. . . c o n n e c t i n g y o u r b u s i n e s s

LANCOM ES-2126+
LANCOM ES-2126P

LANCOM
Systems

LANCOM ES-2126+
LANCOM ES-2126P

LANCOM
Systems

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom.de

Würselen, Oktober 2009

110533/1009

DE

Ein Wort vorab

Vielen Dank für Ihr Vertrauen!

Die LANCOM Switch von Typ LANCOM ES-2126+ und LANCOM ES-2126P sind optimal geeignet für kleine und mittelgroße, aber anspruchsvolle Netzwerke im Business-Umfeld.

Der LANCOM ES-2126+ mit seinen 24 Fast-Ethernet und seinen zwei Combo Ports (TP/SFP) lässt sich perfekt in LANCOMs Advanced Routing und Forwarding integrieren und unterstützt bis zu 256 aktive VLANs. Er führt eine Bandbreitenkontrolle durch und priorisiert nach vorher festgelegten Kriterien den Datenverkehr (z. B. Voice-Daten oder den bestimmter Ports).

Der LANCOM ES-2126P bietet über die Funktionen des LANCOM ES-2126+ hinaus eine komfortable PoE-Versorgung der angeschlossenen Netzwerkgeräte. Die bis zu einer Gesamtleistung von 185 Watt zur Verfügung stehende PoE-Leistung kann flexibel auf die 24 Fast-Ethernet-Ports aufgeteilt werden.

Die LANCOM Switche lassen sich bequem über die übersichtliche WEBconfig administrieren und werden von den LANCOM Management Tools (LANconfig und LANmonitor) unterstützt.

Modellvarianten

Diese Dokumentation wendet sich an Anwender der LANCOM Switche. Folgende Modelle stehen zur Auswahl:

- Der LANCOM ES-2126+ ohne PoE-Unterstützung
- Der LANCOM ES-2126P mit PoE-Unterstützung

Modell-Einschränkungen

Die Teile der Dokumentation, die nur für ein bestimmtes Modell gelten, sind entweder im Text selbst oder durch entsprechende seitliche Hinweise gekennzeichnet.

In den anderen Teilen der Dokumentation werden alle beschriebenen Modelle unter dem Sammelbegriff LANCOM Switch zusammengefasst.

An der Erstellung dieser Dokumentation …

… haben mehrere Mitarbeiter/innen aus verschiedenen Teilen des Unternehmens mitgewirkt, um Ihnen die bestmögliche Unterstützung bei der Nutzung Ihres LANCOM-Produktes anzubieten.

DE

Sollten Sie einen Fehler finden oder einfach nur Kritik oder Anregung zu dieser Dokumentation äußern wollen, senden Sie bitte eine E-Mail direkt an: info@lancom.de

Sollten Sie zu den in diesem Handbuch besprochenen Themen noch Fragen haben oder zusätzliche Hilfe benötigen, steht Ihnen unser Internet-Server www.lancom.de rund um die Uhr zur Verfügung. Hier finden Sie im Bereich 'Support' viele Antworten auf „häufig gestellte Fragen ('FAQs')". Darüber hinaus bietet Ihnen die Wissensdatenbank einen großen Pool an Informationen. Aktuelle Treiber, Firmware, Tools und Dokumentation stehen für Sie jederzeit zum Download bereit.
Außerdem steht Ihnen der LANCOM-Support zur Verfügung. Telefonnummern und Kontaktadressen des LANCOM-Supports finden Sie in einem separaten Beileger oder auf der LANCOM Systems-Homepage.

Hinweis-Symbole	
	Sehr wichtiger Hinweis, dessen Nichtbeachtung zu Schäden führen kann.
	Wichtiger Hinweis, der beachtet werden sollte.
	Zusätzliche Informationen, deren Beachtung hilfreich sein kann aber nicht erforderlich ist.

Inhalt

DE

DE

1 Einleitung

Bei den LANCOM Switches von Typ LANCOM ES-2126+ und LANCOM ES-2126P handelt es sich um gemanagte Layer-2-Switches mit 24 Fast-Ethernet-Ports (für Twisted-Pair-Kabel – TP) sowie zwei Gigabit-Ports (Dual-Media für TP- oder Glasfaserkabel), die den IEEE 802.3-Spezifikationen für Gigabit, Fast Ethernet und Ethernet entsprechen.

Die LANCOM Switche können mit einer direkten Verbindung über den seriellen Port (RS-232) oder über eine LAN-Verbindung mit Telnet oder WEBconfig konfiguriert werden. Als zusätzliche Konfigurationswege stehen für Modelle vom Typ LANCOM ES-2126+ SHH (Secure Shell) oder WEBconfig mit optionaler SSL-Verschlüsselung zur Verfügung. Ein SNMP-Management nach SNMPv2 ist durch die integrierten MIBs ebenfalls möglich.

Mit einem effizienten Netzwerk-Management ermöglichen die LANCOM Switche Anwendungen mit hohem Bandbreitebedarf. Die Geräte unterstützen moderne Funktionen wie QoS (Quality of Service), Rapid Spanning Tree, VLAN, Port Trunking, Bandbreitenbeschränkung, portbasierte Sicherheitseinstellungen, SNMP/RMON und IGMP Snooping. Sie sind damit optimal geeignet für kleine und mittelgroße, aber anspruchsvolle Netzwerke im Business-Umfeld.

Der LANCOM ES-2126+ unterstützt darüberhinaus TACACS+, ein Protokoll für Authentifizierung, Authorisierung und Accounting (AAA), es stellt also den Zugang zu Netzwerkkomponenten nur für bestimmte Nutzer sicher, regelt die Berechtigungen der Benutzer und überträgt Daten für die Protokollierung der Netzwerknutzung.

Der LANCOM ES-2126P entspricht außerdem dem PoE-Standard IEEE 802.3af, über den der Switch angeschlossene PoE-Geräte automatisch erkennt und wichtige Parameter wie die Klassifizierung und Strom-Limits einstellt.

Die 10/100/1000MBit/s-TP-Ports entsprechen den Standards IEEE 802.3/u/x/z (Gigabit und Fast Ethernet).

Die 1000MBit/s-SFP-Ports entsprechen den Standards IEEE 802.3z und 1000Base-SX/LX. Der Glasfaser-Port ist mit der Wavelength Division Multiplexing (WDM) Technologie ausgerüstet, welche die gleichzeitige Full-Duplex-Übertragung in beide Richtungen über eine Faser erlaubt.

DE

1.1 Funktionsübersicht

- QoS:

  Unterstützt Quality of Service nach dem IEEE 802.1P-Standard. Dabei werden zwei prioritätsgesteuerte Warteschlangen nach einem gewichteten Round Robin-Verfahren verwendet (Weighted Round Robin – WRR). Die Klassifizierung der Pakete kann über VLAN-Tags oder portgebunden eingerichtet werden.

- Spanning Tree:

  Unterstützt die Standards IEEE 802.1D und IEEE 802.1w (RSTP: Rapid Spanning Tree Protocol) .

- VLAN:

  Unterstützt portbasiertes VLAN und VLAN-Tagging nach IEEE802.1Q mit bis zu 256 aktiven VLANs und VLAN-IDs von 1 bis 4094.

- Port Trunking:

  Unterstützt statisches Port-Trunking und dynamisches Port-Trunking nach IEEE 802.3ad LACP.

- Bandbreitenbeschränkung:

  Unterstützt die Bandbreitenbeschränkung für eingehende und ausgehende Verbindungen.

- Portbasierte Sicherheitseinstellungen:

  Unterstützt das Erlauben oder Verbieten der Datenverarbeitung auf einem Port in Abhängigkeit von der MAC-Adresse.

- SNMP/RMON:

  SNMP-Agent und RMON MIB. Das Gerät arbeitet als SNMP-Client und übermittelt auf Anfrage des SNMP-Managers Informationen über den aktuellen Zustand. Ausserdem versendet der SNMP-Agent bei Bedarf aktiv TRAP-Nachrichten.

  RMON steht als Abkürzung für Remote Network Monitoring und ist ein zweig der SNMP MIB.

  Das Gerät unterstützt MIB-2 (RFC 1213), Bridge MIB (RFC 1493), RMON MIB (RFC 1757)-Statistiken der Gruppen 1,2,3,9, Bridge MIB (RFC 1493), Ethernet MIB (RFC 1643) usw.

Nur für LANCOM ES-2126+

- TACACS+

  Das TACACS+ (Terminal Access Control Access Control Server) ist ein Protokoll für Authentifizierung, Authorisierung und Accounting (AAA), es

stellt also den Zugang zu Netzwerkkomponenten nur für bestimmte Nutzer sicher, regelt die Berechtigungen der Benutzer und überträgt Daten für die Protokollierung der Netzwerknutzung.

- IGMP Snooping:

  Unterstützt IGMP-Version 2 (RFC 2236). Das Internet Group Management Protocol dient zum Aufbau von Multicast-Gruppen, in denen die Multicast-Pakete ausschließlich an die jeweiligen Gruppenmitglieder übermittelt werden. Mit Hilfe von IGMP wird die benötigte Bandbreite durch unnötige Daten reduziert.

DE

1.2 Das kann Ihr LANCOM Switch

	LANCOM ES-2126+	LANCOM ES-2126P
Hardware		
24 10/100MBit/s Gigabit TP-Ports mit Auto-MDIX-Funktion	✔	✔
2 Gigabit Dual Media Ports (TP/SFP)	✔	✔
Hot-Plugging für SFP-Module	✔	✔
256KB Paket-Zwischenspeicher und 128KB Verwaltungsspeicher	✔	✔
Maximale Paketlänge von 1536 Bytes	✔	✔
Full-Duplex Datenflusssteuerung (IEEE802.3x)	✔	✔
LEDs zur Zustandsanzeige		
System: Power, CPURUN, ACT / FDX / SPD(LEDSET)	✔	✔
TP Port 1-24: LINK/ACT, FDX, SPD	✔	✔
SFP-Ports 25,26: LINK/ACT, FDX, SPD	✔	✔
PoE-Versorgung		
PoE-Versorgung an Port 1 bis 24 nach IEEE802.3af mit 48VDC über RJ-45 Pin 1, 2, 3, 6.		✔
Automatische Erkennung und Klassifizierung der angeschlossenen PoE-Geräte		✔
LEDs zur Anzeige des PoE-Zustands der einzelnen Ports		✔
Management		
Klare Darstellungg der Port-Zustände und einfache Konfguration der Ports	✔	✔
Port-spezifische Traffic-Überwachung	✔	✔
Port-Mirror-Funktion	✔	✔
Unterstützung statischer Trunk-Gruppen	✔	✔
VLAN nach 802.1Q mit 256 Einträgen	✔	✔
Unterdrückung der DHCP-Broadcasts zur Entlastung des Netzwerks	✔	✔
Versand von Trap-Nachrichten, wenn definierte Ereignisse stattfinden	✔	✔
Default-Konfiguration, mit der die aktuelle Konfiguration über Telnet oder WEBconfig überschrieben werden kann	✔	✔

DE

	LANCOM ES-2126+	LANCOM ES-2126P
Fünf Typen von QoS: MAC-Priorität, 802.1p-Priorität, IP TOS-Priorität, und DiffServ DSCP-Priorität.	✔	✔
WEBconfig und CLI-Management über Telnet	✔	✔
WEBconfig mit SSL-Verschlüsselung, CLI-Management über SHH	✔	
Rapid Spanning Tree (802.1w RSTP)	✔	✔
Portbasierte Sicherheitseinstellungen im VLAN nach 802.1x	✔	✔
SNMP-Zugang abschaltbar zum Schutz vor unberechtigten SNMP-Zugriffen	✔	✔
Bandbreitenregelung für ein- und ausgehende Verbindungen	✔	✔
Versand von Trap-Nachrichten über E-Mail und SMS	✔	✔
Diagnose-Funktionen zur Unterstützung des Administrators	✔	✔
Externer Loopback-Test zur Prüfung der Port-Funktion	✔	✔
TFTP für Firmware-Upgrades, System-Logs sowie den Import bzw. Export von Konfigurationen	✔	✔
Remote Boot über WEBconfig, CLI und SNMP	✔	✔
Zeitsynchronisation mit NTP-Servern und Sommerzeitumschaltung	✔	✔
TACACS+ für Authentifizierung, Authorisierung und Accounting (AAA)	✔	
120 Einträge in der Log-Tabelle im Hauptspeicher zur Anzeige über Konsole	✔	✔
Optionen		
LANCOM SFP Glasfaser Transceiver: Art.-Nr. 61556 LANCOM SFP-SX-LC1 Art.-Nr. 61557 LANCOM SFP-LX-LC1	✔	✔

2 Installation

Dieses Kapitel hilft Ihnen, möglichst schnell Hard- und Software zu installieren. Zunächst überprüfen Sie Lieferumfang und Systemvoraussetzungen. Sind alle Voraussetzungen erfüllt, gelingen Anschluss und Inbetriebnahme schnell und ohne Mühe.

