Ports können hier Aktiviert oder Deaktiviert werden. Damit legen Sie fest ob ein Port verwendet werden kann oder nicht.
- Status: Status signalisiert den aktuellen Zustand der Ports:
  - Grün: Der Port ist aktiviert und eine Verbindung besteht.
  - Rot: Der Port ist aktiviert aber es besteht keine Verbindung.
  - Grau: Der Port ist deaktiviert. Eine Verbindung ist nicht möglich.
  - Grün/gelb: LWL-Port ist aktiv und eine Verbindung besteht. Die LWL-Strecke sollte überprüft

werden.

- Auto Negotiation: Ist diese Funktion aktiviert erfolgt eine automatische Konfiguration von Übertragungsgeschwindigkeit und Duplexmodus durch den ***pe-light-S-switch*** und die angeschlossene Gegenstelle. Wird Auto Negotiation deaktiviert, können die Einstellungen von Hand gesetzt werden und die kommunizierenden Geräte müssen mit diesen Einstellungen arbeiten:
  - Geschwindigkeit: Die Datenrate der Ports kann fest vorgegeben werden. Es besteht die Möglichkeit eine Datenrate von 10MBit/s, 100MBit/s oder 1000MBit/s einzustellen. Diese Einstellung kann nur für die M12 Ports verändert werden.
  - Duplex: Der Duplexmodus kann zwischen Halb- und Vollduplex umgeschaltet werden. Diese Einstellung ist damit für eine Verbindung fest vorgegeben. Diese Einstellung kann nur für die M12 Ports verändert werden.

Hinweis: Wenn beide Linkpartner Auto Negotiation verwenden, dann kann nicht garantiert werden, dass sich die Linkpartner auf 1000MBit/s Vollduplex einigen. Ebenso gibt es einen Duplex-Mismatch mit Leistungseinbußen, wenn ein Linkpartner Auto Negotiation verwendet und der andere fest auf 1000MBit/s eingestellt ist. Es wird empfohlen, Linkpartner fest auf eine Geschwindigkeit und einen Duplexmodus einzustellen.

- MDI(X): Der ***pe-light-S-switch*** führt automatisch ein Autocrossover durch. Das bedeutet, der Switch erkennt selbstständig, ob der Teilnehmer über ein gekreuztes oder nicht gekreuztes Kabel angeschlossen ist.
- Flusskontrolle: Die Flusskontrolle sorgt dafür, dass bei Überlastung eines Ports dem gegenüberliegenden Teilnehmer signalisiert wird, dass er langsamer senden soll. Bei Verwendung von QoS (Quality of Service) sollte die Flusskontrolle deaktiviert werden.
- Bezeichnung: In dieser Spalte können Sie den Ports einen Namen geben. Die Namen werden während der gesamten Konfiguration angezeigt und erleichtern die Auswahl der richtigen Einstellungen sowie die Diagnose im Fehlerfall. Die Portbezeichnungen können direkt in der Zeile editiert werden, in der sie angezeigt werden.

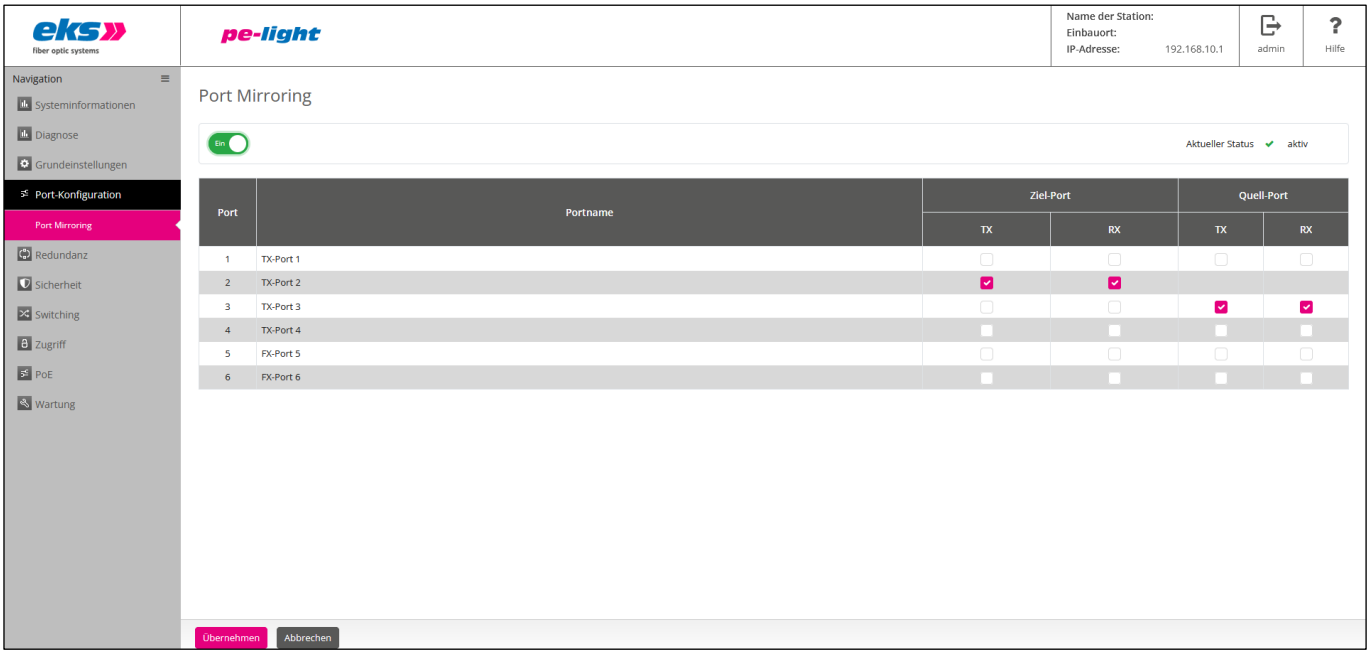


Port	Type	Aktiviert	Status	Auto Negotiation			MDI(X)	Flusskontrolle	Bezeichnung
				Aktiviert	Geschwindigkeit	Duplex			
1		☑	●	☑	1000 MBit/s	voll	Auto MDI(X)	☐	TX-Port 1
2		☑	●	☑	10 MBit/s	halb	Auto MDI(X)	☐	TX-Port 2
3		☑	●	☑	10 MBit/s	halb	MDI	☐	TX-Port 3
4		☑	●	☑	10 MBit/s	halb	MDI	☐	TX-Port 4
5		☑	●		1000 MBit/s	voll	MDI	☐	FX-Port 5
6		☑	●		1000 MBit/s	voll	MDI	☐	FX-Port 6

Abbildung 18: Übersicht der Tabelle Port-Konfiguration

4.7.1 Port Mirroring

Port Mirroring (Abbildung 19) ist eine Methode, um in Netzwerken den Datenverkehr eines Ports (Quelle) auf einen zweiten Port (Ziel) zu spiegeln, um ihn dort zu analyiseren. Entweder können nur gesendete oder gesendete und empfangene Pakete gespiegelt werden. Folgende Einstellungen können vorgenommen werden:



Port	Portname	Ziel-Port		Quell-Port	
		TX	RX	TX	RX
1	TX-Port 1	☐	☐	☐	☐
2	TX-Port 2	☑	☑		
3	TX-Port 3	☐	☐	☑	☑
4	TX-Port 4	☐	☐	☐	☐
5	FX-Port 5	☐	☐	☐	☐
6	FX-Port 6	☐	☐	☐	☐

Abbildung 19: Port Mirroring

- Port und Portname: Hier werden alle Ports angezeigt, um daraus einen Ziel- und ein oder mehrere Quell-Ports auszuwählen.
- Ziel-Port: Ist Port-Mirroring aktiviert, kann hier der Port ausgewählt werden, an den die duplizierten

Daten gesendet werden sollen.

- Quell-Port gibt an, von welchen Ports gesendete (TX) oder empfangene (RX) Datenpakete an den Ziel-Port weiter geleitet werden sollen.

Nachdem Sie die jeweiligen Parameter eingestellt haben, klicken Sie auf den Übernehmen Button, um die Einstellungen zu speichern und anzuwenden.

Hinweis:
Deaktivieren Sie Port Mirroring im normalen Betrieb und verwenden Sie es nur zur Problemanalyse.

4.8 Redundanz

Die Seite Redundanz bietet Ihnen eine Übersicht über die verfügbaren Redundanzprotokolle und deren Status. Es ist nicht möglich, mehrere Redundanzprotokolle gleichzeitig zu aktivieren, daher kann nur eins den Status aktiv besitzen. Ist eines der beiden Protokolle aktiv erhalten Sie auf der Konfigurationsseite des anderen die Hinweismeldung: „ Die gleichzeitige Verwendung von MRP und RSTP ist nicht möglich“, Sie können dann auf dieser Seite keine Einstellungen vornehmen.
Mit Hilfe der Editier-Buttons gelangen Sie zu den Protokollen und können dort die Konfiguration durchführen, dabei stehen folgende Protokolle zur Verfügung:

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

Die Verwendung der Redundanzprotokolle garantiert Ihrem Netzwerk eine erhöhte Ausfallsicherheit und Verfügbarkeit im Fehlerfall.

4.8.1 Media Redundancy Protocol (MRP)

Das Media Redundancy Protocol (Abbildung 20) ist ein Ringprotokoll für hochverfügbare Netzwerke. Die MRP-Switches bilden über jeweils zwei dedizierte Ports einen Ring. Genau ein Switch im Ring wird als Redundanz Manager konfiguriert. Dieser Redundanz Manager testet mit speziellen Testpaketen die Durchgängigkeit des Rings und reaktiviert eine redundante Verbindung, wenn der Ring durch einen Fehler unterbrochen wird.
Die garantierte Rekonfigurationszeit bei bis zu 50 Geräten im Ring beträgt 200ms. In einer typischen

Anwendung beträgt die Rekonfigurationszeit normalerweise weniger als 50ms.

Achtung! Der Ring darf physikalisch erst geschlossen werden, wenn MRP vollständig konfiguriert ist.

Ring Konfiguration

Die folgenden Einstellungen sind bei MRP erforderlich:

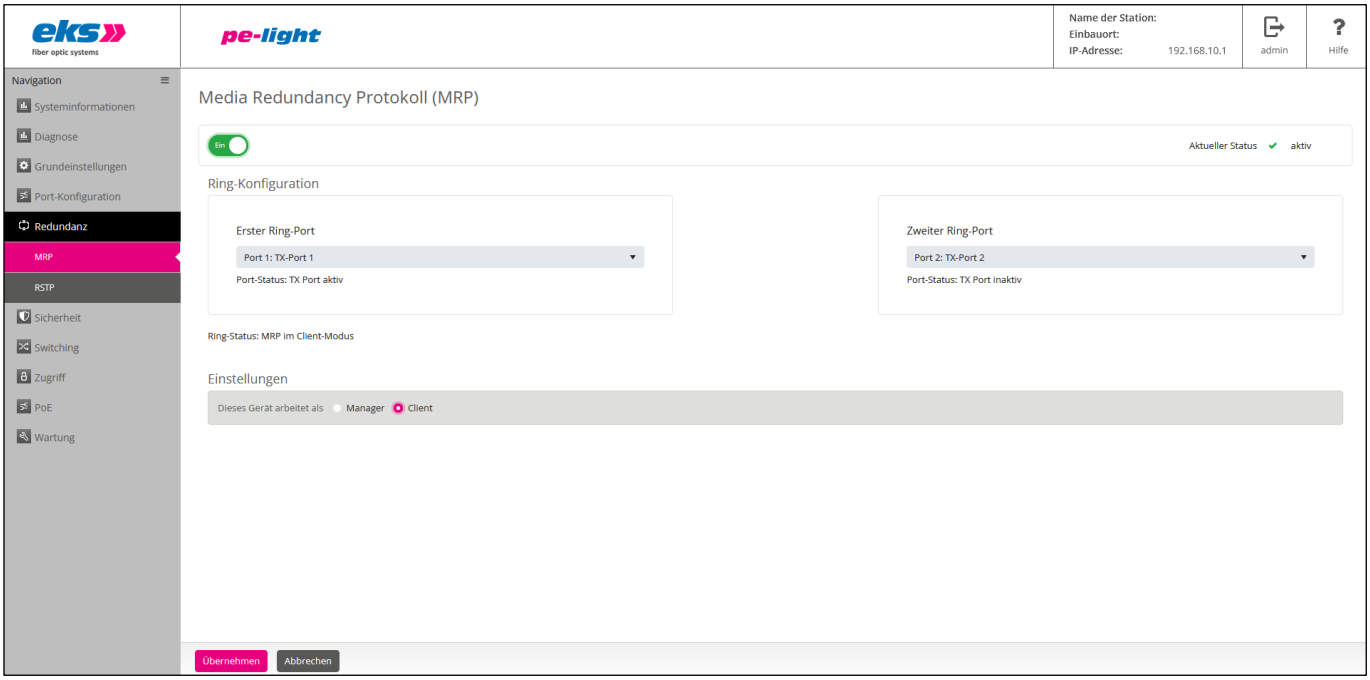


Abbildung 20: Media Redundancy Protokoll (MRP)

- Erster Ring-Port: Bitte wählen Sie einen Port aus, der als primärer Ring-Port arbeiten soll.
- Zweiter Ring-Port: Legen Sie einen zweiten Port fest, der als sekundärer Ring-Port arbeiten soll. Bitte beachten Sie, dass der sekundäre Ring-Port nicht gleichzeitig primärer Ring-Port sein kann.
- Ring-Einstellungen: Bitte legen Sie fest, ob der ***pe-light-S-switch*** als Manager oder als Client agieren soll. Bitte beachten Sie, dass pro Ring nur ein Manager verwendet werden darf.

Hinweis! Um die MRP Einstellungen zu aktivieren müssen Sie, nachdem Sie Ihre Einstellungen übernommen haben, MRP einmal aus und wieder anschalten.

4.8.2 Rapid Spanning Tree Protocol (RSTP)

Das Rapid Spanning Tree Protocol (RSTP) (Abbildung 22 / Abbildung 22) ist eine standardisierte Methode,

mit der beliebige Netzwerkstrukturen inklusive eines Ringes aufgebaut werden können. Das Protokoll bricht das Netzwerk in einen logischen Baum auf und deaktiviert redundante Pfade beziehungsweise aktiviert sie bei Bedarf wieder. Als erster Schritt wird dazu eine Root Bridge gewählt, die die Wurzel des aufzuspannenden Baums darstellt. Von der Root-Bridge ausgehend werden dann Pfade zu allen anderen Bridges im Netz festgelegt. Die Pfade, über die kommuniziert werden darf, werden anhand von Pfadkosten zu den einzelnen Bridges ermittelt.

Geräte-Einstellungen

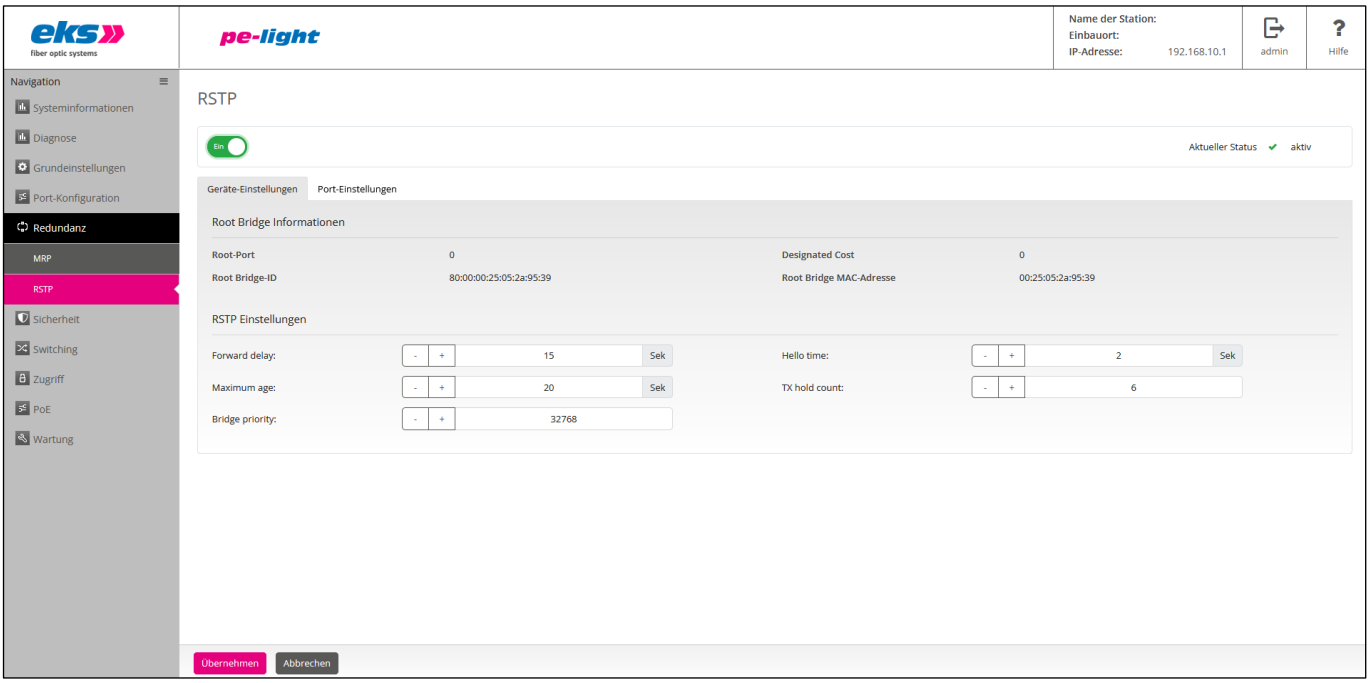


Abbildung 21: Rapid Spanning Tree Protocol – Geräte Einstellungen

Root Bridge Informationen

In diesem Feld werden die folgenden Parameter angezeigt:

- Root-Port: Zeigt an, welcher Port als Root-Port arbeitet, also die Verbindung mit den geringsten Pfadkosten zur Root-Bridge darstellt.
- Root Bridge-ID: Die Bridge-ID ist eine Kombination aus Bridge-Priority und MAC-Adresse einer Bridge. Die Bridge mit der geringsten Bridge-ID wird zur Root-Bridge gewählt. Root-Bridge-ID ist die Bridge-ID der gewählten Root-Bridge.
- Designated cost: Pfadkosten zur Root-Bridge
- Root Bridge MAC-Adresse: Zeigt die MAC-Adresse der Root Bridge an.

RSTP Einstellungen

Um den logischen RSTP-Baum kennenzulernen, geht jeder Port der Switches durch einen Ablauf von Portzuständen, bevor die Ports Nutzdaten übertragen. Die Zeitspanne, die die Ports in den einzelnen Zuständen verweilen, werden durch Timer bestimmt. Unter RSTP-Einstellungen können diese angepasst werden:

- Forward Delay: Die Wartezeit, bevor ein Port vom Status Learning/Listening (noch keine Übertragung von Nutzdaten) nach Forwarding (Übertragung von Nutzdaten) umschaltet. Es kann eine Zeit zwischen 4s und 30s eingegeben werden. In der Grundeinstellung beträgt der Forward Delay 15s.
- Maximum Age: Die Zeit, die eine Bridge vor dem Versuch einer Neukonfiguration wartet, wenn sie keine Nachrichten des Spanning Tree Konfigurations-Protokolls erhält. Es kann eine Zeit von 6s bis 40s eingegeben werden. In der Grundeinstellung beträgt Maximum Age 20s.
- Bridge Priority: Dieser Wert wird verwendet, um die Root-Bridge zu bestimmen. Die Bridge mit dem niedrigsten Wert wird zur Root-Bridge gewählt. Der Wert muss zwischen 0 und 61440 liegen und ein Vielfaches von 4096 sein. Änderungen dieses Wertes erfordern einen Neustart des Switches.
- Hello Time: Die Zeit, in der der Switch ein BPDU Paket (Bridge Protocol Data Unit) sendet, um den aktuellen Status des RSTP zu überprüfen. Es kann eine Zeit zwischen 1s und 10s eingegeben werden. In der Grundeinstellung beträgt die Hello Time 2s.
- TX Hold Count: Die maximale Anzahl der übertragenen Hello-Pakete eines Intervalls. Zur Auswahl stehen zwischen 1 und 10 Pakete. In der Grundeinstellung beträgt TX Hold Count 3.

Hinweis: Halten Sie sich an folgende Regel, um Forward delay, Maximum Age und Hello Time zu konfigurieren:

2 * (Forward Delay Time - 1) >= Maximum age >= 2 * (Hello Time + 1).

Empfohlene Vorgehensweise: Wählen Sie einen Wert für die "Hello Time" aus und berechnen Sie mit der Formel 2*(Hello Time + 1) nach der oben angegebenen Regel die untere Grenze von Maximum Age. Wählen Sie einen Wert für die "Forward Delay Time" aus und berechnen Sie mit der Formel 2*(Forward Delay Time - 1) der oben angegebenen Regel die obere Grenze von Maximum Age. Wählen Sie dann ein Maximum Age zwischen 6 und 40 Sekunden zwischen den berechneten Grenzen aus.

Nach dem Klicken auf Anwenden rekonfiguriert sich das RSTP-Protokoll und zeigt eventuell geänderte Root-Bridge-Parameter im oberen Bereich der Seite an.

Port-Einstellungen

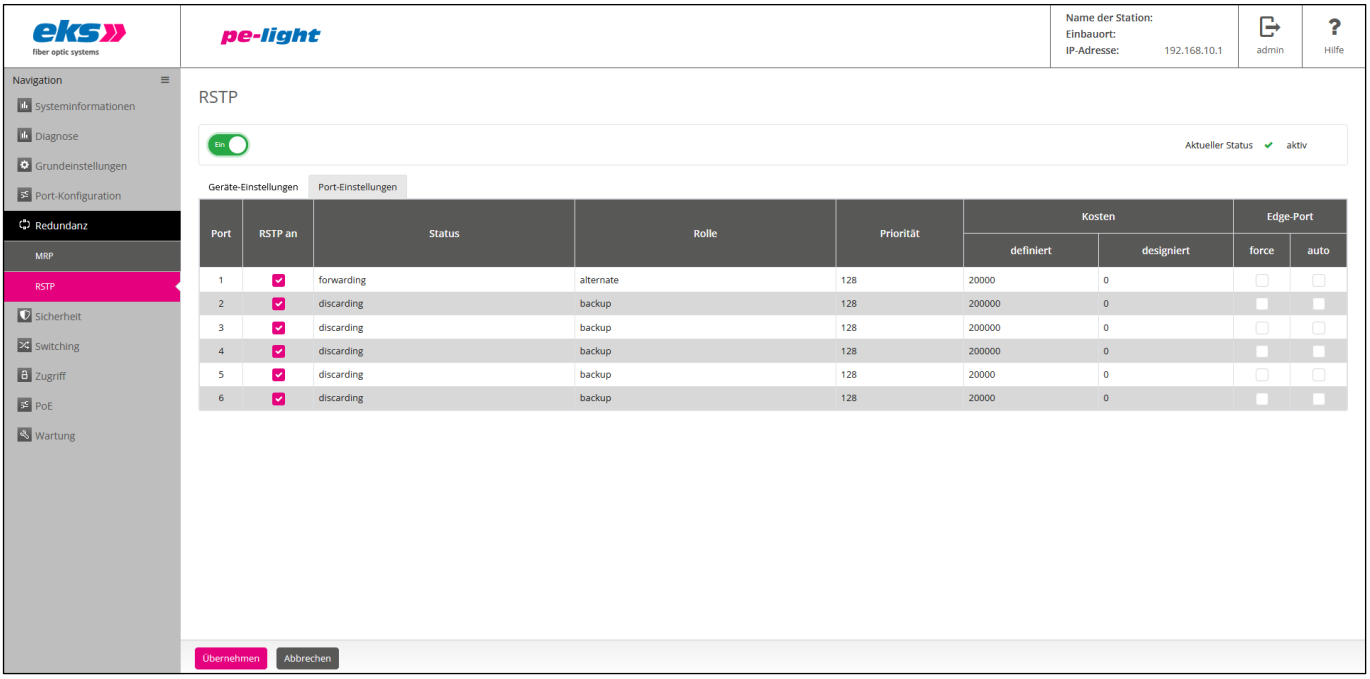


Abbildung 22: Rapid Spanning Tree Protocol – Port-Einstellungen

Unter dem Seitenreiter Port-Einstellungen können folgende Einstellungen vorgenommen werden:

- Port: Anzeige der Portnummer.
- RSTP an: Für jeden Port kann RSTP aktiviert oder deaktiviert werden.
- Status: In dieser Spalte wird der aktuelle Status der einzelnen Ports angezeigt. Dabei wird unterschieden zwischen:
  - Blocking: Verwirft Pakete; lernt keine Adressen; empfängt und verarbeitet keine BPDUs (Bridge Protocol Data Units = RSTP-Protokoll-Pakete)
  - Listening: Verwirft Pakete; lernt keine Adressen; empfängt, verarbeitet und überträgt BPDUs
  - Learning: Verwirft Pakete; lernt Adressen, empfängt; verarbeitet und überträgt BPDUs
  - Forwarding: Leitet Pakete weiter; lernt Adressen; empfängt, verarbeitet und überträgt BPDUs
  - Disabled: Verwirft Pakete; lernt keine Adressen; empfängt und verarbeitet keine BPDUs
- Rolle: Jeder Port kann in einem der folgenden Modi laufen:
  - Root Port: Ein Port im Forwarding-Zustand, der für die beste Baumstruktur ausgewählt wurde.
  - Designierter Port: Ein Port im Forwarding-Zustand, der für jedes geswitchte LAN-Segment ausgewählt wurde.
  - Alternativer Port: Ein alternativer Port zur Root-Bridge, der zusätzlich zum aktuellen Root-Port vorhanden ist.

- Backup Port: Ein Reservepfad, der über einen designierten Port in Richtung der Verästelungen der Baumstruktur bereitgestellt wird.
- Deaktivierter Port: Ein Port, der keine Betriebsfunktion in der Baum-Struktur hat.

- Priorität: Entscheidet, welcher Port bevorzugt behandelt wird, wenn die Pfadkosten zu mehreren Ports gleich sind. Priorität muss ein Vielfaches von 16 zwischen 0 und 240 sein.
- Kosten: Die Pfadkosten von dieser Bridge zur gegenüberliegenden Bridge. Die Kosten können zwischen 1 und 200.000.000 liegen.
  - definiert: Die Kosten der Verbindung zur Root-Bridge können vorgegeben werden, um Kabellängen oder maximale Datenraten zu berücksichtigen.
  - designiert: Berechnete Pfadkosten.
- Edge-Port: Bezeichnet einen Port, der direkt mit einer Endstation verbunden ist. Diese Ports können keine Schleifen verursachen und wechseln daher sofort in den Modus Forwarding. Die Statusänderung eines Edge-Ports führt auf keinen Fall zu einer Änderung der Topologie.
  - Force: Der Port wird standardmässig als Edge-Port konfiguriert.
  - Auto: Die Konfiguration als Edge-Port erfolgt automatisch.

Nach dem Einstellen der RSTP-Paramter müssen sie durch Klick auf den Anwenden-Button gespeichert werden.

4.9 Switching

Die Seite Switching bietet ihnen einen Überblick über die aktivierten und deaktivierten Funktionen im Bereich Switching.