2.1 Lieferumfang

Bitte prüfen Sie den Inhalt der Verpackung auf Vollständigkeit, bevor Sie mit der Installation beginnen. Neben dem LANCOM Switch sollte der Karton folgendes Zubehör für Sie bereithalten:

	LANCOM ES-2126+	LANCOM ES-2126P
Netzkabel zum Anschluss an die Stromversorgung	✔	✔
19''-Adapter (2 Stück) und Befestigungsmaterial	✔	✔
Serielles Konfigurationskabel	✔	✔
LANCOM-CD	✔	✔
Gedruckte Dokumentation	✔	✔

Falls etwas fehlen sollte, wenden Sie sich bitte umgehend an Ihren Händler oder an die Kontaktadresse, die auf dem Lieferschein zu Ihrem Gerät angegeben ist.

2.2 Systemvoraussetzungen

Rechner, die mit einem LANCOM in Verbindung treten möchten, müssen mindestens die folgenden Voraussetzungen erfüllen:

- Betriebssystem mit TCP/IP-Unterstützung, z. B. Windows, Linux, BSD Unix, Apple Mac OS, OS/2.
- Zugang zum LAN über das TCP/IP-Protokoll.
- Browser für die webbasierte Konfiguration.

Die LANtools benötigen zudem ein Windows-Betriebssystem. Für den Zugriff auf WEBconfig ist ein Web-Browser unter einem beliebigen Betriebssystem erforderlich.

DE

2.3 Statusanzeigen und Schnittstellen

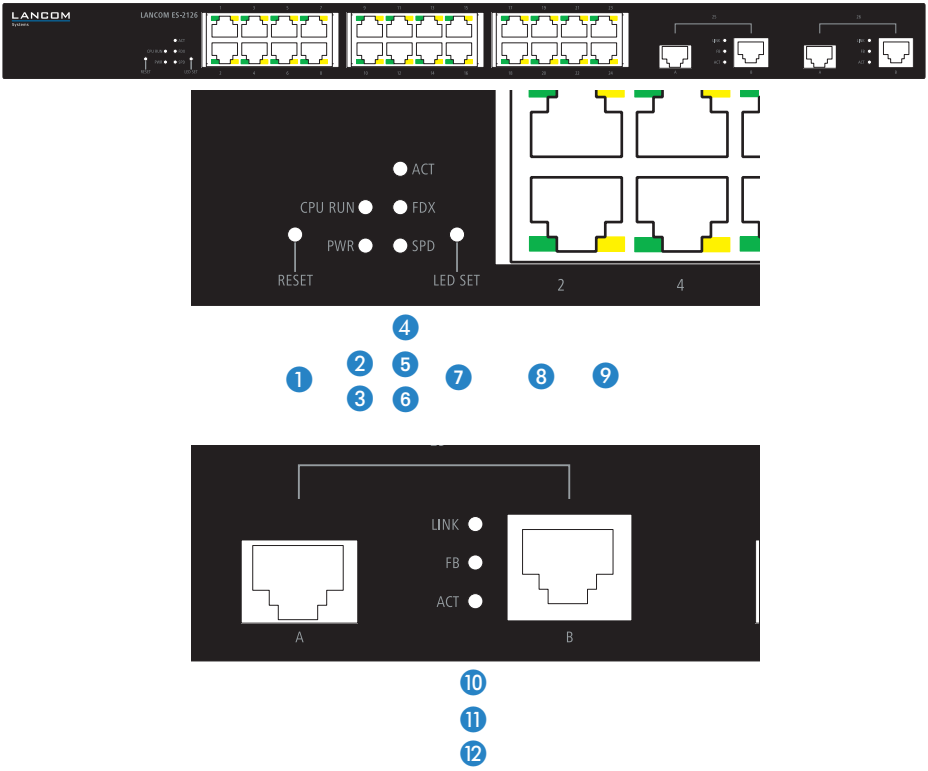
Bedeutung der LEDs

In den folgenden Abschnitten wird das Verhalten der LEDs beschrieben.

Bitte beachten Sie, dass der LANmonitor über die Anzeige der LEDs hinaus weitere wichtige Informationen über den Status der LANCOM Switche anzeigt '→ LANCOM Switch mit LANmonitor überwachen'.

2.3.1 LEDs und Taster beim LANCOM ES-2126+

Auf der Vorderseite des Geräts befinden sich Leuchtdioden (LEDs), die Informationen über den Status des Geräts geben, sowie zwei Taster.



1 Reset — Taster zum Neustarten des Systems.

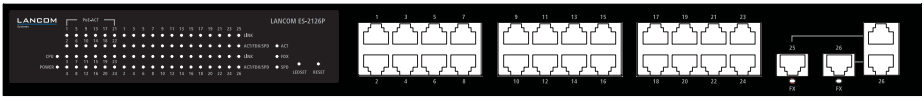
2 CPU RUN — Blinkt grün, wenn die CPU fehlerfrei läuft.

DE

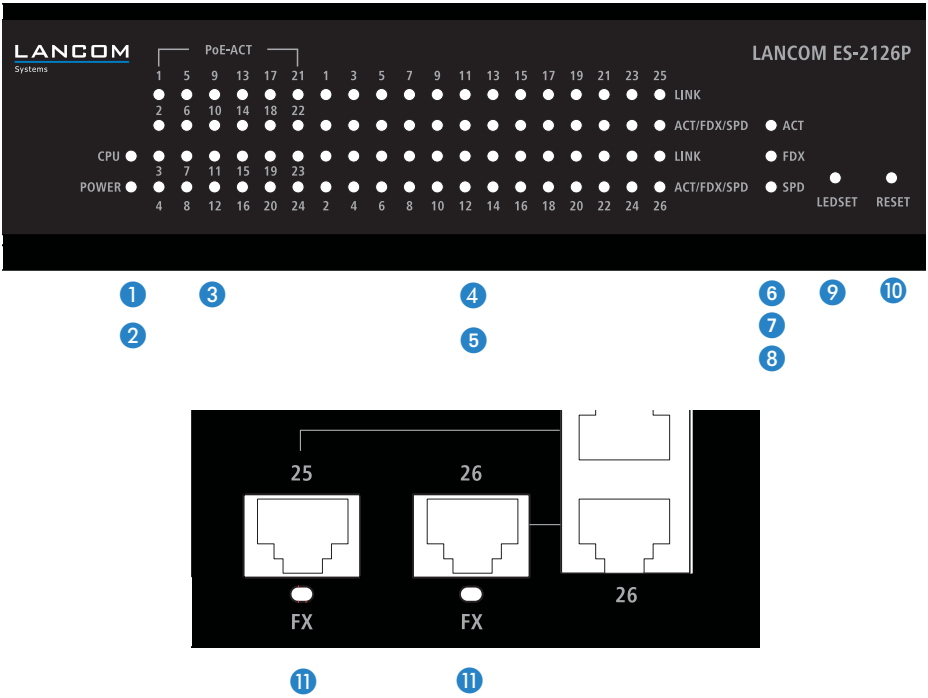
3 PWR	Power-LED, dauerhaft grün, wenn die Spannungsversorgung des Gerätes hergestellt ist.
4 ACT	Dauerhaft grün, wenn der LED-Modus auf "Active" eingestellt ist.
5 FDX	Dauerhaft grün, wenn der LED-Modus auf "Full-Duplex" eingestellt ist.
6 SPD	Dauerhaft grün, wenn der LED-Modus auf "Speed" eingestellt ist.
7 LEDSET	Taster zum Umschalten des LED-Modus zwischen "Active", "Full-Duplex" und "Speed".
8 LINK Port 1 bis 24	Dauerhaft grün, wenn die Netzwerkverbindung zum angeschlossenen Gerät hergestellt ist. Aus, wenn keine Netzwerkverbindung zum angeschlossenen Gerät hergestellt werden kann.
9 ACT/FDX/SPD Port 1 bis 24	Diese LED zeigt je nach gewähltem LED-Zustand folgende Informationen: ■ LED-Modus "Active": Blinkt gelb bei Datenübertragung. ■ LED-Modus "Full-Duplex": Dauerhaft gelb, wenn Full-Duplex-Modus für diesen Port aktiv ist, blinkt gelb bei Kollisionen. ■ LED-Modus "Speed": Dauerhaft gelb, wenn 100 MBit/s-Modus aktiv ist. Aus, wenn 10 MBit/s-Modus aktiv ist.
10 Link Port 25 und 26	Dauerhaft grün, wenn die Netzwerkverbindung zum angeschlossenen Gerät hergestellt ist. Aus, wenn keine Netzwerkverbindung zum angeschlossenen Gerät hergestellt werden kann.
11 FB Port 25 und 26	Dauerhaft grün, wenn Glasfaser-Port aktiv ist. Aus, wenn der TP-Port aktiv ist
12 ACT Port 25 und 26	Diese LED zeigt je nach gewähltem LED-Zustand folgende Informationen: ■ LED-Modus "Active": Blinkt gelb bei Datenübertragung. ■ LED-Modus "Full-Duplex": Dauerhaft gelb, wenn Full-Duplex-Modus für diesen Port aktiv ist, blinkt gelb bei Kollisionen. ■ LED-Modus "Speed": Dauerhaft grün, wenn GBit/s-Modus aktiv ist. Aus, wenn 10 MBit/s- oder 100 MBit/s-Modus aktiv ist.

2.3.2 LEDs und Taster beim LANCOM ES-2126P

Auf der Vorderseite des Geräts befinden sich Leuchtdioden (LEDs), die Informationen über den Status des Geräts geben, sowie zwei Taster.



DE

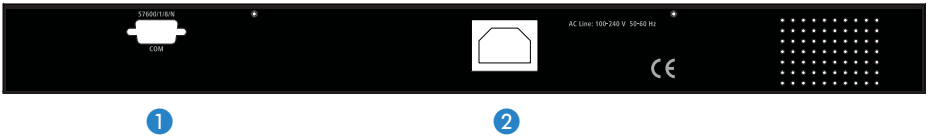


1	CPU RUN	Blinkt grün, wenn die CPU fehlerfrei läuft.
2	PWR	Power-LED, dauerhaft grün, wenn die Spannungsversorgung des Gerätes hergestellt ist.
3	PoE-ACT	Dauerhaft grün, wenn über diesen das angeschlossene Gerät via PoE mit Strom versorgt wird.
4	LINK Port 1 bis 24	Dauerhaft grün, wenn die Netzwerkverbindung zum angeschlossenen Gerät hergestellt ist. Aus, wenn keine Netzwerkverbindung zum angeschlossenen Gerät hergestellt werden kann.
5	ACT/FDX/SPD Port 1 bis 24	Diese LED zeigt je nach gewähltem LED-Zustand folgende Informationen: ■ LED-Modus "Active": Blinkt gelb bei Datenübertragung. ■ LED-Modus "Full-Duplex": Dauerhaft gelb, wenn Full-Duplex-Modus für diesen Port aktiv ist, blinkt gelb bei Kollisionen. ■ LED-Modus "Speed": Dauerhaft gelb, wenn 100 MBit/s-Modus aktiv ist. Aus, wenn 10 MBit/s-Modus aktiv ist.
6	ACT	Dauerhaft grün, wenn der LED-Modus auf "Active" eingestellt ist.