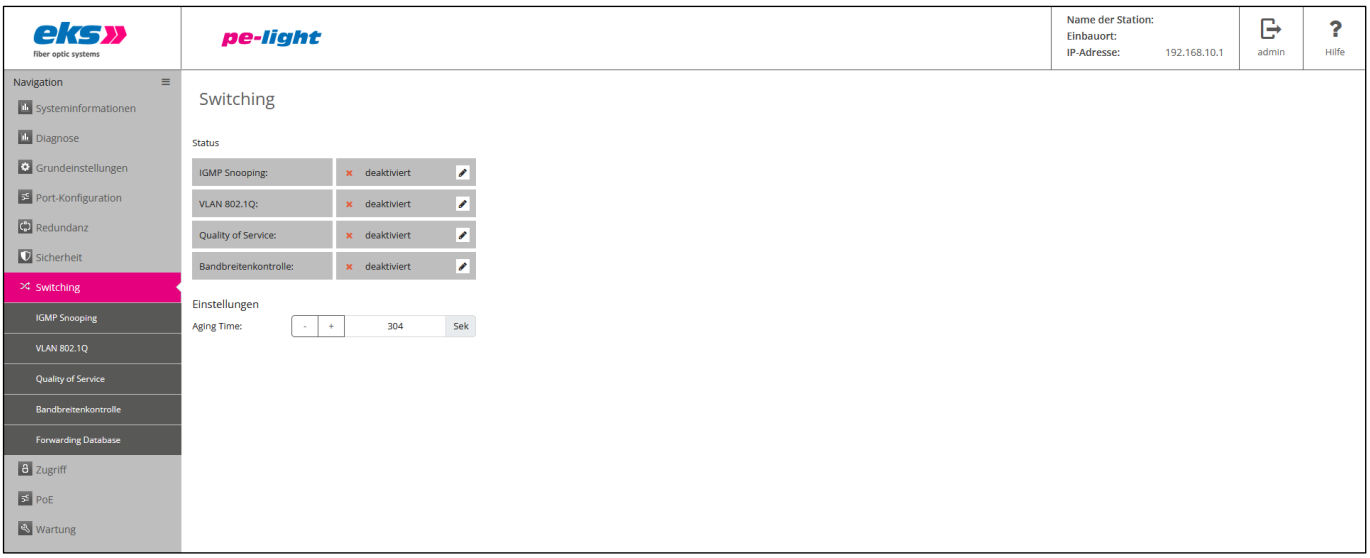


Abbildung 23: Seite Switching

Aging Time: Gibt den Zeitraum an, indem eine MAC-Adresse nach dem Entfernen vom Port oder Abschalten des Gerätes noch erhalten bleibt. Sie können Werte zwischen 16 und 4080 Sekunden wählen, in Schritten von jeweils 16 s.

4.9.1 IGMP Snooping

Das Internet Group Management Protocol (IGMP) wird von Switches, Routern und Hosts verwendet, um Multicastgruppen einzurichten. Multicast-Datenverkehr muss bei aktiviertem IGMP nicht mehr zu jedem einzelnen Multicast-Empfänger geschickt werden, sondern nur noch zu jeder Gruppe. Die Netzlast wird dadurch stark reduziert.

IGMP-Snooping arbeitet auf Layer 3 des OSI-Modells und wird durch das Layer 2-Protokoll IGMP-Snooping erweitert. IGMP-Snooping hört dem IGMP-Datenverkehr zu und lernt, über welche Ports welche Multicast-Daten verschickt werden müssen.

IGMP-Snooping-Einstellungen

Folgende Einstellungen werden angezeigt oder können angepasst werden:

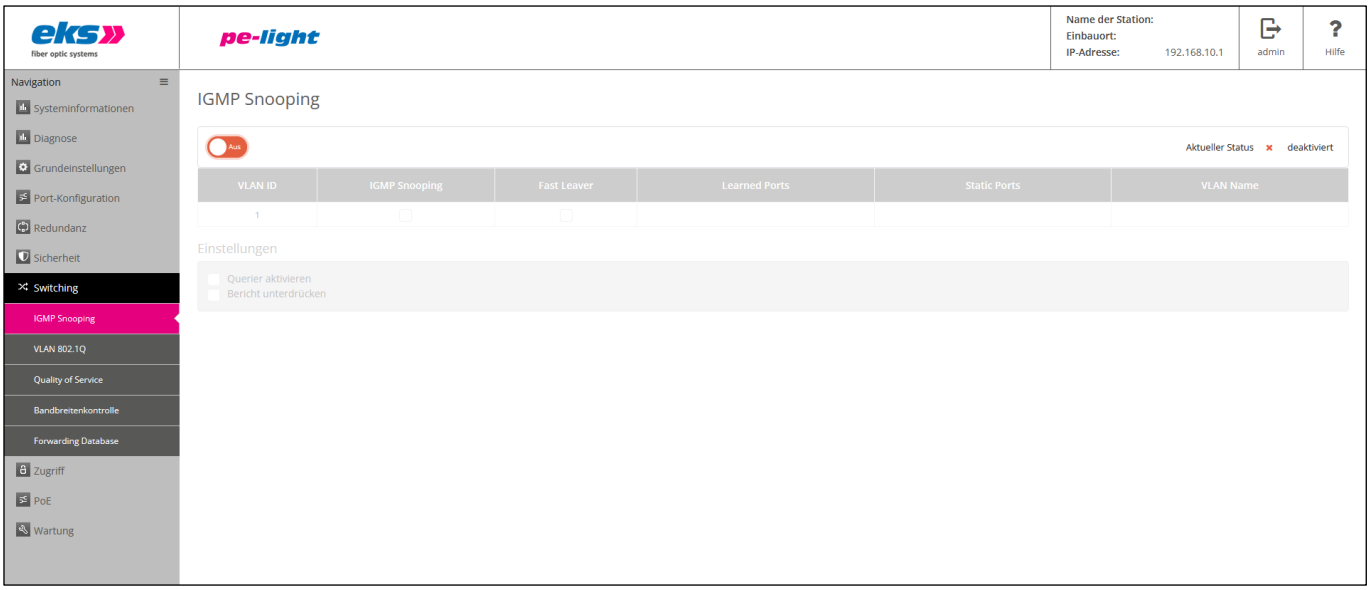


Abbildung 24: IGMP Snooping

- VLAN ID: IGMP Snooping operiert auf VLAN Basis und kann für jede einzelne VLAN ID aktivert werden.
- Fast Leaver: Wenn eine Multicast-Gruppe entfernt werden soll, wird normalerweise nachgefragt, ob wirklich kein Teilnehmer mehr in der Gruppe vorhanden ist (Query-Message). Fast Leaver ist ein Port, der die Multicast-Gruppe ohne weitere Nachfrage entfernt. Interessant ist diese Einstellung für Ports, an die nur ein Multicast-Empfänger angeschlossen ist.
- Learned Ports: Zeigt, an welchen Ports Multicast-Empfänger verbunden sind und an welchen Ports dementsprechend die Multicast-Daten weitergeleitet werden.
- Static Ports: Frei konfigurierbare Ports, die unabhängig von IGMP-Nachrichten immer Multicast-Daten empfangen sollen.
- VLAN Name: Der Name des VLANs.

Weitere Einstellungen

- Querier aktivieren: Sollte sich kein Multicast Router im VLAN befinden und die IGMP-Anfragen (Queries) versenden, kann hier konfiguriert werden, dass von diesem Switch Query-Pakete erzeugt werden sollen.
- Bericht unterdrücken: Treten Empfänger Multicast-Gruppen bei oder verlassen sie, dann übermitteln sie Status-Berichte über das IGMP-Protokoll. Diese Statusdaten können vom IGMP-Snooping Protokoll gebündelt werden, indem „Bericht unterdrücken“ aktiviert wird. Durch die Beschränkung auf notwenige Berichte wird die Netzlast verringert.

4.9.2 **VLAN 802.1Q**

Ein Virtuelles LAN (VLAN) ist eine Gruppe von Ports, die irgendwo im Netzwerk sein können, aber so kommunizieren, als ob sie im gleichen Bereich wären. VLANs können verwendet werden, um Abteilungen (R&D, Marketing), Anwendungen (z.B. email) oder Multicast-Gruppen für Videoübertragungen zu trennen und das Netzwerkmanagement dadurch zu vereinfachen.

Beim VLAN nach 802.1Q werden Ethernet-Datenpakete mit einem VLAN-Tag versehen, einer Erweiterung, die unter anderem eine VLAN-ID, eine eindeutige Nummer des VLAN enthält, zu dem das Datenpaket gehört. Welche Ports Datenpakete eines VLAN mit VLAN-Tag und welche Ports Datenpakete eines VLAN ohne VLAN-Tag versenden sollen und welche Ports dem VLAN zugeordnet sind, kann im Web-Interface-Menü VLAN komfortabel konfiguriert und übersichtlich angezeigt werden.

Tab VLANs

Sie bekommen übersichtlich angezeigt, welche VLANs angelegt sind und wie sie konfiguriert sind. So können sie auf einen Blick erkennen, wie viele VLANs angelegt sind.

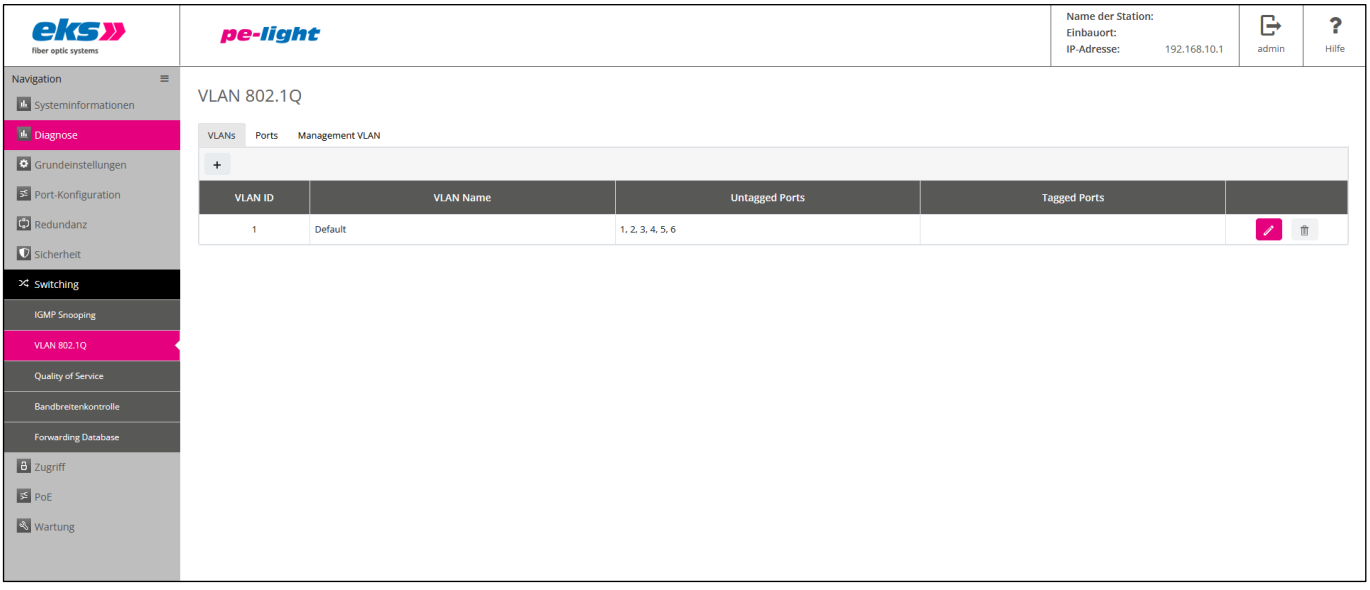


Abbildung 25: VLAN 802.1Q

Zudem können Sie hier neue VLANs angelegen, konfigurieren und löschen. Dazu werden beim Hinzufügen von VLANs mit dem „+“-Button oder beim Editieren mit dem Editier-Button folgende Einstellungen vorgenommen:

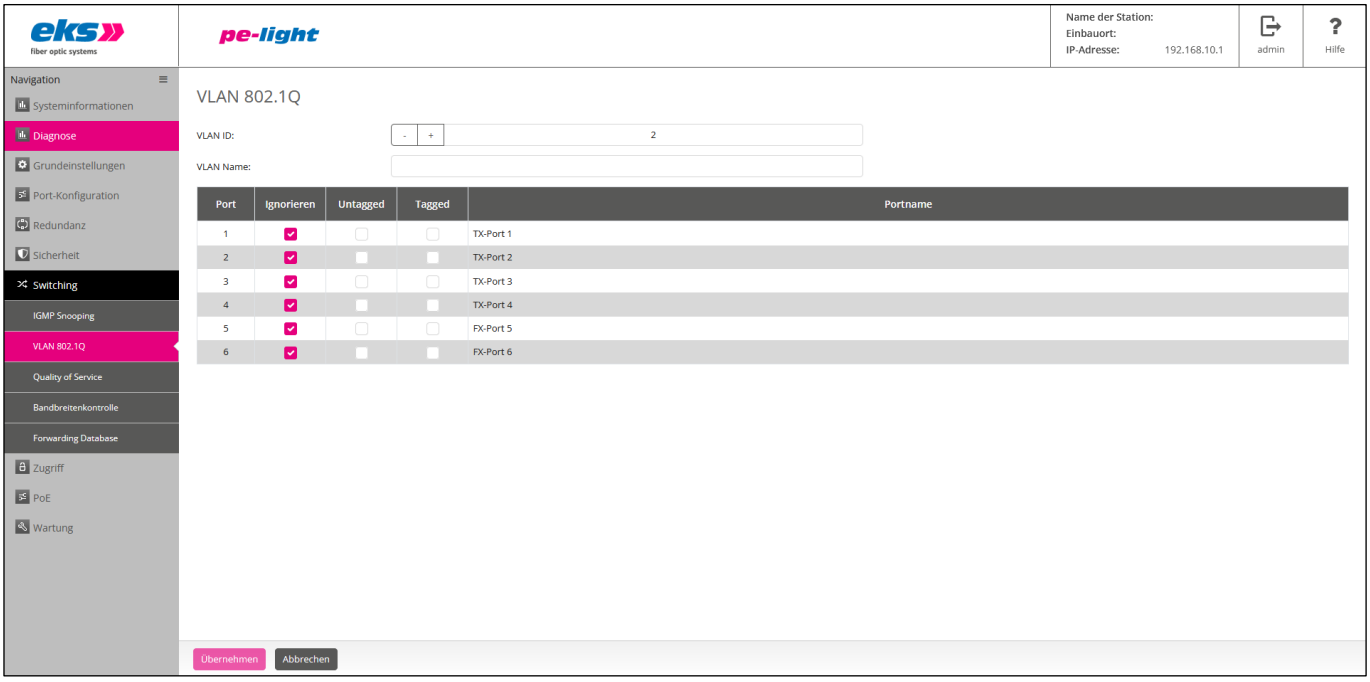


Abbildung 26: VLAN anlegen / editieren

- **VLAN ID**: Diese Identifikationsnummer ist einem VLAN eindeutig zugeordnet. VLAN IDs zwischen 1 und 4094 sind möglich. (Nur wenn das VLAN neu angelegt wird, beim Editieren ist dieser Eintrag fest.)
- **VLAN Name:** Ein beliebiger Name für das VLAN.
- **Einstellungen für den jeweiligen Port:** Sie können anhaken, ob der Port in diesem VLAN ignoriert wird oder ob über ihn tagged bzw. untagged Pakete versendet werden.

Mit dem Lösch-Button können beliebige VLANs außer das Default VLAN (VLAN ID 1) gelöscht werden.

Tab Ports

Diese Seite bietet einen übersichtlichen Überblick über die Zuordnung der Ports des ***pe-light-S-switches*** zu den konfigurierten VLANs. Für jeden Port ist eine eigene Zeile vorgesehen, und in den Spalten „Untagged in VLANs“ sowie „Tagged in VLANs“ wird aufgeführt, in welchen VLANs (VLAN IDs) der jeweilige Port in diesem Status enthalten ist. So können sie auf einen Blick erkennen, wie vielen VLANs die jeweiligen Ports zugeordnet sind.

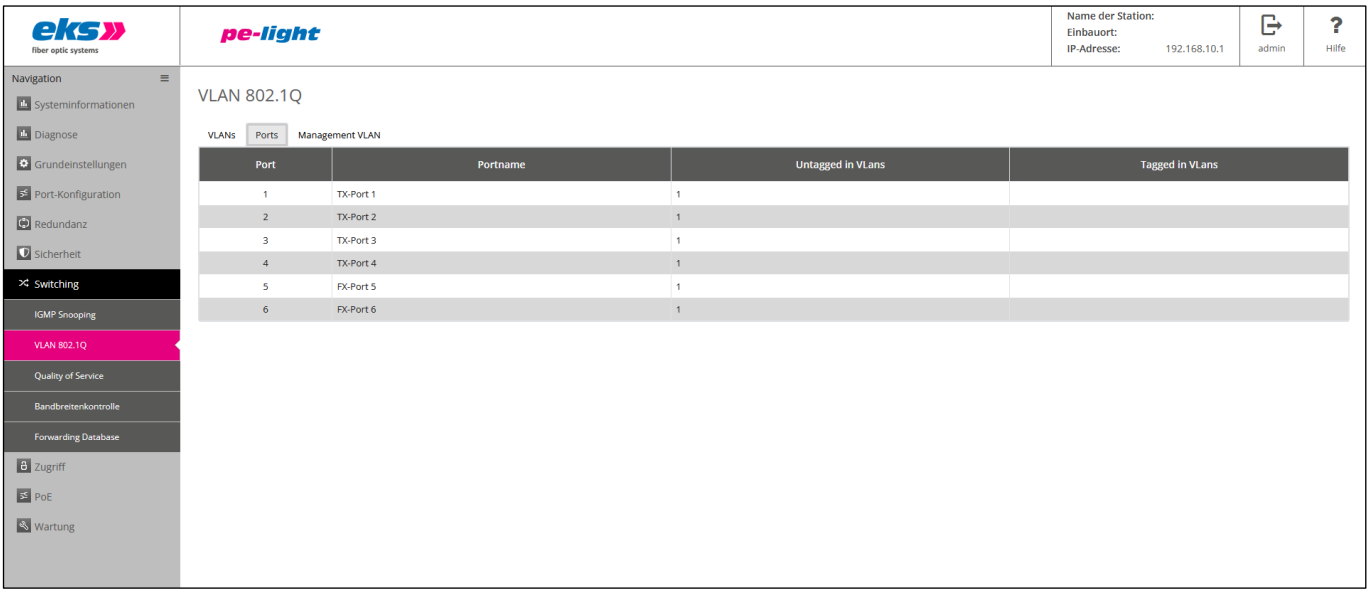


Abbildung 27: VLAN - Portübersicht

Tab Management VLAN

Hier können Sie konfigurieren, welches VLAN als Management VLAN festgelegt werden soll. Der Zugriff auf das Gerät, beispielsweise über das Webinterface, ist ausschließlich über die dem Management VLAN zugeordneten Ports möglich.

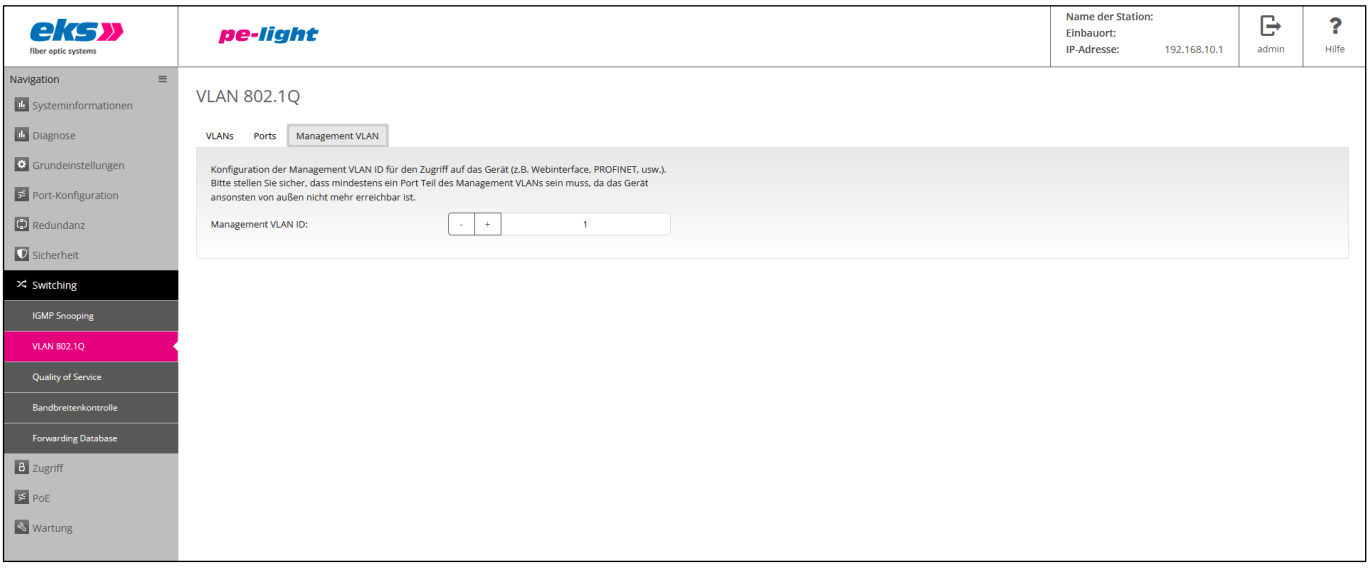


Abbildung 28: VLAN - Zuordnung Management VLAN

Verwendung von VLANs nach VLAN 802.1Q

Werden an einem Port Datenpakete empfangen, die keinen VLAN-Tag enthalten, so erhalten sie für die interne Verarbeitung die VLAN-ID des VLAN, für das der Empfangsport untagged konfiguriert ist. Jeder Port

kann daher nur für ein VLAN untagged konfiguriert werden. Werden Datenpakete empfangen, die einen VLAN-Tag enthalten, so werden sie verworfen, wenn ihre VLAN-ID weder der Default-VLAN-ID noch der VLAN-ID eines VLAN entspricht, dem der Empfangsport tagged oder untagged zugeordnet ist.

Intern haben somit alle eingehenden Datenpakete eine VLAN-ID. Diese interne VLAN-ID entscheidet darüber, auf welchen Ports die Datenpakete ausgegeben werden. Daten des Default-VLAN werden auf allen Ports ausgegeben, Daten anderer VLANs nur auf Ports, die dem VLAN mit der VLAN-ID der Datenpakete zugeordnet sind.
Ob die Datenpakete mit oder ohne VLAN-Tag verschickt werden, wird durch die Art der Zuordnung der Ports zum VLAN entschieden. Ist ein Port einem VLAN tagged zugeordnet, dann werden Datenpakete mit der VLAN-ID des VLAN auf dem entsprechenden Port mit VLAN-Tag verschickt. Ist er dem VLAN untagged zugeordnet, dann werden die Pakete auf dem Port ohne VLAN-Tag verschickt.

Achtung! Pakete des Default-VLAN werden auf allen Ports ausgegeben. Das Default-VLAN sollte daher allenfalls für Management-Pakete verwendet werden. Ports ohne VLAN-Zuordnung müssen einem VLAN zugeordnet werden, das nicht verwendet wird, damit Pakete, die auf diesen Ports empfangen werden, nicht ins Default VLAN gelangen können (siehe **Fehler! Verweisquelle konnte nicht gefunden werden.**).

Achtung! Pakete mit VLAN-ID 1 werden auf allen Ports empfangen und auf allen Ports ausgegeben.

4.9.3 **Quality of Service (QoS)**

Quality of Service (Abbildung 29) beeinflusst den Datenverkehr im Switch so, dass Dienste dem Empfänger mit einer festgelegten Qualität zur Verfügung stehen. Dazu werden Datenpakete abhängig von Prioritätsangaben aus verschiedenen Priorisierungsverfahren (Portbasiert, Class of Service, Type of Service) in vier Prioritäts-Schlangen einsortiert, die am Ausgang entsprechend eines Prioritätsmodus (strikt oder gewichtet) geleert werden.

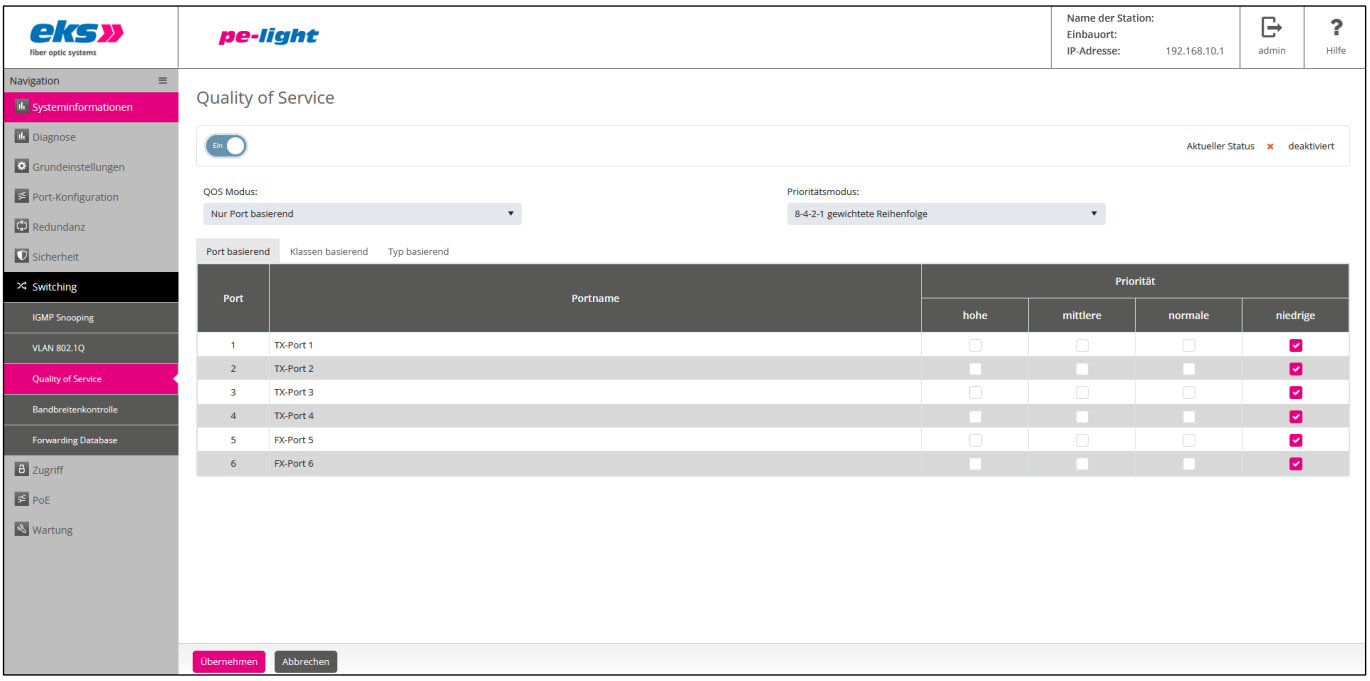


Abbildung 29: Quality of Service

Priorisierungsverfahren:

- Nur Port basierend: Die Priorisierung erfolgt ausschliesslich anhand der Priorität der Ports.
- Nur Class of Service (CoS) (Klassen basierend): Die Priorisierung erfolgt anhand des CoS-Felds im VLAN-Tag der Datenpakete. Nicht VLAN-Pakete werden in die Prioritäts-Schlange niedrigster Priorität geleitet.
- Nur Type of Service (ToS) (Typ basierend): Die Priorisierung erfolgt anhand des ToS-Felds im IP-Header von IP-Datenpaketen. Pakete ohne ToS-Feld bzw. Nicht-IP-Pakete werden in die Prioritäts-Schlange niedrigster Priorität geleitet.
- Class of Service zuerst: Pakete mit CoS-Information im VLAN-Tag werden danach priorisiert. Pakete ohne CoS-Information werden nach ToS-Feld im IP-Header oder bei fehlendem ToS-Feld nach Portpriorität priorisiert.
- Type of Service zuerst: Pakete mit ToS-Feld im IP-Header werden danach priorisiert. Pakete ohne ToS-Feld werden nach CoS-Feld im VLAN-Tag oder bei fehlendem VLAN-Tag nach Portpriorität priorisiert.

Prioritätsmodus:

- Striktes Prioritätsschema: Beim strikten Prioritätsschema werden erst alle Pakete aus einer hohen Prioritäts-Schlange verschickt, bevor Pakete aus der nächst niedrigeren Prioritäts-Schlange verschickt werden.

- 8-4-2-1 gewichtete Reihenfolge: Nachdem 8 Pakete der höchsten Prioritäts-Schlange verschickt wurden, werden 4 Pakete der zweithöchsten, 2 Pakete der dritthöchsten und 1 Paket der niedrigsten Prioritäts-Schlange verschickt. Durch dieses Vorgehen werden extreme Wartezeiten der Pakete niedriger Priorität vermieden.

Hinweis: Bei Verwendung von Quality of Service sollte die Flusskontrolle abgeschaltet werden, da bei aktivierter Flusskontrolle Datenpakete unabhängig von der Priorität gedrosselt übertragen werden (siehe Abschnitt 4.7).

4.9.4 Bandbreitenkontrolle

Die Bandbreitenkontrolle kann dazu verwendet werden, verschiedene Typen von Paketen auf eine einstellbare Datenrate zu begrenzen. So kann beispielsweise sichergestellt werden, dass übermäßig viele Broadcast-Pakete (Pakete, die an alle Teilnehmer geschickt werden) nicht den normalen Unicast-Datenverkehr (Pakete, die nur an einen Teilnehmer geschickt werden) stören.