7	FDX	Dauerhaft grün, wenn der LED-Modus auf "Full-Duplex" eingestellt ist.
8	SPD	Dauerhaft grün, wenn der LED-Modus auf "Speed" eingestellt ist.
9	LEDSET	Taster zum Umschalten des LED-Modus zwischen "Active", "Full-Duplex" und "Speed".
10	Reset	Taster zum Neustarten des Systems.
11	FX Port 25 und 26	Dauerhaft grün, wenn Glasfaser-Port aktiv ist. Aus, wenn der TP-Port aktiv ist.

2.3.3 Anschlüsse beim LANCOM ES-2126+ und LANCOM ES-2126P

Auf der Rückseite des Geräts befinden sich folgende Anschlüsse.



1. Anschluss für serielles Konfigurationskabel zur direkten Konfiguration.
2. Anschluss für Kaltgerätekabel zur Stromversorgung.

2.4 Montage und Anschluss des LANCOM Switches

Die Installation des LANCOM Switches erfolgt in folgenden Schritten:

① **Montage** – montieren Sie das Gerät in einem freien 19"-Einschub in einem entsprechenden Serverschrank. Nutzen Sie dazu die mitgeleiferten 19"-Montagewinkel. Bringen Sie ggf. die Gummifüße auf der Unterseite des Gerätes an, um Kratzer auf den Oberflächen anderer Geräte zu vermeiden.

Achten Sie auf eine ausreichende Belüftung des Gerätes, um Schäden durch übermäßige Wärmeentwicklung zu vermeiden.

② **LAN-Anschluss** – schließen Sie die Netzwerkgeräte über ein geeignetes Twisted-Pair-Kabel (TP-Kabel) an die Ports des LANCOM Switches an. Die Anschlüsse erkennen die mögliche Überrtagungsgeschwindigkeit und die Pin-Belegung automatisch (Autosensing).

Verwenden Sie nur normgerechte TP-Kabel der Kategorie CAT 5 oder besser mit einer maximalen Länge von 100 m, um eine einwandfreie

Datenübertragung zu gewährleisten. Crossover-Kabel mit gekreuzten Kontakten können aufgrund der Autosensing-Funktion ebenfalls verwendet werden.

Zur Nutzung der Glasfaseranschlüsse sind zusätzliche Module erforderlich, die Sie als Zubehör erwerben können.

③ **Mit Spannung versorgen und einschalten** – versorgen Sie das Gerät über das Kaltgerätekabel mit Spannung.

④ **Betriebsbereit?** – Nach einem kurzen Selbsttest des Geräts leuchtet die Power-LED permanent. Grün leuchtende LAN-LINK-LEDs zeigen an, an welchen LAN-Anschlüssen funktionierende Verbindungen hergestellt sind.

2.5 Installation der Software

Der folgende Abschnitt beschreibt die Installation der mitgelieferten SystemsoftwareLANtools unter Windows.

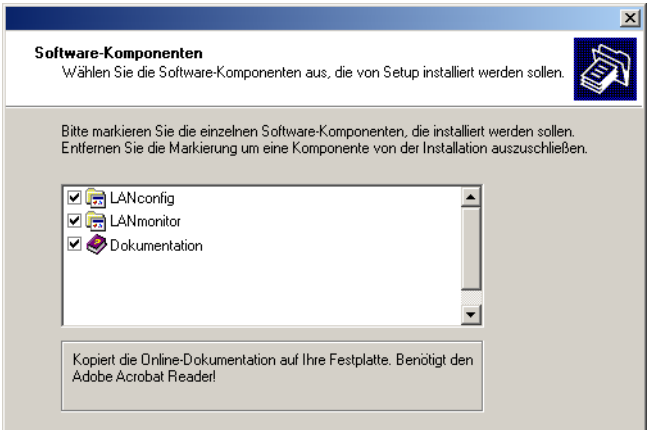
Sollten Sie Ihren LANCOM Switch ausschließlich mit PCs verwenden, die unter anderen Betriebssystemen als Windows laufen, können Sie diesen Abschnitt überspringen.

2.5.1 Software-Setup starten

Legen Sie die Produkt-CD in Ihr Laufwerk ein. Daraufhin startet das Setup-Programm automatisch.

Sollte das Setup nicht automatisch starten, so rufen Sie die Datei AUTORUN.EXE aus dem Hauptverzeichnis der LANCOM-CD auf.

Klicken Sie im Setup auf **Software installieren**. Es erscheint folgendes Auswahlmenü auf dem Bildschirm:



2.5.2 Welche Software installieren?

- **LANconfig** ist das Windows-Konfigurationsprogramm für alle LANCOM-Geräte. Mit LANconfig können Sie alle LANCOM-Geräte im Netzwerk suchen. Für einen LANCOM Switch können Sie damit die webbasierte Konfiguration starten.
- Mit **LANmonitor** überwachen Sie auf einem Windows-Rechner alle LANCOM-Geräte. Für einen LANCOM Switch können Sie damit alle wichtigen Statusinformationen wie z. B. den Link-Status oder den PoE-Zustand der Ports einsehen.

Wählen Sie die gewünschten Software-Optionen aus und bestätigen Sie mit **Weiter**. Die Software wird automatisch installiert.

DE

3 LANCOM Switch konfigurieren und überwachen

3.1 Konfigurationsmöglichkeiten

Zur Konfiguration des Geräts stehen zwei unterschiedliche Wege zur Auswahl:

- Grafische Benutzeroberfläche über einen Browser (WEBconfig): diese Konfigurationsmöglichkeit können Sie nur über eine Netzwerkverbindung nutzen, wenn Sie das Gerät von Ihrem Rechner aus über die IP-Adresse erreichen können. Zusätzlich steht Ihnen WEBconfig auch über SSL-Verschlüsselung zur Verfügung (nur LANCOM ES-2126+).

  Hinweise zur Konfiguration über WEBconfig finden Sie im Kapitel "Webbasierte Konfiguration".

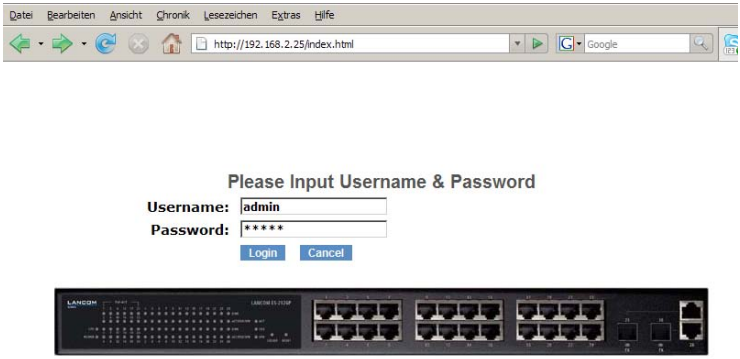
- Textorientierte Konfiguration über eine Konsole (Command Line Interface – CLI): diese Konfigurationsmöglichkeit können Sie über Telnet, SSH (nur LANCOM ES-2126+), Hyperterminal o.ä. sowohl über eine Netzwerkverbindung als auch über eine Direktverbindung über die serielle Konfigurationsschnittstelle (RS-232) nutzen.

  Hinweise zur Konfiguration über CLI finden Sie im Kapitel "Command Line Interface".

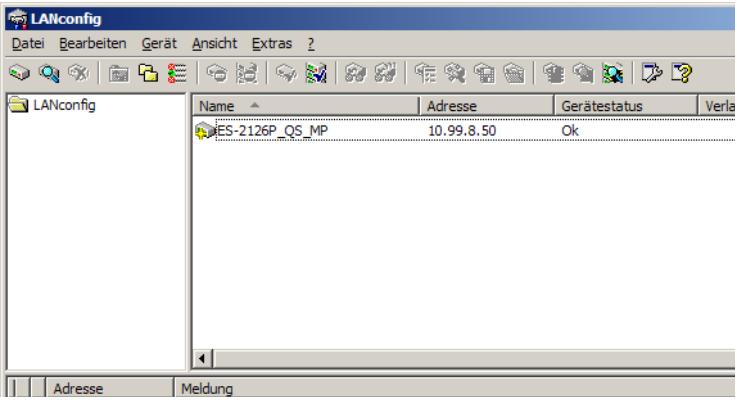
3.1.1 WEBconfig starten

Sie können die Konfiguration über einen Browser auf zwei Wegen starten:

- Wenn Ihnen die IP-Adresse des Gerätes bekannt ist, geben Sie einfach die IP-Adresse in die Adresszeile des Browsers ein. Die bei Auslieferung gültigen Zugangsdaten lauten: Username „admin", Password „admin".



- Wenn Ihnen die IP-Adresse des Gerätes nicht bekannt ist, können Sie mit Hilfe von LANconfig danach suchen. Starten Sie dazu LANconfig über **Start ▶ Programs ▶ LANCOM ▶ LANconfig**.



LANconfig sucht automatisch nach erreichbaren Geräten in Ihrem Netzwerk. Neben anderen evtl. vorhandenen LANCOM-Geräten wird dabei auch ein LANCOM Switch gefunden und in der Liste angezeigt. Mit einem Doppelklick auf diesen Eintrag starten Sie automatisch einen Browser zur entsprechenden IP-Adresse.

Welche IP-Adresse hat mein LANCOM Switch?

Die aktuelle IP-Adresse des LANCOM Switches nach dem Einschalten hängt von der Konstellation des Netzwerks ab.

Netzwerk mit DHCP-Server – Der LANCOM Switch ist bei Auslieferung auf den Auto-DHCP-Modus eingestellt, er sucht also nach einem DHCP-Server, der ihm eine IP-Adresse, die Subnetzmaske und die Adresse des Gateways zuweisen kann. Die zugewiesene IP-Adresse kann dann über entsprechende Tools oder den DHCP-Server ermittelt werden. Handelt es sich beim DHCP-Server z. B. um ein LANCOM-Gerät, so kann die IP-Adresse des LANCOM Switches in der DHCP-Tabelle nachgesehen werden. Der LANCOM Switch kann in diesem Fall von jedem Rechner aus dem Netzwerk erreicht werden, der ebenfalls seine IP-Adresse vom DHCP-Server bezieht.

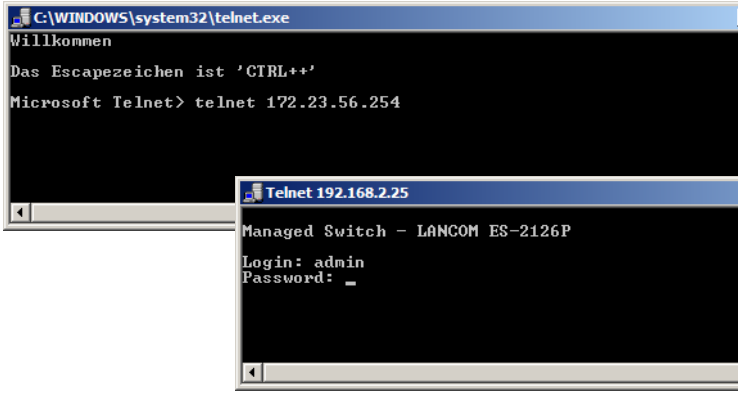
Netzwerk ohne DHCP-Server – Falls im Netzwerk kein DHCP-Server vorhanden ist, so verwendet der LANCOM Switch automatisch die Adresse "172.23.56.250" (LANCOM ES-2126+) bzw. "172.23.56.251" (LANCOM ES-2126P). Der LANCOM Switch kann in diesem Fall von jedem Rechner aus dem Netzwerk erreicht werden, der auf eine IP-Adresse aus dem Adressbereich "172.23.56.x" eingestellt ist.

DE

3.1.2 Command Line Interface über Netzwerk starten

Wenn Ihnen die IP-Adresse des Gerätes bekannt ist (siehe auch vorhergehender Abschnitt) und der LANCOM Switch von Ihrem Rechner aus über das Netzwerk erreichbar ist, können Sie das Command Line Interface über das Netzwerk nutzen.

1. Starten Sie dazu z. B. eine Konsole wie Telnet und geben Sie als Ziel die aktuelle IP-Adresse des Gerätes ein.
2. Melden Sie sich mit Benutzername und Kennwort an (Default: admin, admin).



3.1.3 Command Line Interface über serielle Verbindung starten

Wenn Ihnen die IP-Adresse des Gerätes nicht bekannt ist, können Sie das Command Line Interface über eine serielle Direktverbindung nutzen.

1. Stellen Sie über das serielle Konfigurationskabel eine Verbindung zwischen dem LANCOM Switch und dem Konfigurationsrechner her (→ 'Montage und Anschluss des LANCOM Switch').
2. Starten Sie auf dem Konfigurationsrechner ein Terminalprogramm, z. B. Hyperterminal auf einem Windows-System. Verwenden Sie dabei als Verbindungsparameter:
   - Baudrate: 57600
   - Stop Bits: 1
   - Data Bits: 8

- Parity: N
- Fluss-Kontrolle: keine

3. Melden Sie sich mit Benutzername und Kennwort an (Default: admin, admin).

3.2 Welche Konfiguration verwendet das Gerät?

Der Switch untersützt vier unterschiedliche Konfigurationen: Die Start-Konfiguration, die aktuell aktive Working-Konfiguration, die Benutzer-Konfiguration und die Default-Konfiguration.

1. Start-Konfiguration

   Bei Systemstart übernimmt das Gerät die Parameter aus der Start-Konfiguration und kopiert diese in die Working-Konfiguration. Bei Auslieferung ist diese Start-Konfiguration gleich der Default-Konfiguration.

Um die Start-Konfiguration zu ändern, müssen die geänderten Parameter gezielt als Start-Konfiguration gespeichert werden.

2. Working-Konfiguration:

   Dies ist die aktuell im Gerät aktive Konfiguration, sie kann jederzeit verändert werden. Alle Einstellungsänderungen werden in diesen Einstellungssatz gespeichert. Wann immer Sie eine Änderung mit <Apply> (Anwenden) bestätigen, wird diese Änderung in der Working-Konfiguration gespeichert.

Die Änderungen in der Working-Konfiguration werden **nicht** automatisch in die Start-Konfiguration übernommen, sondern müssen gezielt als Start- oder User-Konfiguration gespeichert werden. Falls die Änderungen in der Working-Konfiguration nicht gespeichert werden, wird beim nächsten Systemstart wieder die vorherige Start-Konfiguration verwendet, die Änderungen an der Working-Konfiguration gehen verloren!

3. User-Konfiguration:

   Diese Konfiguration ist für spezielle Anforderungen oder zu Backup-Zwecken angelegt. Sie können einen beliebigen Stand der Working-Konfiguration als User-Konfiguration speichern und diesen Zustand später mit der

Funktion "Restore User Configuration" (Wiederherstellen der Benutzerkonfiguration) wiederherstellen.

Mit Hilfe der User-Konfiguration kann z. B. über die serielle Konfigurationsschnittstelle und das Command Line Interface eine funktionsfähige, gesicherte Konfiguration wieder als Start-Konfiguration geladen werden, wenn die aktuelle Start-Konfiguration fehlerhaft ist und das Gerät über das Netzwerk nicht mehr erreichbar ist.

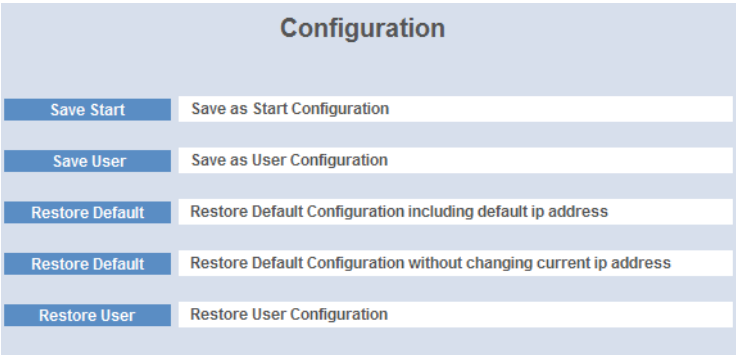
4 Default-Konfiguration:

Dies ist die Werkseinstellung, sie kann nicht verändert werden. In der Web-Oberfläche werden folgende Möglichkeiten angeboten, den Switch auf diesen Einstellungssatz zurückzusetzen.

- Mit der Funktion "Restore Default Configuration included default IP Adress" (Auf Werkseinstellungen inklusive Default-IP-Adresse zurücksetzen) setzen Sie den Swich wieder in den Auslieferungszustand zurück (inklusive des Administrator-Kennworts und der Auto-DHCP-Einstellung).
- Die Funktion "Restore Default Configuration without changing current IP address" erlaubt es ihnen den Switch auf Werkseinstellungen zurückzusetzen, ohne dessen IP-Adresse zu verändern. Der Switch wird auch weiterhin über die von Ihnen zuletzt eingestellte IP-Adresse erreichbar sein.
- Über die serielle Konfigurationsschnittstelle können Sie das Gerät auch ohne Kenntnis des aktuellen Administrator-Kennworts auf den Auslieferungszustand zurücksetzen. Stellen Sie dazu eine serielle Verbindung zu dem Gerät her wie unter → 'Command Line Interface über serielle Verbindung starten' beschrieben. Drücken Sie im Terminalprogramm vor der Eingabe des Benutzernamens Strg+Z und verwenden Sie „RESET" als Benutzernamen und die MAC-Adresse des geräts (ohne Leerzeichen) als Kennwort.

Mit dieser Aktion wird der Reset-Prozess gestartet, dabei werden alle Einstellungen auf den Auslieferungszustand zurückgesetzt, inklusive des Administrator-Kennworts und der Auto-DHCP-Einstellung.

3.2.1 Save/Restore



- Save As Start Configuration

  Hier können Sie die aktuelle Konfiguration als Start-Konfiguration im Flash-Speicher ablegen.

- Save As User Configuration

  Speichern Sie hier die aktuelle Konfiguration als Benutzerkonfiguration im Flash-Speicher.

- Restore Default Configuration (includes default IP address)

  Sie können den Switch hier auf Werkseinstellungen zurücksetzen. Die Default-Konfiguration wird die Start-Konfiguration ersetzen. Das Gerät wird dabei auch auf Auto-DHCP zurückgesetzt und bezieht die IP-Adresse von einem DHCP-Server im Netzwerk. Falls kein DHCP-Server erreichbar ist, verwendet das Gerät die IP-Adresse "172.23.56.252" (LANCOM ES-2126+) bzw. "172.23.56.251" (LANCOM ES-2126P).

- Restore Default Configuration (excludes current IP address)

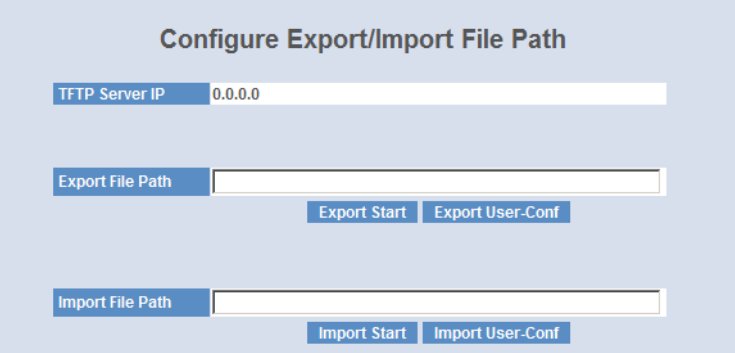
  Sie können den Switch hier auf Werkseinstellungen zurücksetzen. Die Default-Konfiguration wird die Start-Konfiguration ersetzen. Allerdings wird der Switch auch nach dem Zurücksetzen unter der aktuellen IP-Adresse erreichbar sein und nicht auf die Default-IP-Adresse eingestellt.

- Restore User Configuration

  Die Wiederherstellung der Benutzerkonfiguration kann die letzte, als funktionierend bekannte Konfiguration aus dem Flash-Speicher laden und als Start-Konfiguration einstellen. Nachdem der Wiederherstellungsvorgang abgeschlossen ist und die Startkonfiguration neu gesetzt wurde,

muss das System neu gestartet werden um die Änderungen wirksam werden zu lassen.

3.2.2 Config File



- Config File

  Hier können Sie die Start- und Benutzerkonfiguration per TFTP als Backup sichern oder laden.

- Parameter
  - Export File Path:

    Export Start: Sie können die Start-Konfiguration aus dem Flash-Speicher exportieren.

    Export User-Conf: Sie können die Benutzer-Konfiguration aus dem Flash-Speicher exportieren.
  - Import File Path:

    Import Start: Hier können Sie die Start-Konfiguration aus dem Flash-Speicher importieren.

    Import User-Conf: Hier können Sie die Benutzer-Konfiguration aus dem Flash-Speicher importieren.

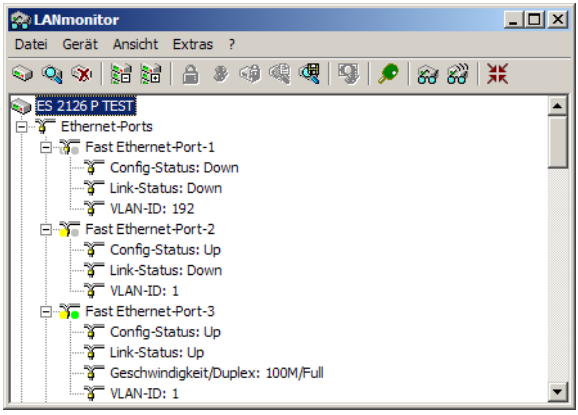
3.3 LANCOM Switch mit LANmonitor überwachen

Der Zustand des Gerätes und der einzelnen Ports kann über die LEDs an der Vorderseite beobachtet werden. Mit dem LANmonitor kann diese Überwachung sehr komfortabel von jedem Arbeitsplatz aus geschehen – ohne direkte Sichtverbindung zu den LEDs. Neben den Statusinformationen der LEDs kön-

nen mit dem LANmonitor noch weitere wichtige Zustandsinformationen über die Ports abgefragt werden.