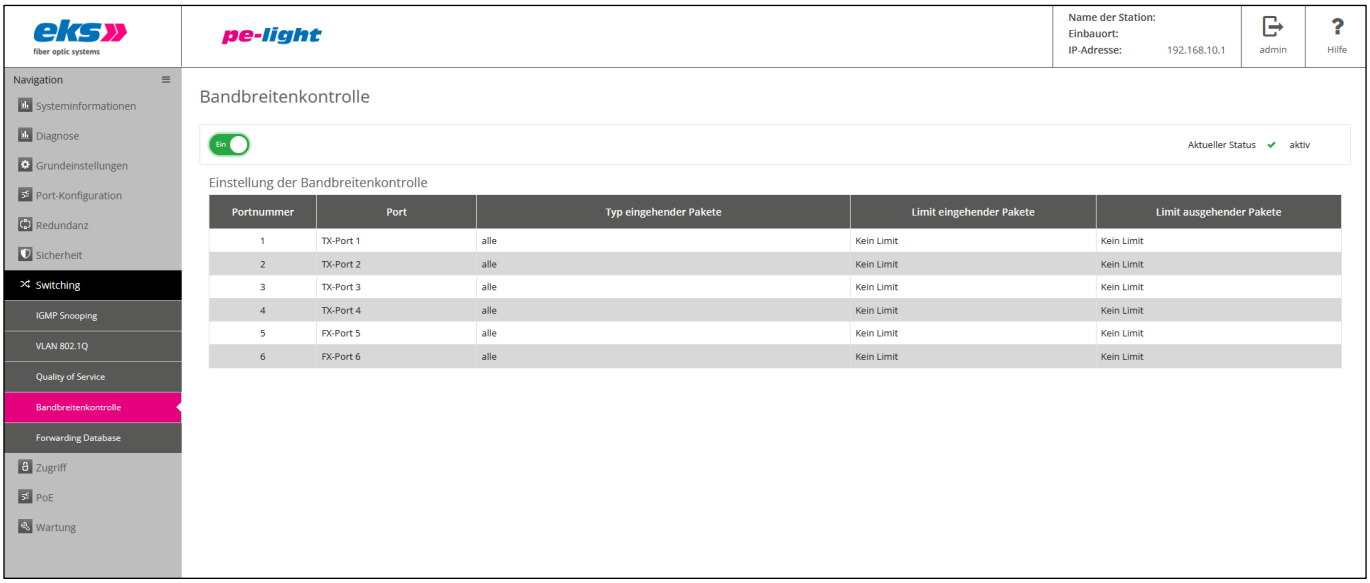


Abbildung 30: Einstellung der Bandbreitenkontrolle

Folgende Einstellungen können pro Port vorgenommen werden:

- Port: Gibt die Portnummer an.
- Typ eingehender Pakete: Gibt an, welche Arten von Datenpaketen begrenzt werden sollen:
  - Alle: Alle Pakete werden limitiert.
  - Broadcasts: Nur Broadcast-Pakete werden limitiert.

- Multicasts: Nur Multicast-Pakete (Pakete an Empfänger-Gruppen) werden limitiert.
- Unbekannte Unicasts: Nur Unicast-Pakete unbekannter Empfänger werden limitiert.

» Limit eingehender Pakete: Die Datenraten-Limitierungen der Eingangsdaten. Möglich sind 128kBit/s, 256kBit/s, 512kBit/s, 1MBit/s, 2MBit/s, 4MBit/s und 8MBit/s. Als Standardwert ist "Kein Limit" definiert.

» Limit ausgehender Pakete: Die Datenraten-Limitierungen für abgehende Pakete. Sie beziehen sich immer auf alle Paketarten. Möglich sind 128kBit/s, 256kBit/s, 512kBit/s, 1MBit/s, 2MBit/s, 4MBit/s und 8MBit/s. Als Standardwert ist "Kein Limit" definiert.

Die gewünschten Einstellungen können durch den Anwenden-Button gespeichert werden.

4.9.5 Forwarding Database

Eine Forwarding Database, auch bekannt als Weiterleitungstabelle oder MAC-Tabelle, ist eine wichtige Komponente in Netzwerken. Sie wird verwendet, um herauszufinden, an welchen Port ein Datenpaket weitergeleitet werden soll.

Die Tabelle wird automatisch aktualisiert, basierend auf den MAC-Adressen der Geräte im Netzwerk. Wenn sich ein neues Gerät verbindet, werden seine Adresse und der zugehörige Port hinzugefügt.

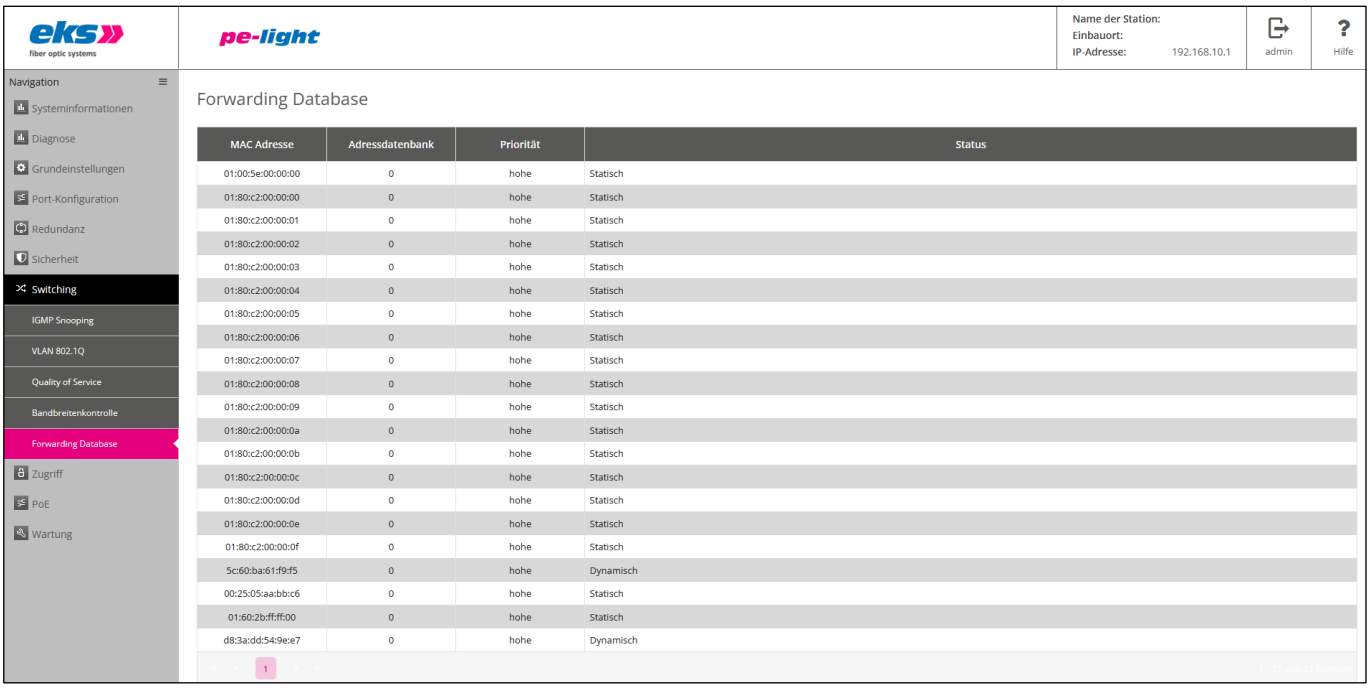


Abbildung 31: Forwarding Database

Der ***pe-light-S-switch*** ermöglicht es Ihnen in diesem Menü, die intern gespeicherte Forwarding Database

einzusehen. In dieser Datenbank sind die vom ***pe-light-S-switch*** gelernten MAC-Adressen aufgeführt, zusammen mit der zugehörigen Adressdatenbank, der Priorität, mit der sie angelegt wurden, und dem Status. Ein statischer Status bedeutet, dass die Einträge manuell konfiguriert wurden und unverändert bleiben. Im Gegensatz dazu bedeutet ein dynamischer Status, dass der ***pe-light-S-switch*** die Einträge automatisch basierend auf dem Netzwerkverkehr erstellt hat.

4.10 Zugriff

Im Menüpunkt Zugriff wird festgelegt, über welche Wege auf den ***pe-light-S-switch*** zugegriffen werden darf.

Abbildung 32: Auswahl der verschiedenen Zugriffsmöglichkeiten

- Ping: Um zu überprüfen, ob das Gerät in Ihrem Netzwerk erreichbar ist, können Sie dem Gerät Anfragen senden, auf die es eine Antwort zurücksendet. Die Antworten auf diese Ping-Pakete werden unterdrückt, wenn Sie unter Zugriff Ping deaktivieren.
- Device Identifier: Um ein Gerät im Netzwerk zu identifizieren blinken die Status LEDs (PWR, Fail und Door Contact) mit einer Frequenz von 1 Hz für 30 Sekunden.

Einstellungen

Hier gibt es drei Einstellmöglichkeiten, um den Zugriff auf das Webinterface des ***pe-light-S-switches*** zu konfigurieren und die Möglichkeit ein eigenes HTTPS-Zertifikat hochzuladen und zu nutzen.

- Zeit bis zum automatischen Logout: Die Zeit bis zum automatischen Logout legt fest, wie lange eine Sitzung im Webmanagement ohne Aktivität bestehen bleibt, bis ein automatischer Logout erfolgt. Die Zeit kann zwischen 3 Minuten und 30 Minuten konfiguriert werden.

- Webgui Access Mode:
  - http: Auf das Webinterface des ***pe-light-S-switches*** kann nur unverschlüsselt zugegriffen werden.
  - https: Auf das Webinterface des ***pe-light-S-switches*** kann nur verschlüsselt zugegriffen werden. Dazu wird ein gültiges https Zertifikat benötigt.
  - http und https: Auf das Webinterface des ***pe-light-S-switches*** kann sowohl verschlüsselt als auch unverschlüsselt zugegriffen werden.
- Eigenes HTTPS-Zertifikat verwenden: Es kann eingestellt werden, dass ein HTTPS-Zertifikat hochgeladen und genutzt werden soll. Wird der Haken gesetzt bekommen Sie die Möglichkeit ein HTTPS-Zertifikat hochzuladen. Dieses wird dann genutzt. Wird der Haken wieder entfernt wird das HTTPS-Zertifikat wieder vom Gerät gelöscht und stattdessen das standard HTTPS-Zertifikat verwendet.

Mit dem Übernehmen-Button werden die Einstellungen gespeichert.

4.10.1 Simple Network Management Protocol (SNMP)

Das Simple Network Management Protocol (SNMP) dient zur Überwachung und Steuerung von Netzwerkelementen durch eine zentrale Station. Welche Einstellungen in einem Netzwerkelement vorgenommen und welche Werte abgefragt werden können, ist nicht im SNMP definiert, sondern in sogenannten MIBs (Management Information Base)

Neben einigen allgemeingültigen MIBs gibt es zu den meisten Geräten herstellerspezifische MIBs mit gerätespezifischen Informationen. Die gerätespezifische MIB für den ***pe-light-S-switch*** kann auf der Seite Wartung unter der Rubrik Lizenzen heruntergeladen werden.

Der ***pe-light-S-switch*** unterstützt sowohl SNMP V1/2c als auch SNMP V3.

- SNMP V1/2c: SNMP-Anfragen werden von der Managementstation mit einem sogenannten Community-String verschickt, der eine einfache Zugriffsbeschränkung darstellt. Nur auf Anfragen mit einem Community-String, der zu den im Switch definierten Community-Strings passt, wird geantwortet. Da der Community-String im Klartext über das Netzwerk geschickt wird, erhöht seine Verwendung die Sicherheit nicht zwangsläufig.
- SNMP V3: Im Vergleich zu SNMP V1/2c bietet SNMP V3 verbesserte Sicherheitsmerkmale, einschließlich Authentifizierung, Verschlüsselung und Integritätsschutz. Diese Funktionen sorgen dafür, dass nur autorisierte Benutzer auf Netzwerkdaten zugreifen können und dass die übertragenen Informationen während der Kommunikation geschützt und unverändert bleiben.

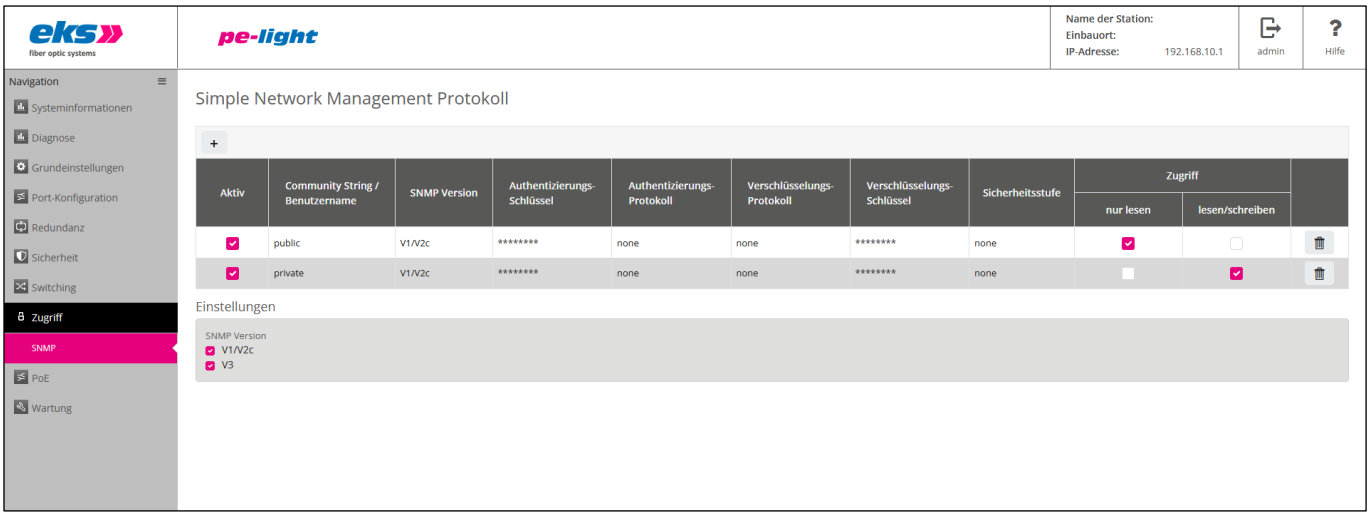


Abbildung 33: Übersicht der aktuell vorhandenen SNMP Zugänge

SNMP Zugänge anlegen

Im SNMP-Menü (Abbildung 33) des ***pe-light-S-switches*** können weitere Zugänge angelegt werden. Dazu wird durch Anwählen des „+“-Buttons ein neuer View geöffnet, in dem Sie zunächst den Name und das Zugriffslevel für den Zugang setzen können. Standardmäßig werden neue Einträge immer als SNMP V1/2c angelegt.