3.3.1 Status der Ethernet-Ports

Der LANmonitor zeigt für alle Ethernet-Ports des Gerätes den aktuellen Status an. Dabei wird sowohl der vom Administrator konfigurierte Status angezeigt (Config-Status) als auch der tatsächliche Verbindungs-Status des Ports (Link-Status). Dazu wird jeder Port mit zwei farbigen Punkten im LANmonitor dargestellt:



- Der linke Punkt zeigt den Config-Status:
  - grau: der Port ist in der Konfiguration deaktiviert
  - gelb: der Port ist in der Konfiguration aktiviert
- Der rechte Punkt zeigt den Link-Status:
  - grau: an den Port ist kein aktives Netzwerkgerät angeschlossen
  - grün: an den Port ist ein Netzwerkgerät angeschlossen und aktiv

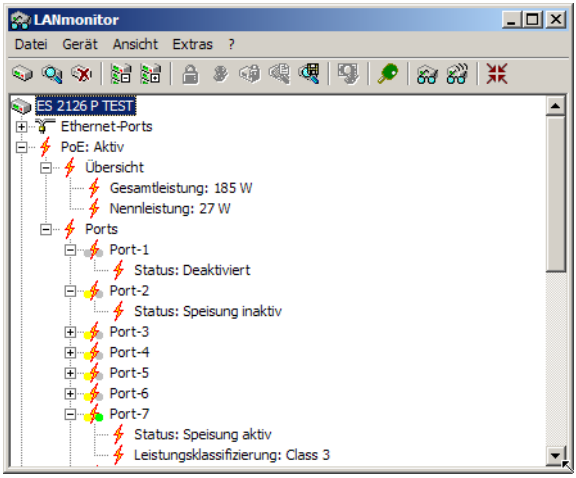
Neben dem Status zeigt LANmonitor außerdem die VLAN-ID für jeden Port an und für aktive Ports mit aktiven Netzwerkgeräten die ermittelte Übertragungsgeschwindigkeit.

3.3.2 PoE-Status der Ports

Der LANmonitor zeigt für alle Ports des Gerätes den aktuellen PoE-Status an. Dabei wird sowohl der vom Administrator konfigurierte Status angezeigt (PoE aktiviert oder deaktiviert) als auch die tatsächliche Speisung der angeschlos-

DE

senen Netzwerkgeräte. Dazu wird jeder Port mit zwei farbigen Punkten im LANmonitor dargestellt:



- Der linke Punkt zeigt den PoE-Konfiguration:
  - grau: die PoE-Speisung ist für den Port in der Konfiguration deaktiviert
  - gelb: die PoE-Speisung ist für den Port in der Konfiguration aktiviert
- Der rechte Punkt zeigt die aktuelle Stromversorgung:
  - grau: an dem Port ist kein aktives Netzwerkgerät angeschlossen, das eine PoE-Versorgung benötigt
  - grün: an den Port ist ein Netzwerkgerät angeschlossen, das über PoE mit Strom versorgt wird

Neben dem PoE-Status zeigt LANmonitor ausserdem für die über PoE versorgten Netzwerkgeräte an, welche PoE-Klasse jeweils ermittelt wurde. Das Power Source Equipment (PSE) misst beim Anschluss eines Powered Device (PD), welchen Leistungsbedarf das Gerät hat. Der Leistungsbedarf der PDs wird in folgenden Klassen angegeben:

PoE-Klasse	Verwendung	Leistungsbereich
0	default	0,44 W - 12,95 W
1	optional	0,44 W - 3,84 W

PoE-Klasse	Verwendung	Leistungsbereich
2	optional	3,84 W - 6,49 W
3	optional	6,49 W - 12,95 W
4	reserviert	15,4 W

DE

4 Anleitung zum webbasierten Management

Dieses Kapitel zeigt Ihnen, wie Sie mit Hilfe des webbasierten Managements (WEBconfig) den LANCOM Switch konfigurieren. Diese Methode ermöglicht Ihnen auf einfache Weise den Zugang zu jedem Port und Status des Switchs. Ebenso können Sie den MIB-Status, Spanning Tree Status, Prioritätenstatus, den Multicast Traffic und das VLAN einsehen sowie die unerlaubte Nutzung überwachen.

Die Grundeinstellungen des Switchs sind in der folgenden Tabelle aufgelistet:

	LANCOM ES-2126+	LANCOM ES-2126P
IP Adress	172.23.56.252	172.23.56.251
Subnet Mask	255.255.255.0	255.255.255.0
Default Gateway	172.23.56.254	172.23.56.254
Default DNS-Server	172.23.56.254	172.23.56.254
Username	admin	admin
Password	admin	admin

Wenn Sie die erste Konfiguration des Switchs mit Hilfe des Command Line Interfaces durchgeführt und dabei die IP-Adresse geändert haben, können Sie die entsprechende IP-Adresse eingegeben. Sie sehen den folgenden Bildschirm, in dem Sie Ihren Benutzernamen und Ihr Passwort zur Authentifizierung eingeben müssen. Wenn Sie sich das erste Mal einloggen, geben Sie sowohl als Benutzername wie auch als Passwort “admin” ein und schließen die Anmeldung ab, indem Sie auf Login klicken.

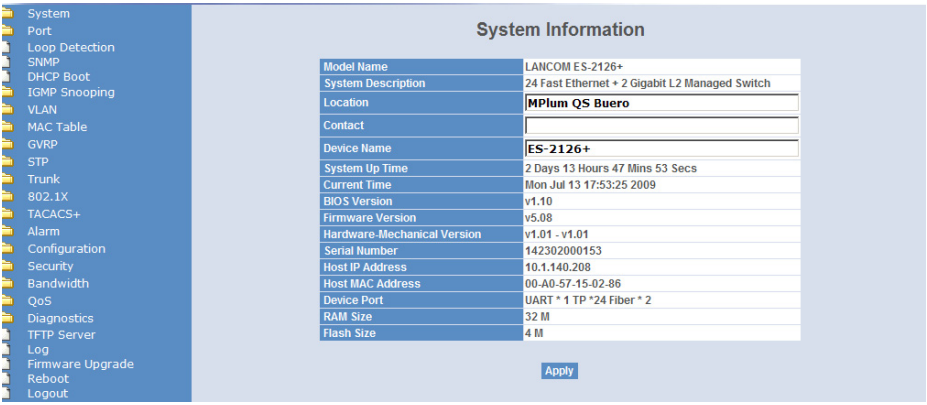
Ihnen steht alternativ auch eine Anmeldung über eine verschlüsselte Verbindung zur Verfügung. Der LANCOM Switch verwendet hierzu “SSL”(Secure Sockets Layer) über HTTPS und verfügt bereits über das benötigte Zertifikat. Bei dieser Übertragungsmethode sind alle Daten verschlüsselt und lassen sich nicht von Unbefugten missbrauchen.

In den Switch können sich gleichzeitig maximal drei Benutzer einloggen. Das Gerät erlaubt jedoch jeweils nur einem Administrator, das System zu konfigurieren. Wenn gleichzeitig mehrere Administratoren eingeloggt sind, erlaubt der Switch demjenigen Administrator das System zu konfigurieren, der sich als erster eingeloggt hat. Die anderen Benutzer können in diesem Fall, auch wenn sie Administratorrechte besitzen, das System nur überwachen.

Zur Darstellung der WEBconfig empfehlen wir Internet Explorer 6.0 oder höher bzw. einen aktuellen Firefox bei einer Bildschirmauflösung von 1024x768.

4.1 Übersicht über das webbasierte Management

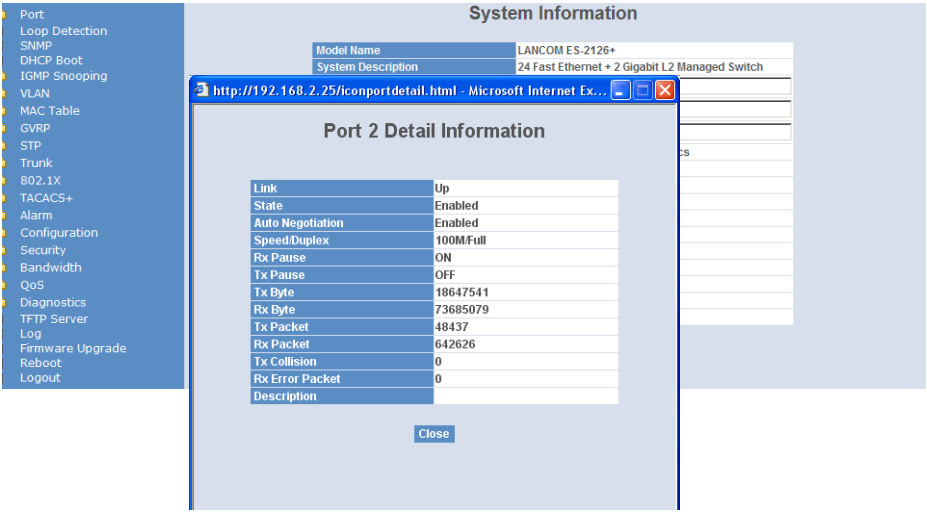
Nach dem Einloggen sehen Sie auf dem Bildschirm die Systeminformationen, wie "Model Name", "System Description", "Location", "Contact", "Device Name", "System Up Time", "Current Time", "BIOS Version", "Firmware Version", "Hardware-Mechanical Version", "Serial Number", "Host IP Address", "Host MAC Address", "Device Port", "RAM Size" and "Flash Size". Sie erhalten auch Informationen über die Software Version, die MAC Adresse, die Seriennummer, die Anzahl der Ports usw. .



Informationen zum Seiten-Aufbau

Oben auf der Seite sehen Sie die Vorderseite des Switchs. Die verlinkten Ports leuchten grün, im Gegensatz dazu leuchten die unverlinkten Ports nicht.

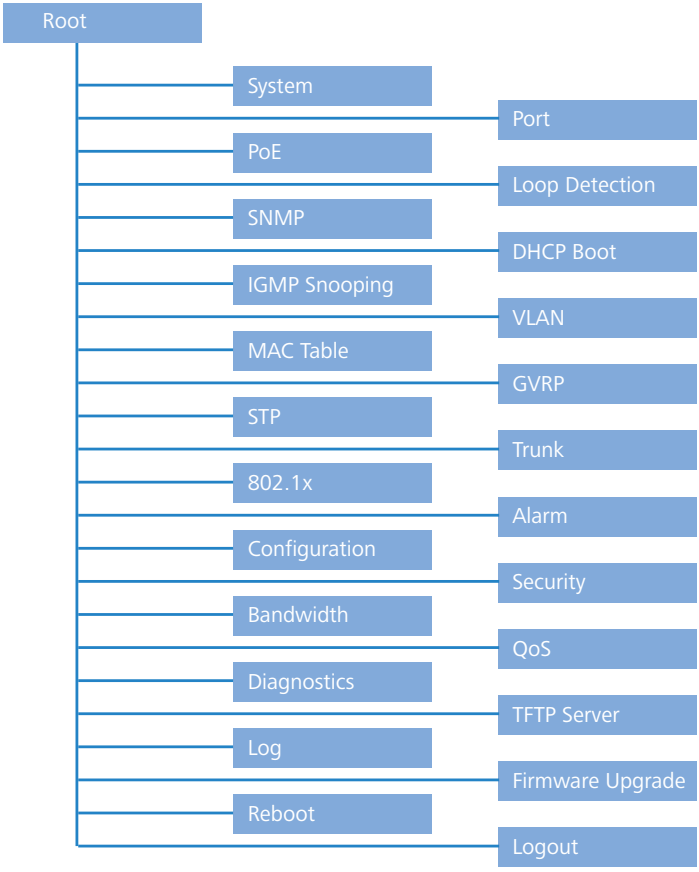
Mit einem Klick auf die einzelnen Ports in der Grafik öffnen Sie ein Fenster mit Detail-Informationen (gegebenenfalls Pop-Up-Blocker ausschalten).



Das Detailfenster zeigt die grundlegenden Informationen zum Status, zum Traffic und der Bandbreite für den jeweiligen Ein- und Ausgang eines gewählten Ports.