SNMP Zugänge löschen

Im SNMP-Menü (Abbildung 33) des ***pe-light-S-switches*** können weitere Community-Strings gelöscht werden. In dem rechts neben dem Eintrag auf den kleinen „Mülleimer“-Button geklickt wird, wird der Eintrag zum Löschen markiert. Mit dem Übernehmen-Button werden die Einstellungen übernommen und der Eintrag gelöscht.

SNMP Zugänge konfigurieren

Im SNMP-Menü (Abbildung 33) des ***pe-light-S-switches*** können die bestehenden Community-Strings bearbeitet werden. Folgende Einstellungen können dabei konfiguriert werden:

Für SNMP V1/2c und SNMP V3:

- Aktiv: Zeigt an welche Community Strings aktiviert sind und welche nicht
- Community String: Die Zugänge sind durch eindeutige Namen definiert, die hier eingestellt werden können. Maximal kann ein Name 32 Zeichen lang sein.
- SNMP Version: Gibt an welche SNMP Version dieser Zugang nutzt.

- Nur Lesen: Anfragen mit diesem Community-String werden beantwortet, können aber keine Einstellungen am Switch vornehmen.
- Lesen und Schreiben: Anfragen mit diesem Community-String werden beantwortet und können Einstellungen am Switch vornehmen.
- Entfernen: Löschen des Community-Strings

Zusätzlich für SNMP V3:

- Sicherheitsstufe: SNMP V3 bietet 3 verschiedene Sicherheitsstufen an.
  - NoAuthNoPriv: In dieser Stufe werden keine Authentifizierungs- und Verschlüsselungsmechanismen angewendet. Folglich sind keine Angaben für Authentifizierungs-Protokoll und Authentifizierungs-Key, sowie für Verschlüsselungs-Protokoll und Verschlüsselungs-Key zu tätigen.
  - AuthNoPriv: In dieser Stufe wird eine Authentifizierung durchgeführt, jedoch keine Verschlüsselung. Demnach müssen ein Authentifizierungs-Protokoll und ein Authentifizierungs-Key für diesen Eintrag gesetzt werden. Für Verschlüsselungs-Protokoll und Verschlüsselungs-Key sind keine Angaben zu tätigen.
  - AuthPriv: Diese Stufe bietet Authentifizierungs- und Verschlüsselungsmechanismen. Daher müssen sowohl ein Authentifizierungs-Protokoll und ein Authentifizierungs-Key wie auch ein Verschlüsselungs-Protokoll und ein Verschlüsselungs-Key, gesetzt werden.
- Authentifizierungs-Protokoll: Das Authentifizierungs-Protokoll stellt sicher, dass nur autorisierte Benutzer auf die SNMP-Daten zugreifen können, indem es die Anmeldedaten (Benutzername und Authentifizierungs-Key) überprüft. Es gewährleistet, dass die übertragenen Daten nicht manipuliert wurden. Bei der Übertragung wird ein Hash-Wert (z. B. HMAC) erstellt, um die Integrität der Nachricht zu überprüfen. SNMP V3 bietet zwei Authentifizierungs-Protokolle:
  - MD5: Ein älteres Authentifizierungsprotokoll, das einen Hash-Wert zur Authentifizierung erstellt. Es gilt jedoch als weniger sicher, da es anfällig für Kollisionen ist.
  - SHA: Ein moderneres und sichereres Authentifizierungsprotokoll, dass bessere Sicherheitsmerkmale bietet und gegen viele Angriffe robuster ist.
- Authentifizierungs-Key: Geben Sie hier das für die Authentifizierung erforderliche Passwort ein. Das Passwort muss mindestens 8-Stellig sein
- Verschlüsselungs-Protokoll: Das Verschlüsselungs-Protokoll ist entscheidend für die Sicherstellung der Datensicherheit. SNMP V3 bietet zwei Verschlüsselungsprotokolle:

- Data Encryption Standard (DES): Ein älteres Verschlüsselungsverfahren, das eine 56-Bit-Schlüssellänge verwendet
- Advanced Encryption Standard (AES): Ein modernes und sichereres Verschlüsselungsverfahren, das eine stärkere Sicherheit bietet und als aktueller Standard für die Datenverschlüsselung angesehen wird.

Verschlüsselungs-Key: Geben sie hier das für die Verschlüsselung erforderliche Passwort ein. Das Passwort muss mindestens 8-Stellig sein.

Einstellungen

Sie können wählen welche SNMP Version (V1/2c oder V3) aktiv ist. Dabei ist es möglich nur eine Version zu aktivieren oder aber beide Versionen parallel. Ist keine Version aktiv, so wird SNMP deaktiviert.

Speichern Sie die Einstellungen durch Anklicken des Übernehmen-Buttons.

4.11 PoE (Power over Ethernet)

In diesem Menüpunkt erhalten Sie einen umfassenden Überblick über den PoE-Status des ***pe-light-S-switches***, unterteilt in den Systemstatus (Informationen über bereitgestellte und abgenommene Leistung), Informationen zum PoE Chip und Informationen über die einzelnen Ports. Es wird Ihnen für jeden Port der aktuelle Staus, mit umfangreichen Informationen angezeigt, zudem können Sie die Ports einzeln aktivieren, bzw. deaktivieren und ihnen eine Priorität vergeben.

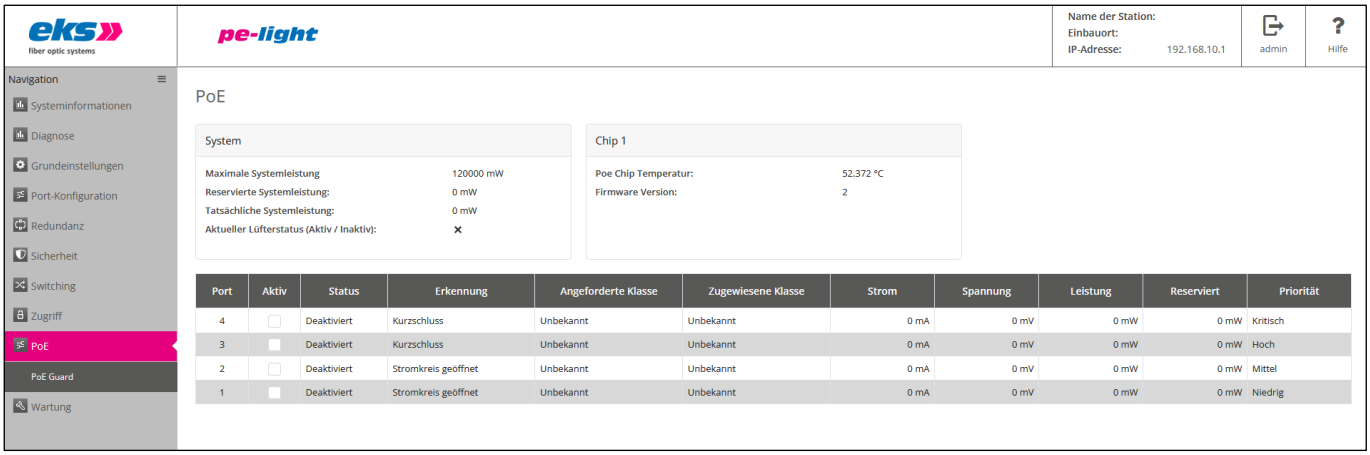


Abbildung 34: PoE

Folgende Informationen werden Ihnen angezeigt:

System

- Maximale Systemleistung: Gibt die maximale Leistung in mW an, die der ***pe-light-S-switch***, verteilt auf alle PoE Ports bereitstellt.
- Reservierte Systemleistung: Gibt die Leistung in mW an, die vom ***pe-light-S-switch*** für die angeschlossenen PoE-Geräte bereitgestellt wird. Sie wird im Voraus festgelegt, um sicherzustellen, dass genügend Energie für alle Geräte verfügbar ist
- Tatsächliche Systemleistung: Gibt die Leistung in mW an, die von den angeschlossenen PoE-Geräten tatsächlich verbraucht wird. Sie variiert je nach Bedarf der Geräte zu einem bestimmten Zeitpunkt.
- Aktueller Lüfterstatus (Aktiv/Inaktiv): Zeigt an, ob der Lüfter aktiv ist.

Chip1

- PoE Chip Temperatur: Zeigt an, wie warm der PoE Chip ist.
- Firmware Version: Zeigt die Firmware Version des PoE Chips an.

Portübersicht

- Aktiv: Aktivieren oder deaktivieren Sie die PoE-Versorgung für den ausgewählten Port.
- Status: Zeigt den aktuellen Status des Ports an (z.B. aktiv, inaktiv).
- Erkennung: Hier wird angezeigt, ob ein PoE-fähiges Gerät an den Port angeschlossen ist.
- Angeforderte Klasse: Gibt die vom angeschlossenen Gerät angeforderte PoE-Klasse an.
- Zugewiesene Klasse: Zeigt die tatsächlich zugewiesene PoE-Klasse an, die der Port bereitstellt.
- Strom: Gibt die aktuelle Stromaufnahme (in mA) des angeschlossenen Geräts an.
- Spannung: Zeigt die Spannung (in mV), die der Port an das angeschlossene Gerät liefert.
- Leistung: Zeigt die gesamte Leistung (in mW) an, die über den Port abgegeben wird.
- Reserviert: Gibt an, wie viel PoE-Leistung (in mW) für den jeweiligen Port reserviert ist.
- Priorität: Die PoE-Priorität ermöglicht es Ihnen, die Reihenfolge zu bestimmen, in der die PoE-Leistung für die einzelnen Ports abgeschaltet wird, sollte der ***pe-light-S-switch*** seine kritische Temperatur überschreiten (siehe Abschnitt 4.11.2).

Im derzeitigen Stand der ***pe-light-S-switch*** Steuerung sind die M12-Ports bei der Abschaltung mit folgenden voreingestellten Prioritäten versehen (siehe Tabelle 2).

Port	Priorität
Port 1	Kritisch
Port 2	Hoch
Port 3	Mittel
Port 4	Niedrig

Tabelle 2: *pe-light-S-switch* standard Port Prioritäten

4.11.1 PoE Guard

In diesem Menüpunkt (Abbildung 35) können sie das Verhalten der PoE Ports detailliert festlegen. Es kann überwacht werden, ob das angeschlossene PoE-Gerät erreichbar ist und festgelgt werden, wie sich der Port im Fehlerfall verhalten soll.

Folgende Konfigurationen können vorgenommen werden:

- Aktiv: PoE Guard kann für die einzelnen Ports aktiviert und deaktiviert werden. Ist PoE Guard aktiviert, prüft der ***pe-light-S-switch*** kontinuierlich, ob das angeschlossene Gerät erreichbar ist.
- IP Adresse: Geben Sie die IP Adresse (in Dezimalpunktschreibweise) des, an diesem Port, angeschlossenen PoE-Gerätes an.
- Start Verzögerung [Sek]: Geben Sie eine Zeit in Sekunden ein, die der ***pe-light-S-switch*** nach einem Start oder der Aktivierung von PoE auf dem jeweiligen Port warten soll, bevor er versucht das angeschlossene Gerät zu erreichen. Zulässig ist eine Zeit zwischen 0 und 19264 Sekunden.
- Max. verpasste Pings: Geben Sie an, nach wie vielen unbeantworteten Ping-Anfragen der ***pe-light-S-switch*** PoE auf dem Port ausschalten soll. Sie können eine Zahl zwischen 0 und 80 eingeben.
- Ping Intervall [Sek]: Geben Sie eine Zeit in Sekunden ein. Diese Zeit wird der ***pe-light-S-switch*** zwischen zwei Ping-Anfragen warten. Zulässig ist eine Zeit zwischen 0 und 19264 Sekunden.
- Port ausschalten für [Sek]: Geben Sie eine Zeit in Sekunden ein. Für diese Zeit wird der ***pe-light-S-switch*** den jeweiligen Port abschalten, wenn die angegebene Anzahl an Ping-Anfragen (Max. verpasste Pings) überschritten wurde. Zulässig ist eine Zeit zwischen 0 und 19264 Sekunden.

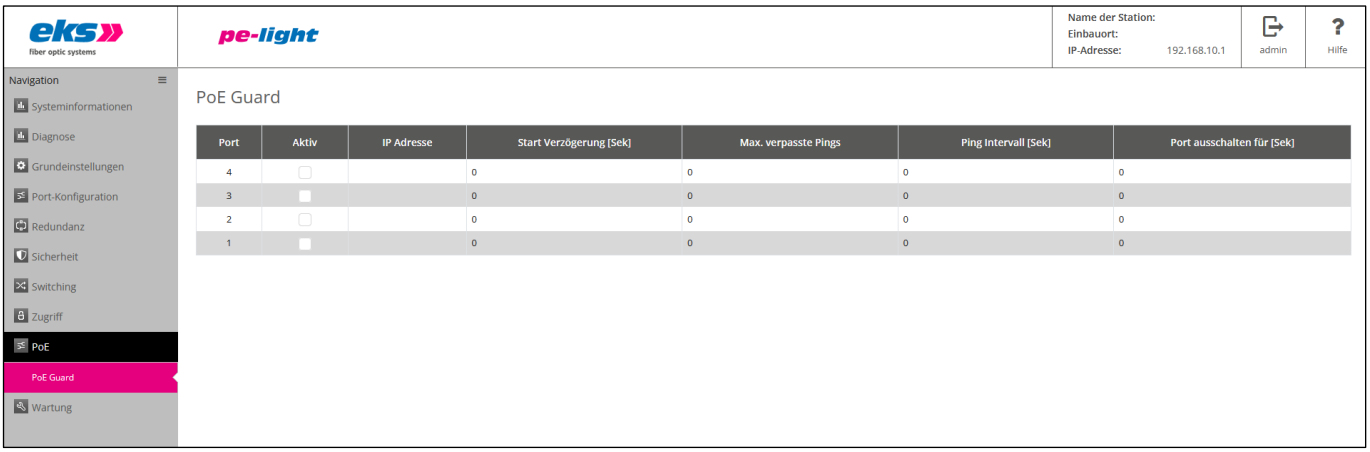


Abbildung 35: PoE Guard

4.11.2 PoE technische Spezifikationen

Der ***pe-light-S-switch*** unterstützt den PoE+ Standard bis zu einer Gesamtleistung von 120W. Pro Port werden maximal 60W bereitgestellt. Bei der Berechnung der Gesamtleistung wird die maximale Leistung der jeweiligen Geräteklassen verwendet.

Unterstützte PoE Klassen

Der ***pe-light-S-switch*** unterstützt die folgenden PoE Standards:

- ieee 802.3 af, Klasse 1 bis 3, Typ 1 (4W, 7W, 15.4W)
- ieee 802.3 at, Klasse 4, Typ 2 (30W)
- ieee 802.3 bt, Klasse 1 bis 6, Typ 3 (4W, 7W, 15.4W, 30W, 60W)

Derating

Ab einer Systemtemperatur von 70°C wird die Gesamtleistung des ***pe-light-S-switches*** in einem zeitlichen Zyklus von 5 Minuten prioritätsgesteuert heruntergefahren. Überschreitet die Temperatur 70°C, wird der Port mit der niedrigsten Priorität abgeschaltet. Sollte die Temperatur nach einer Karenzzeit von 5 Minuten nicht unter die kritische Marke fallen, wird alle 5 Minuten ein weiterer Port abgeschaltet, bis die Temperatur unter die kritische Marke fällt.

4.12 Wartung

Der Menüpunkt Wartung unterteilt sich in die Punkte Sicherung, Wiederherstellung, Firmwareupdate, Werkseinstellungen und Neustart, die im Folgenden beschrieben werden.

4.12.1 Sicherung

Dieser Menüpunkt bietet Ihnen die Möglichkeit, die aktuelle Konfiguration des ***pe-light-S-switches*** über eine http-, oder eine TFTP-Verbindung (Trivial File Transfer Protocol), in einer Datei abzulegen. In Verbindung mit der Wiederherstellung erlaubt Ihnen die Sicherungsfunktion, alle Einstellungen zu speichern und zu einem späteren Zeitpunkt wiederherzustellen bzw. die Switch-Konfiguration in weiteren Geräten zu verwenden.

Um die Konfiguration per TFTP sichern zu können, muss auf einem Rechner im Netz ein TFTP-Server eingerichtet werden. Verschiedene TFTP-Server-Programme stehen als Freeware im Internet zum Download zur Verfügung.

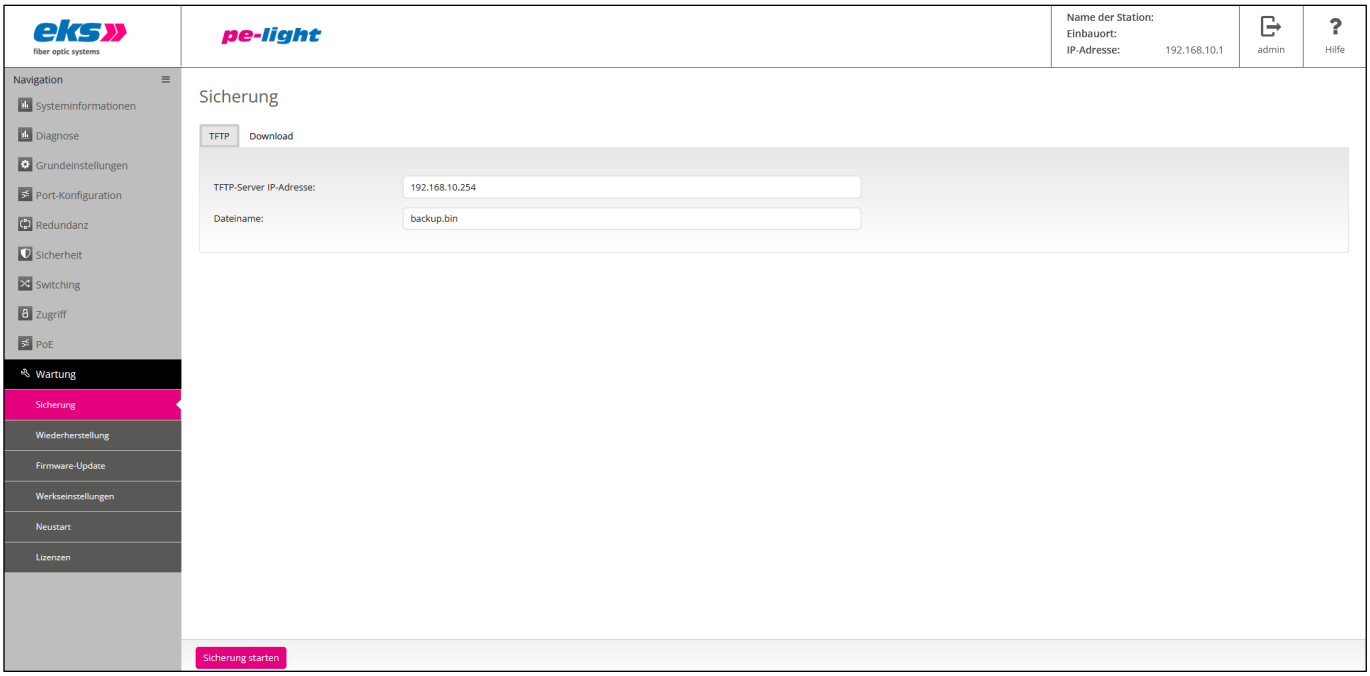


Abbildung 36: Einstellungen zur Sicherung der Konfiguration

Einstellungen TFTP

- TFTP Server IP-Adresse: IP-Adresse des im Netzwerk verfügbaren TFTP Servers in Dezimalpunktschreibweise.
- Dateiname: Dateiname unter dem die Switch-Konfigurationsdatei auf dem TFTP Server gespeichert werden soll.

Einstellungen Download

- Es können keine Einstellungen vorgenommen werden, das Backup wird im Standard-Downloadverzeichnis des Browsers unter dem Namen backup.bin gesichert.

Wenn die Parameter korrekt eingegeben wurden, kann die Sicherung durch einen Klick auf "Sicherung starten" ausgeführt werden.

4.12.2 Wiederherstellung

Dieser Menüpunkt dient dem Einspielen einer Konfiguration, die zuvor als Sicherungsdatei gespeichert wurde. Zudem können Sie diese Funktion nutzen, um die Konfiguration von einem ***pe-light-S-switch*** auf weitere ***pe-light-S-switche*** zu übertragen (indem Sie auf einem ***pe-light-S-switch*** eine Sicherung durchführen und diese dann, über diese Option, in weitere ***pe-light-S-switche*** übertragen.

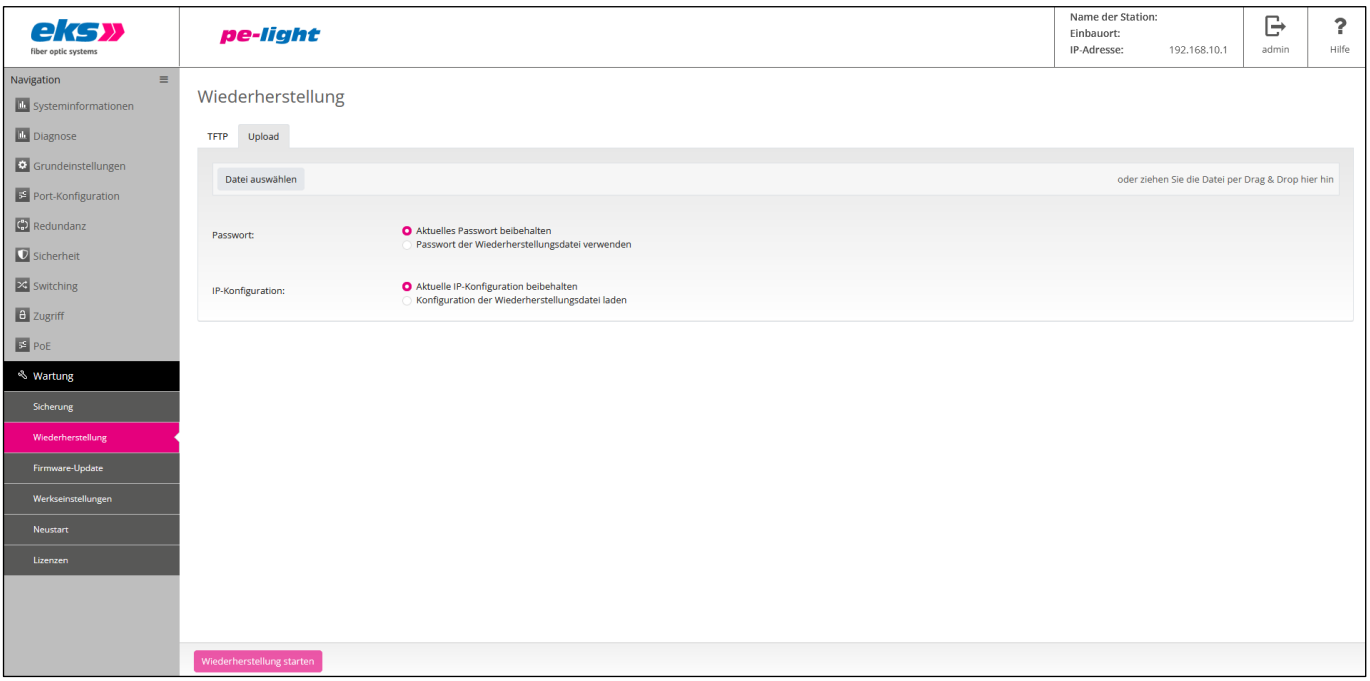


Abbildung 37: Einstellungen zur Wiederherstellung einer Konfiguration

Einstellungen

Diese Einstellungen sind gleich, egal ob die Sicherung von einem TFTP-Server aus oder über das Webinterface eingespielt werden soll.

- Passwort: Gibt an, ob die aktuellen Passwort-Einstellungen beim Widerherstellen der Konfiguration erhalten oder mit den Einstellungen aus der Konfigurationsdatei überschrieben werden sollen.
- IP-Konfiguration: Gibt an, ob die aktuell eingestellte IP-Adresse, Subnetzmaske und das Gateway erhalten oder mit den Einstellungen aus der Konfigurationsdatei überschrieben werden sollen.

Einstellungen TFTP

- TFTP-Server IP-Adresse: IP-Adresse des im Netzwerk verfügbaren TFTP-Servers in Dezimalpunkt-

schreibweise.

- Dateiname: Der Dateiname der Switch-Konfigurationsdatei, die auf dem TFTP-Server gespeichert wurde und die auf dem ***pe-light-S-switch*** eingespielt werden soll.

Einstellungen Upload

- Datei auswählen: Durch anwählen des Buttons „Datei auswählen“ kann zu der Switch-Konfigurationsdatei navigiert werden, die eingespielt werden soll. Alternativ kann die Datei per Drag and Drop auf diesen Button gezogen werden.

Durch Klick auf den Button "Wiederherstellung starten" wird die Konfigurationsdatei von der gewählten Quelle auf den ***pe-light-S-switch*** geladen. Anschließend führt der ***pe-light-S-switch*** einen Neustart durch, um die aufgespielte Konfiguration zu übernehmen.

4.12.3 Firmwareupdate

Unter dem Menüpunkt Firmwareupdate kann die Firmware des ***pe-light-S-switch*** aktualisiert werden. Bitte verwenden Sie nur Firmwareversionen, die von der Firma eks Engel FOS GmbH & Co. KG freigegeben und für Geräte der ***pe-light-S-switch*** Serie entwickelt wurden. Das Update kann per TFTP oder Upload durchgeführt werden.

Abbildung 38: Firmwareupdate

Achtung! Führen Sie diese Aktion **nicht** durch, wenn Sie nicht vorher vom Hersteller dazu autorisiert wurden. Die Funktion soll nur dann verwendet werden, wenn Probleme auftreten, die nur durch Änderung der Gerätesoftware behoben werden können. Aus diesem Grund erhalten Sie nur dann eine neue bzw. geänderte Firmware, wenn es der Hersteller für notwendig erachtet.

Einstellungen TFTP-Update

- TFTP-Server IP-Adresse: IP Adresse des im Netzwerk verfügbaren TFTP-Servers in Dezimalpunktschreibweise.

Einstellungen TFTP oder Upload-Update

- Dateinamen: Dateiname der neuen Firmwaredatei.

Durch Klick auf den Button "Firmwareupdate starten" wird das Update gestartet.

Achtung: Bitte beachten Sie während dem Firmwareupdate folgende Regeln:

- Trennen Sie das Gerät auf keinen Fall von der Versorgungsspannung.
- Ziehen Sie keine Netzwerkstecker raus oder stecken diese um.

Während des Updates erscheint im Web-Interface eine Fortschrittsanzeige. Sobald das Update abgeschlossen ist, startet der ***pe-light-S-switch*** neu.

4.12.4 Werkseinstellungen

Dieser Menüpunkt dient dem Zurücksetzen des Gerätes auf seine Werkseinstellungen.