In der Ecke rechts oben befindet sich die Zeit des Auto-Logouts, welcher Sie nach dem Verlassen des Programms vor unberechtigten Nutzern schützt. Wenn Sie die Voreinstellung des Auto-Logouts unverändert lassen, wird sich das System drei Minuten nach der letzten Aktivität automatisch ausloggen. Wenn Sie die Funktion des Auto-Logouts ausschalten, bleiben Sie dauerhaft eingeloggt.

Auf der linken Seite sehen Sie das Hauptmenü. Wenn Sie einen Ordner öffnen, erscheint ein Untermenü. Die Funktionen jedes einzelnen Ordners sind in den entsprechenden Kapiteln erklärt. Wenn Sie eine Funktion anklicken, erfolgt die Ausführung. Die folgende Liste zeigt alle Funktionen für WEBconfig.



4.2 System

4.2.1 System Information

Zeigt die grundlegenden Informationen des Systems an.

- Parameter:
  - Model name:

    Den Modellnamen entnehmen Sie dieser Anleitung.
  - System description:

Beschreibt das System, in diesem Fall handelt es sich um ein "24-Port 10/100/1000BaseT/TX Managed Switch".

- Location:

Dies ist der Ort an dem sich der Switch befindet (benutzerdefiniert).

- Contact:

Hier können Sie den Namen und die Telefonnummer der Kontaktperson eingeben, die Ihnen Hilfestellung leistet. Sie können diese Einstellung über die Benutzeroberfläche oder SNMP konfigurieren.

- Device name:

Der Name des Switchs (benutzerdefiniert). Die Voreinstellung ist "LANCOM ES-2126+" bzw. "LANCOM ES-2126P".

- System up time:

Angabe der Zeit, seit der Switch in Betrieb genommen wurde. (Format: Tag, Stunde, Minute und Sekunde)

- Current time:

Aktuelle Zeitangabe (Format: Tag der Woche, Monat, Tag, Stunden und Minuten, z. B. Thu May 15 12:36:14 2008)

- BIOS version:

Die Version des BIOS in diesem Switch.

- Firmware version:

Die Firmware Version in diesem Switch.

- Hardware-Mechanical version:

Die Version der Hardware und der Mechanik.

- Serial number:

Die Seriennummer wird von der Fabrik vergeben.

- Host IP address:

Die IP-Adresse des Switchs.

- Host MAC address:

Die Ethernet MAC Adresse des Managers von diesem Switch.

- Device Port:

Zeigt alle Typen und Nummern des Switch-Ports.

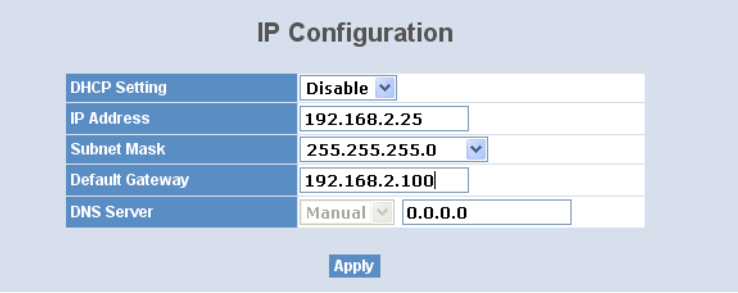
- RAM size:

Die Größe des DRAM in diesem Switch.

- Flash size:

  Die Größe des Flash-speicher in diesem Switch.

4.2.2 IP Configuration



Die IP Konfiguration ist eine der wichtigsten Systemeinstellungen des Switchs, denn hiermit kann der Netzwerkmanager die Einstellungen einsehen und bearbeiten. Sie können beim Switch manuelle IP-Adressen oder automatischen IP-Adressen mit Hilfe des DHCP Server einstellen. Wenn Sie die IP-Adresse ändern, müssen Sie den Switch neu booten und können anschließend die neue IP-Adresse für das webbassierte Management und CLI nutzen.

- IP Configuration

  Bestimmt die IP Adresse, die Subnetzmaske, Gateway und DNS (domain name system) des Switchs.

- Parameter:

  - DHCP Einstellung:

    DHCP ist die Abkürzung für Dynamic Host Configuration Protocol. Der Switch bekommt mit Hilfe des DHCP-Client automatisch eine IP-Adresse , wenn Sie die Funktion auf “enable” stellen. Bei dieser Einstellung übermittelt der Switch die Anfrage an den, sich im Netzwerk befindenden, DHCP Server, um eine I- Adresse zu erhalten. Wenn der DHCP Server ausgeschaltet oder nicht vorhanden ist, wird der Switch so lange weiter anfragen (und dies auch anzeigen) bis der DHCP Server angeschlossen bzw. angeschaltet ist. Sie benötigen zuerst die IP-Adresse vom DHCP Server um weitere booting Prozesse ausführen zu können. Wenn Sie die Einstellung “disable” wählen, müssen Sie die IP-Adresse manuell eingeben. Weitere Details zum Thema IP-Adresse und DHCP finden Sie in Kapitel 2.1.5 “Einstellung der IP-Adresse”.

DE

Default: Disable

- IP-Addresse:

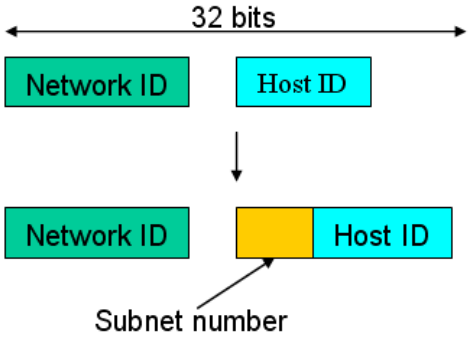
  Wenn Sie die DHCP Funktion auf “disable” einstellen, können Sie die IP-Adresse konfigurieren und neue Werte eintragen. Klicken Sie zum Updaten “apply”. Wenn DHCP gesperrt ist, lautet der Default “172.23.56.252” (LANCOM ES-2126+). Wenn DHCP freigegeben ist, wird diese Angabe vom DHCP Server bestimmt und lässt sich nicht mehr vom Benutzer einstellen.

- Subnetzmaske:

  Die Subnetzmaske teilt die IP-Adresse des Geräts in einen Netzwerkteil und einen Geräteteil auf. Der Netzwerkteil bezeichnet das Netzwerk, in dem sich der Rechner befindet. Nur Rechner in einem gemeinsamen Netzwerk können direkt miteinander kommunizieren. Alle Geräte in anderen Netzwerken können nur über Router erreicht werden. Der Geräteteil bezeichnet dann das einzelne Gerät innerhalb des Netzwerks. Die Geräteadresse muss innerhalb eines Netzwerks eindeutig sein.

  Weitere Informationen zu diesem Thema finden Sie in Kapitel “Bestimmung der IP Adresse”.

  Default: 255.255.255.0



- Default gateway:

Stellen Sie eine IP-Adresse für ein Gateway ein, um mit Datenpaketen umzugehen, die die Kriterien eines Pfades nicht erfüllen. Wenn ein Datenpaket die Kriterien eines voreingestellten Pfades nicht erfüllt, muss es auf einem Default-Pfad an einen Router weitergeleitet werden. Das bedeutet, dass jedes Paket mit einer undefinierten IP-Adresse automatisch an diese Default-Einheit gesendet wird.

Default: 172.23.56.254

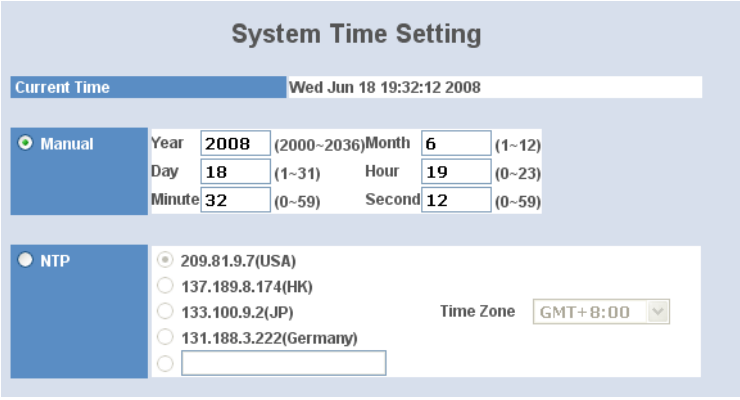
- DNS (Domain Name System):

Die Übersetzung/Übermittlung der IP-Adresse und der Namensadresse erfolgt mit dem DNS Server. Der Switch unterstützt die DNS Funktion um die Adresse zum DNS Server zu senden und die zugehörige IP Adresse für den Internetzugang zu bekommen.

Es gibt zwei Wege die IP Adresse des DNS festzulegen. Die eine Möglichkeit ist der "fixed mode" und bestimmt die IP Adresse manuell. Die andere ist im "dynamic mode" welche dem DHCP Server zugewiesen ist, wenn DHCP aktiviert/freigegeben ist. Das DNS hilft Ihnen, den "mnemonic adress name" in Erinnerung zu behalten. Der default ist keine Zuteilung einer DNS Adresse.

Default: 172.23.56.254

4.2.3 Time



Der Switch bietet den manuellen und den automatischen Weg zum Einstellen der Zeit mit NTP an. Die manuelle Einstellung ist unkompliziert, denn Sie tragen einfach Jahr, Monat, Tag, Stunde, Minute und Sekunde mit einem gülti-

gen Wert ein. Wenn Sie einen ungültigen Wert eintragen, z. B. 61 Minuten , wird der Switch die Eingabe auf die Zahl 59 korrigieren.

NTP ist ein Protokoll, das die Uhren des Switch Zeitsystems synchronisiert. Bei NTP handelt es sich um einen Internet Entwurf, der in der dritten Version in das Protokoll eingebunden wurde und standardmäßig in RFC 1305 formalisiert wird. Der Switch besitzt vier eingebaute NTP Server IP-Adressen im Internet und eine benutzerdefinierte NTP Server IP-Adresse. Die Zeitzone ist Greenwich mean time und wird dargestellt in der Form GMT+/- xx hours.

Time

Stellen Sie das System manuell ein oder synchronisieren Sie die Zeitangaben mit Hilfe eines Zeit-Servers. Sie können außerdem verschiedene Zeitzonen einstellen.

- Parameter
  - Current Time:

Zeigt die aktuelle Zeit des Systems an.

  - Manuelle Einstellung:

Mit dieser Funktion können Sie die Zeit manuell einstellen. Füllen Sie die Felder mit gültigen Werten für Jahr, Monat, Tag, Stunde, Minute und Sekunde und klicken Sie anschließend auf “apply”. Mögliche Werte für die Parameter Jahr, Monat, Tag, Stunde, Minute und Sekunde sind entsprechend >=2000, 1-12, 1-31, 0-23, 0-59 und 0-59. Wenn Sie einen falschen Wert eingeben und “apply” drücken, wird das System die Zeiteinstellung nicht annehmen.

Default: Jahr = 2000, Monat = 1, Tag = 1, Stunde = 0, Minute = 0, Sekunde = 0

  - NTP:

NTP ist ein Network Time Protocol und wird dazu benutzt um die Greenwich mean time zu synchronisieren. Wenn Sie den NTP-Modus gebrauchen, wählen Sie einen eingebauten NPT Time Server oder stellen Sie manuell einen benutzerdefinierten NTP Server ein. Bestimmen Sie eine Zeitzone. Der Switch wird die Zeit synchronisieren nachdem Sie “apply” drücken. Auch wenn der Switch die Zeit automatisch synchronisiert, kann NTP die Zeit ohne die Bearbeitung des Benutzers nicht regelmäßig updaten .

Die Zeitzone ist eine offset Zeit von GMT. Bestimmen Sie zuerst die Zeitzone und führen Sie dann die Synchronisation mit Hilfe des NTP aus. Der

Switch wird NTP updaten. Der Switch unterstützt konfigurierbare Zeitzonen von -12 bis +13 in Schritten von einer Stunde.