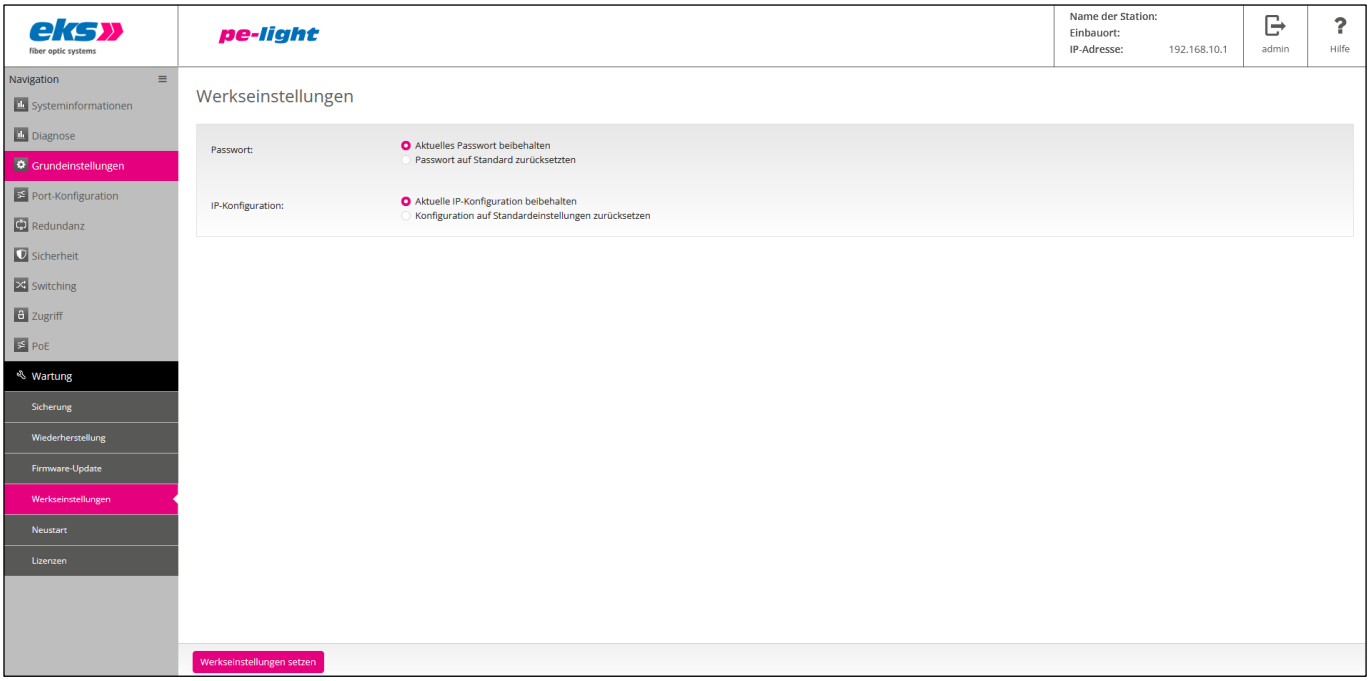


Abbildung 39: Werkseinstellungen

Einstellungen:

- Passwort: Gibt an, ob die aktuellen Passwort-Einstellungen beim Zurücksetzen der Konfiguration erhalten oder mit den Werkseinstellungen überschrieben werden sollen.
- IP-Konfiguration: Gibt an, ob die aktuelle IP-Adresse, Subnetzmaske und das Gateway erhalten oder mit den Werkseinstellungen überschrieben werden sollen.

Durch Klick auf den Button "Werkseinstellungen setzen" wird der ***pe-light-S-switch*** zurückgesetzt.
Sind die Werkseinstellungen erfolgreich übernommen worden, führt der ***pe-light-S-switch*** einen Neustart durch.

4.12.5 Werksreset über den Türkontakt

Es besteht die Möglichkeit den ***pe-light-S-switch*** über den Türkontakt wieder auf die Werkseinstellungen zurückzusetzen. Um den Werksreset auszuführen müssen Sie die den Türkontakt öffen, dann beginnt die LED für den Türkontakt für 10 Sekunden zu blinken. Innerhalb dieses Zeitfensters muss der Türkontakt eine bestimmte „Reset-Sequenz“ durchlaufen: geschlossen – geöffnet – geschlossen – geöffnet – geschlossen - geöffnet. Geschieht dies innerhalb des Zeitfensters, so geht die LED für den Türkontakt aus

und das Gerät führt einen Werksrest mit anschließendem Neustart aus.

Wird die „Reset-Sequenz“ nicht ausgeführt, so hört die Türkontakt LED nach 10 Sekunden auf zu blinken und zeigt von da an den Status des Türkontaktes an.

Es ist jeder Zeit möglich das Zeitfenster für den Werksreset neu zu starten, indem der Türkontakt geschlossen und wieder geöffnet wird.

4.12.6 **Neustart**

Hier kann der Neustart des Switches bzw. ein Software Reset durchgeführt werden. Durch Drücken des Neustart Buttons wird die Software des Switches beendet und das Gerät bootet neu.

Alternativ können Sie die Versorgungsspannung des Switches aus- und wieder einschalten und so einen Hardware-Reset durchführen.

4.12.7 **Lizenzen**

Herstellerinformationen

Wenn Sie schwerwiegende Probleme bei der Konfiguration des Geräts oder Fragen zum Gerät haben kontaktieren Sie eks Engel FOS GmbH & Co. KG. Bitte lesen Sie die Online Hilfe des Geräts und die Anleitung bevor Sie sich mit dem Support in Verbindung setzen.

Bedienungsanleitung

Sie können die aktuelle Bedienungsanleitung als PDF-Dokument direkt vom Gerät herunterladen. Einen geeigneten PDF-Reader finden Sie kostenlos im Internet.

SNMP-MIB File

Die SNMP-MIB (**S**imple **N**etwork **M**anagement **P**rotocol - **M**anagement **I**nformation **B**ase)–Datei steht zum Download auf dem Gerät zur Verfügung, Sie liefert alle Gerätespezifischen Informationen die mit einem SNMP Browser vom Gerät ausgelesen werden können.

Lizenzinformationen

Das Gerät enthält Open Source Software. In der Datei license.txt finden Sie Informationen zu allen zu beachtenden Lizenzen.

5 Hinweise zur Fehlerbehebung

- Überprüfen Sie die korrekte Spannungsversorgung. Die VDC-LED muss grün leuchten.
- Überprüfen Sie die Link/Act-LEDs der verkabelten M12-Buchsen und Lichtwellenleiter-Transceiver. Bei aufgebauter Verbindung müssen die Link-LEDs leuchten bzw. bei Übertragung von Daten müssen sie blinken.
- Überprüfen Sie die Verkabelung der M12-Buchsen. Wählen Sie das richtige Netzwerkkabel. Benutzen Sie „unshielded twisted pair“ (UTP) oder „shielded twisted pair“ (STP) für M12 Verbindungen, um das Netzwerk aufzubauen: 100Ω Kategorie 3, 4, 5 oder bessere Kabel für Verbindungen mit 10 MBit/s oder 100Ω Kategorie 5 oder bessere Kabel für Verbindungen mit 100 MBit/s oder 1000 MBit/s. Versichern Sie sich, dass die Kabel nicht länger als 100 Meter sind.
- Trennen Sie im Zweifelsfall redundante Netzwerkstrukturen auf und Setzen Sie den ***pe-light-S-switch*** auf Werkseinstellungen. Wenn die Kommunikation dann funktioniert, nehmen Sie Ihre Einstellungen nach und nach vor und beobachten Sie, bei welchen Einstellungen der Fehler auftritt.

6 Technische Spezifikation

LED Anzeige	Status-LEDs / Port LEDs (gelb/grün) / Spannungsversorgung (grün)
IEEE	IEEE 802.3 10Base-T Ethernet / IEEE 802.3u 100Base-TX und 1000Base-FX Fast Ethernet / IEEE802.1d spanning tree / IEEE802.1w rapid spanning tree / IEEE802.1p class of service / IEEE802.1Q VLAN Tag
Protokoll	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 EtherLike-MIB / RFC 1215 Trap MIB Private MIB für Switch Informationen, Ring, Portalarm, TFTP Firmware Update, Reset, Port Mirror, IP Security Management, IGMP Management MIB
Technologie	Store und Forward Switching Architektur, Profinet Class B, Netload Class III
SNMP Trap	Trap-Receiver / Kaltstart / Port link Up / Port link Down / Authentifikations-fehler / Private Trap für Power Status / Portalarm Konfiguration / Fehler-alarm Ring
Transfer Rate	14,880 pps für 10Base-T Ethernet Port 148,800 pps für 100Base-TX Fast Ethernet Port 148,800,000 pps für 1000Base-TX/FX Gigabit Ethernet Port
MAC Adresstabelle	2K MAC Adresstabelle
Paketfilter	4 Typen von Paketfilterregeln mit verschiedenen Paketkombinationen
Ring	2 Ports für den Ring, um eine Erholzeit unter 200ms zu garantieren
VLAN	Port based VLAN Tagged VLAN IEEE 802.1Q
Class of Service	IEEE802.1p Class of Service mit 4 Prioritätswarteschlangen per Port
Spanning Tree	IEEE802.1d Spanning Tree und IEEE802.1w Rapid Spanning Tree
IGMP	IGMP v1 und Query Modus, mit bis zu 256 Gruppen
SNTP	SNTP zur Zeitsynchronisation
SMTP	SMTP Server und E-Mail-Konten für Ereignismeldungen
Port Mirror	Nur TX Pakete oder TX und RX Pakete
Firmware Update	Firmwareupdate, Sicherung und Wiederherstellung via TFTP, HTTP
Bandbreitenkontr.	Ingress und Egress mit Kombinationsmöglichkeiten
DHCP Client	DHCP Client-Funktion, um eine IP-Adresse vom DHCP Server zu erhalten

Tabelle 3: Funktionen, Standards und Technologien der *pe-light-S-switche*

7 GPL/LGPL Garantie und Haftungsausschluss

Die ***pe-light-S-switches*** der eks Engel FOS GmbH & Co. KG (im folgenden eks) enthalten neben proprietärer Software auch Bestandteile an „Open Source Software“. Die Open Source Software wird Ihnen unter den Bedingungen der GNU General Public License (GPL) und der GNU Lesser General Public License (LGPL) ohne Lizenzgebühren zur Verfügung gestellt. Sie wurde von Dritten geschrieben und unterliegt dem Urheberrechtsschutz.
Sie sind berechtigt, die Open Source Software unter den Bedingungen der GPL oder LGPL zu nutzen. Im Fall eines Konflikts zwischen eks Lizenzbedingungen und den Bedingungen der GPL oder LGPL gilt für die Open Source Anteile der Software die GPL und LGPL.

Die GPL und die LGPL Lizenzen sowie weitere Lizenzinformationen sind unter folgender URL auf dem Gerät verfügbar (IP-Adresse im Auslieferungszustand): http://<device-ip>/download/license.txt

In dem Fall, dass die Quellcodes der Open Source Software nicht mit dem ***pe-light-S-switch*** ausgeliefert wurden, können sie (zusammen mit den zugehörigen Urheberrechtshinweisen) unter der folgenden E-mail-Adresse angefordert werden: info@eks-engel.de. Die Quellcodes werden Ihnen dann gegen Erstattung der Kopier- und Versandkosten zugesandt.

Alle Quellcode-Anfragen müssen innerhalb von drei Jahren nach Kauf des ***pe-light-S-switch*** eingehen. Bitte fügen Sie Ihrer Anforderung eine Kopie des Kaufbelegs bei. Ergänzen Sie bitte außerdem den exakten Namen des Geräts und die Versionsnummer der installierten Software.

Die Nutzung der mit dem ***pe-light-S-switch*** ausgelieferten Open Source Software in irgendeiner anderen Weise als der Verwendung mit der ***pe-light-S-switch*** -Hardware erfolgt auf eigenes Risiko, ohne jedwede Haftungsansprüche gegen eks.

Für weitere Informationen zu Garantieansprüchen an die Autoren der mit dem ***pe-light-S-switch*** ausgelieferten Open Source Software verweisen wir auf die GPL und die LGPL.

Wir schließen jede Haftung für Schäden aus, die durch von anderen als eks durchgeführte Änderungen an Teilen

der Software oder ihrer Konfiguration entstanden sind. Außerdem schließen wir jede Haftung durch eks aus, wenn die Open Source Software gegen Urheberrechte Dritter verstößt.

Für nicht durch eks vorgenommene Änderungen der Software übernehmen wir keinen technischen Support.

8 Abbildungsverzeichnis

Abbildung 1: Frontansicht des *pe-light-S-switches* 9
Abbildung 2: *pe-light-S* in einem sternförmigen Netzwerk 12
Abbildung 3: *pe-light-S* in einem vermaschten Netzwerk 13
Abbildung 4: *pe-light-S* in einem ringförmigen Netzwerk 14
Abbildung 5: Login-Maske 16
Abbildung 6: Status und Diagnose 17
Abbildung 7: Übersicht der Alarmtrigger 19
Abbildung 8: Alarme / Meldungen: Hinzufügen eines Alarmauslösers 20
Abbildung 9: Hinzufügen eines Alarmempfängers 21
Abbildung 10: Port Statistiken 22
Abbildung 11: Syslog Meldungen 23
Abbildung 12: Link Layer Discovery Protokoll (LLDP) 25
Abbildung 13: Grundeinstellungen des *pe-light-S-switches* 26
Abbildung 14: Änderung der IP-Konfiguration 28
Abbildung 15: Änderung des Passwortes für Administrator- und Gastzugriff 28
Abbildung 16: Konfiguration der Zeiteinstellung (SNTP) 30
Abbildung 17: Konfiguration der Zeiteinstellungen (manuell) 31
Abbildung 18: Übersicht der Tabelle Port-Konfiguration 33
Abbildung 19: Port Mirroring 33
Abbildung 20: Media Redundancy Protokoll (MRP) 35
Abbildung 21: Rapid Spanning Tree Protocol – Geräte Einstellungen 36
Abbildung 22: Rapid Spanning Tree Protocol – Port-Einstellungen 38
Abbildung 23: Radius/802.1x ..... **Fehler! Textmarke nicht definiert.**
Abbildung 25: Seite Switching 40
Abbildung 26: IGMP Snooping 41
Abbildung 27: VLAN 802.1Q 42
Abbildung 28: VLAN anlegen / editieren 43
Abbildung 29: VLAN - Portübersicht 44
Abbildung 30: VLAN - Zuordnung Management VLAN 44

Abbildung 31: Quality of Service 46
Abbildung 32: Einstellung der Bandbreitenkontrolle 47
Abbildung 33: Forwarding Database 48
Abbildung 34: Auswahl der verschiedenen Zugriffsmöglichkeiten 49
Abbildung 35: Übersicht der aktuell vorhandenen SNMP Zugänge 51
Abbildung 36: PoE 53
Abbildung 37: PoE Guard 56
Abbildung 38: Einstellungen zur Sicherung der Konfiguration 57
Abbildung 39: Einstellungen zur Wiederherstellung einer Konfiguration 58
Abbildung 40: Firmwareupdate 59
Abbildung 41: Werkseinstellungen 61

9 Tabellenverzeichnis

Tabelle 1: LED Beschreibung 10

Tabelle 2: *pe-light-S-switch* standard Port Prioritäten.....55

Tabelle 3: Funktionen, Standards und Technologien der *pe-light-S-switche* 64