Default Zeitzone: Germany +1 Stunde

- Einstellung der Sommerzeit:

Für einige Länder wird die Sommerzeit übernommen. Diese Einstellung gleicht die Zeitverschiebung an oder ändert die Zeit, gemäß des Start- und Enddatums. Stellen Sie die Sommerzeit z. B. auf eine Stunde ein. Wenn das eingegebene Startdatum um eine Minute überschritten wird, so wird die Zeit des Systems eine Stunde zurückgesetzt. Wenn das Enddatum überschritten wird, wird ebenfalls so verfahren.

Die Einstellung der Sommerzeit kann -5 bis +5 Stunden betragen, in Schritten von je einer Stunde. Wenn die Zeitverschiebung von der Winter- zur Sommerzeit (und umgekehrt) nicht übernommen werden muss/soll, geben Sie in das Feld eine Null ein (oder deaktivieren Sie die Sommerzeiteinstellung). Sie müssen in diesem Fall kein Start- und Enddatum angeben. Wenn Sie eine Zeitverschiebung für die Sommerzeit angeben, müssen Sie für die Aktivierung auch ein Start- und Enddatum angeben.

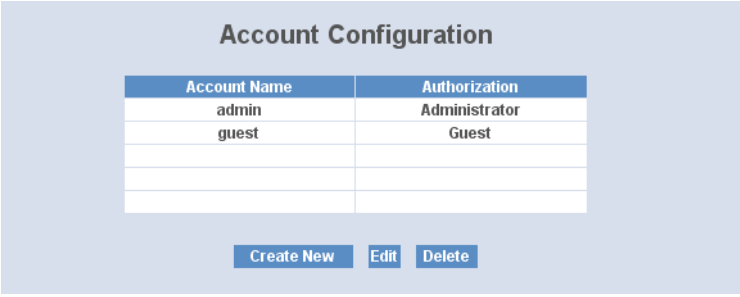
Default für die Einstellung der Sommerzeit: 0.

Die folgenden Parameter sind konfigurierbar für die Sommerzeiteinstellung:

- Day Light Saving Start / Start der Sommerzeit:
  Gibt an, wann die Sommerzeit beginnt.
- Mth /Monat:
  Eingabe 1 ~ 12; Default: 1
- Day /Tag:
  Eingabe 1 ~ 31; Default: 1
- Hour/ Stunde:
  Auswahl 0 ~ 23; Default: 0
- Day Light Saving End/ Ende der Sommerzeit :
  Gibt an, wann die Sommerzeit endet.
- Mth/ Monat:
  Eingabe 1 ~ 12; Default: 1
- Day/ Tag:
  Eingabe1 ~ 31; Default: 1

- Hour/ Stunde:
  Eingabe 0 ~ 23; Default: 0

4.2.4 Account



Mit dieser Funktion kann der Administrator den Benutzernamen und das Passwort erstellen, verändern oder löschen. Der Administrator kann die Passwörter anderer Gastbenutzer verändern ohne das Passwort zu bestätigen. Gastbenutzer können nur ihr eigenes Passwort verändern. Bitte denken Sie daran, dass Sie die jeweilige Identität (Gast/ Administrator) in dem Feld "authorization" eingeben, bevor Sie den Benutzernamen und das Passwort erstellen. Es kann nur ein Administrator angemeldet werden. Dieser kann nicht gelöscht werden. Zusätzlich können jedoch vier Accounts für Gastbenutzer erstellt werden.

Nur für LANCOM ES-2126+

Beim Verwenden von TACACS+ wird die Benutzer-Authentifizierung von einem externen AAA-Server durchgeführt und muss daher auch dort konfiguriert werden.

- Die Voreinstellung für den Benutzer-Account ist:
  Username/ Benutzername: admin
  Password/ Passwort: admin

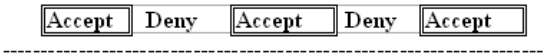
4.2.5 Management Policy

Mit dieser Einstellungen kann der verantwortliche Manager das genaue Setup erstellen um den Switch zu kontrollieren und die Anzahl der Benutzer zu bestimmen.

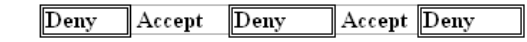
Die folgenden Regeln stehen Ihnen zum Managen des Switchs zur Verfügung:

1. Wenn keine Liste existiert, werden alle Verbindungen akzeptiert.

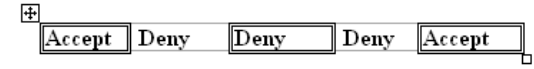
2. Wenn es nur "accept lists" gibt, werden alle Verbindungen abgelehnt, außer diejenigen innerhalb des akzeptierten Bereichs .



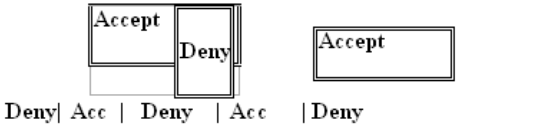
3. Wenn es nur "deny lists" gibt, werden alle Verbindungen akzeptiert, außer die Verbindungen innerhalb des abgelehnten Bereichs.



4. Wenn es sowohl "accept and deny lists" gibt, werden alle Verbindungen abgelehnt, außer die Verbindungen innerhalb des akzeptieren Bereichs.



5. Wenn es sowohl "accept and deny lists" gibt, werden alle Verbindungen abgelehnt, außer die Verbindungen innerhalb des akzeptiereten Bereichs, die nicht gleichzeitig im abgelehnten Bereich sind.

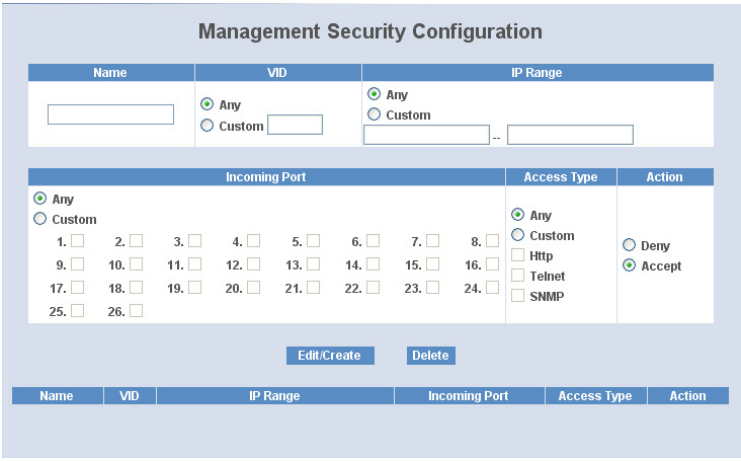


- Management Security Configuration

  Der Switch bietet verschiedene Sicherheitseinstellungen. Mit dieser Funktion kann der Manager den Modus der verbundenen Benutzer kontrollieren. Je nach Modus können Benutzer in zwei Klassen eingeteilt werden:

DE

Diejenigen, die Zugang zum Switch haben (accept) und diejenigen, die keinen Zugang zum Switch haben (deny). Einige Einschränkungen können für die Benutzer, die Zugang zum Switch haben, gemacht werden. Zum Beispiel können Sie entscheiden, welcher VLAN VID vom Switch akzeptiert oder abgelehnt wird. Auch der IP-Bereich der Benutzer, der Port für die Verbindung oder die Verbindung zum Switch über http, telnet oder SNMP kann akzeptiert oder abgelehnt werden.



- Parameter:
  - Name:

    Der Name sollte maximal acht Stellen haben und kann sich aus jedem beliebigen Buchstaben des Alphabeths (A-Z, a-z) sowie aus Zahlen (0-9) zusammensetzen.
  - VID:

    Der Switch unterstützt zwei Optionen um VLAN VID zu bestimmen, "any" und "custom". Default ist "any". Wenn Sie "custom" auswählen, können Sie eine VID Nummer eingeben. Der zugelassene Bereich der Nummer ist 1 ~ 4094 .
  - IP Range:

    Der Switch unterstützt zwei Optionen um den IP Range zu bestimmen, "any" und "custom". Default ist "any". Wenn Sie "custom" wählen, können Sie einen IP Bereich zuweisen. Der zugelassene Bereich ist 0.0.0.0~255.255.255.255 .
  - Incoming Port:

Der Switch unterstützt zwei Optionen um den Port zu bestimmen, “any” und “custom”. Default ist “any”. Wenn Sie “custom” wählen, können Sie die Ports bestimmen, mit denen in der Konfiguration Management Sicherheit gearbeitet werden soll.

- Access Type:

  Der Switch unterstützt zwei Optionen um den Access Type zu bestimmen, “any” und “custom”. Default ist “any”. Wenn Sie “custom” wählen, können Sie den Zugriff unter den drei Optionen “http”, “telnet” und “SNMP” auswählen.

- Action:

  Der Switch unterstützt zwei Optionen um die gültige Aktivität zu bestimmen, “deny” und “accept”. Default ist “deny”. Wenn Sie “accept” wählen, haben Sie die Authorität den Switch zu managen. Wenn Sie die Einstellung “deny” wählen, werden Sie aufgefordert den Switch mit dem von Ihnen gewählten “Access Type” zu managen.

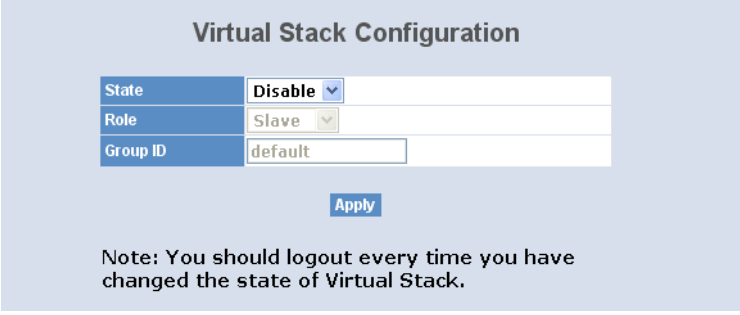
- Edit/Create:

  Neue Einstellungen bezüglich der Sicherheit können übernommen werden, wenn die oben genannten Parameter eingestellt wurden und Sie auf “edit/create” klicken. Natürlich können Sie die Einträge auch verändern, indem Sie die jeweilige Schaltfläche betätigen.

- Delete:

  Löscht die bestehenden Einstellung der Sicherheitstabelle.

4.2.6 Virtual Stack



Virtual Stack Management (VSM) ist die Funktion für das Gruppenmanagement. Mit der Konfiguration dieser Funktion, werden mehrere Switches in dem selben LAN automatisch als Gruppe betrachtet. Ein Switch in der Gruppe wird

DE

als Master angesehen, die anderen werden so genannte "slave devices" (Folgegeräte).

VSM bietet eine einfache Management Funktion. Es ist nicht notwendig, dass Sie sich die Adresse von allen Geräten merken, denn der Manager kann das Netzwerk mit der Adresse des Masterswitchs konfigurieren. Anstelle von SNMP oder Telnet UI, ist VSM auch verfügbar in WEBconfig. Wenn Sie die Einstellung zum Masterswitch vornehmen, werden oben auf dem WEBconfig zwei Buttons für die Gruppeneinstellungen erscheinen. Wenn Sie diese Buttons anklicken, können Sie sich direkt in die Gruppeneinstellungen des WEBconfig einloggen.

Die Schaltfläche ganz links ist für das Mastergerät bestimmt. Wenn Sie auf die Schaltfläche klicken, verändert sich die Hintergrundfarbe , damit wird angezeigt, dass das Gerät von Ihnen gemanagt wird.

Hinweis: Die Gruppierung wird vorübergehend entfernt, wenn Sie sich mit Hilfe der Konsole einloggen.

Die Einstellung der Gruppe wird angezeigt als "station address" (die letzte Nummer der IP-Adresse) mit dem "device name" der Schaltfläche (z. B. 196_LANCOM ES-2126+). Wenn keine entsprechende Einstellung existiert, wird " ----" angezeigt.

Wenn die Gruppeneinstellung vorgenommen wurde, können Sie das System nicht mehr durch Telnet, Console oder Web konfigurieren, sondern nur noch mit Hilfe des Mastergerätes.

Es können bis zu 16 Geräte für VSM zusammengeschaltet werden, jedoch kann es in jeder Gruppe nur einen Master geben. Für die Masterredundanz können Sie mehr als zwei Master bestimmen. Der Master mit dem kleineren MAC-Wert ist der primäre Master. Jedes dieser 16 Geräte kann das Mastergerät werden und die Geräte können gegenseitig ein Backup machen.

- Parameter:
  - State:

    Diese Einstellung wird für die Aktivierung oder Deaktivierung des VSM gebraucht. Default ist aktiv.
  - Role:

    Gibt die Rolle des Switchs im Virtual Stack an. Es werden zwei Typen angeboten, master oder slave (Folgegerät). Default ist master.
  - Group ID:

Dies ist der Gruppen-Identifier (group identifier (GID)) des VSM. Gültig sind alle Buchstaben von A-Z, a-z, Zahlen von 0-9, die Zeichen "-" und "_". Die maximale Länge beträgt 15 Stellen.

4.2.7 System Log

Der Sytem Log gibt Ihnen Informationen über System Logs, inklusive der Information darüber, wann das Gerät gebootet wurde, wie die Ports arbeiten, ob Benutzer eingeloggt sind, Sessions ablaufen und andere Systeminformationen.

System Log:

Die Trap-Log-Angabe zeigt die Log-Einträge der "SNMP Private Trap events", "SNMP Public Traps" und die Benutzer-Logs die im System auftreten. In der Reporttabelle befinden sich drei Felder mit der Nummer, dem Zeitpunkt und dem Ereignis des Trap-Protokolls.

- Parameter:
  - No.:

    Zeigt die Ordnungszahl des Traps an.
  - Time:

    Zeigt die Zeit des Traps an.
  - Desc:

    Zeigt eine Beschreibung der Events im System Log.
  - Clear:

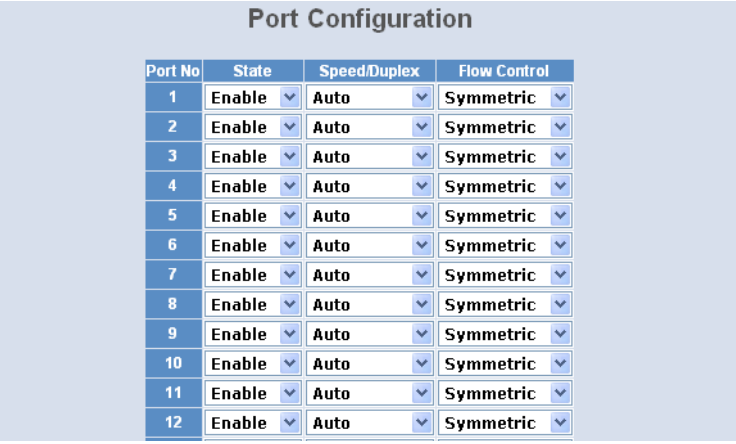
    Löscht die Log Daten.

4.3 Port

Dieser Zweig der Konfiguration beinhaltet die Bereiche Port Konfiguration, Port Status, Simple Counter und Detail Counter.

DE

4.3.1 Configuration



In der Port-Konfiguration können Sie Einstellungen für jeden Port vornehmen. Die folgenden Einstellungen können von Ihnen vorgenommen werden.

Port Konfiguration

Hier können Sie den Operations-Modus für jeden Port festlegen.

- Parameter:
  - State:

    Schalten Sie hier die Kommunikations-Fähigkeit des Ports ein (Enabled). Datenverkehr kann über diesen Port nur stattfinden, wenn Sie diesen Wert auf "Enable", also Aktiviert setzen. Sollte er deaktiviert sein, wird jeder Verkehr über diesen Port blockiert, auch wenn er den Anschein macht verbunden zu sein. Sie können frei zwischen "Enable" (Aktiviert) und "Disable" (Deaktiviert) entscheiden.

    Default: Enable.

  - Speed/Duplex:

    Hier können Sie die Geschwindigkeit und Duplex-Methode des Ports festlegen. Bei der Geschwindigkeit können Sie zwischen 10 und 100 MBit/s Baud-Rate für Fast-Ethernet an den Ports 1-24 wählen. Wenn an die SFP-Ports 25 und / oder 26 ein Glasfaserkabel angeschlossen ist, wird die Geschwindigkeit automatisch auf 1000 MBit/s festgelegt. Mit einem Twisted-Pair-Kabel können Sie die Geschwindigkeit an diesen Ports zwischen 10/100/1000 MBit/s wählen. Beim

Duplex-Modus haben Sie die Wahl zwischen "half duplex" (Semiduplex) und "full duplex" (Vollduplex).

Die folgende Tabelle fasste alle Konfigurationsoptionen zusammen.

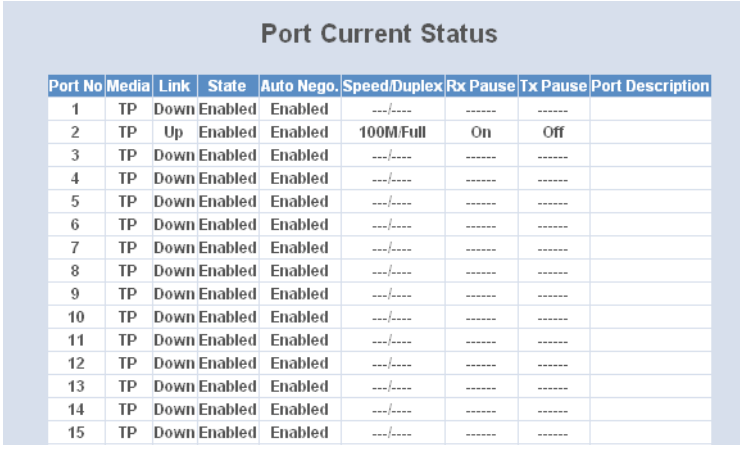
Media type	NWay	Speed	Duplex
100M TP	ON/OFF	10/100M	Full/Half
1000M TP	ON/OFF	10/100/1000M	Full for all, Half for 10/100
1000M Fiber	ON/OFF	1000M	Full

Im automatischen Verhandlungs-Modus (Auto-Negotiation) ist kein Default-Wert gesetzt. Im erzwungenen Modus (Forced Mode) bestimmt Ihre Einstellung den Default-Wert.

- Flow Control:

  Bei der Flusskontrolle (Flow Control) können Sie zwischen dem symmetrischen und dem asymmetrischen Modus wählen. Im symmetrischen Modus können beide Partner ein "PAUSE"-Paket senden, wenn sie überlastet sind. Im asymmetrischen Modus wird ein Gerät, das nur empfängt, die "PAUSE"-Pakete anderer Geräte beachten, aber selber keine versenden. Dies bezeichnet man als unidirektionale Flusskontrolle. Default: Symmetric (Symmetrisch).

4.3.2 Status



Port Current Status

Port No	Media	Link	State	Auto Nego.	Speed/Duplex	Rx Pause	Tx Pause	Port Description
1	TP	Down	Enabled	Enabled	---/----	------	------	
2	TP	Up	Enabled	Enabled	100M/Full	On	Off	
3	TP	Down	Enabled	Enabled	---/----	------	------	
4	TP	Down	Enabled	Enabled	---/----	------	------	
5	TP	Down	Enabled	Enabled	---/----	------	------	
6	TP	Down	Enabled	Enabled	---/----	------	------	
7	TP	Down	Enabled	Enabled	---/----	------	------	
8	TP	Down	Enabled	Enabled	---/----	------	------	
9	TP	Down	Enabled	Enabled	---/----	------	------	
10	TP	Down	Enabled	Enabled	---/----	------	------	
11	TP	Down	Enabled	Enabled	---/----	------	------	
12	TP	Down	Enabled	Enabled	---/----	------	------	
13	TP	Down	Enabled	Enabled	---/----	------	------	
14	TP	Down	Enabled	Enabled	---/----	------	------	
15	TP	Down	Enabled	Enabled	---/----	------	------	

Im Port-Status werden Informationen über den Status aller Ports gesammelt und angezeigt. Die Einträge können nach Port-Nummer, Medium, Link-Status, Port-Status, Status der Auto-Negotiation, Geschwindigkeit/Duplex, PX-Pause und TX-Pause sortiert werden. Für die Ports 25 und 26 wird eine zusätzliche Information über den Medien-Typ angezeigt.

Port-Status

Zeigt den aktuellen Status aller Ports im Switch. Die Anzeige wird alle 5 Sekunden aktualisiert, so dass geänderte Zustände der Ports schnell angezeigt werden.

- Parameter
  - Port No:

    Die Nummer des Ports von 1 bis 26. Die beiden Ports 25 und 26 sind optional.
  - Media:

    Der an den Ports angeschlossene Medien-Typ. Die Ports 25 und 26 sind optionale Module, die sowohl Glasfaser-Kabel als auch UTP-Kabel für Gigabit Ethernet (1000Mbit/s) oder 10/100Mbit/s Fast Ethernet unterstützen. Die Ports können unterschiedliche Medien verwalten. Für einen Glasfaser-Port können umfangreiche Informationen über den Anschlusstyp, die Entfernung usw. angezeigt werden.
  - Link:

    Zeigt an, ob der Port aktiv ist oder nicht. Wenn der Port mit einem aktiven Netzwerkgerät verbunden ist, zeigt der Link "Up", sonst "Down". Dieser Zustand bezieht sich auf beide Seiten der Verbindung.

    Kein Default-Wert.
  - State:

    Zeigt an, ob die Datenübertragung für den Port aktiviert oder deaktiviert ist. Wenn die Datenübertragung aktiviert ist, können über diesen Port Daten empfangen und versendet werden. Wenn die Datenübertragung deaktiviert ist, können über den Port keine Daten übertragen werden. Der Port-Status wird vom Anwender eingestellt.

    Default: aktiviert.
  - Auto Nego.:

    Zeigt den Aushandlungsmodus für die Ethernet-Verbindung. Wenn die Auto-Negotiation (automatische Aushandlung) aktiviert ist, werden die Verbindungsgeschwindigkeit und die Duplexfähigkeit zwi-

schen dem Switch und dem angeschlossenen Netzwerkgerät automatisch ausgehandelt. Dabei wird die beste Verbindungsmöglichkeit gewählt. Wenn die Auto-Negotiation deaktiviert ist, müssen die beiden Geräte auf die gleichen Werte für Geschwindigkeit und Duplex-Modus eingestellt werden, sonst geht der Port in den Zustand "Down".

Default: Aktiviert

- Speed / Duplex:

  Zeigt die Verbindungsgeschwindigkeit und den Duplex-Status des Ports. Für TP-Kabel werden die Geschwindigkeiten 10, 100 oder 1000 MBit/s unterstützt, Full- und Half-Duplex sind möglich. Für ein 1 GBit-Glasfaserkabel wird nur 1000 MBit/s unterstützt.

  Der Status der Geschwindigkeit und des Duplex-Modus hängt von den Einstellungen für die automatische Verhandlung und den Vorgaben des Benutzers ab.

  Default: Keiner. Hängt von den Ergebnissen der automatischen Aushandlung ab.

- Rx Pause:

  Das Verfahren beim Annehmen von PAUSE-Frames. Wenn diese Option aktiviert ist, beachtet der Port die PAUSE-Frames, anderenfalls ignoriert er sie.

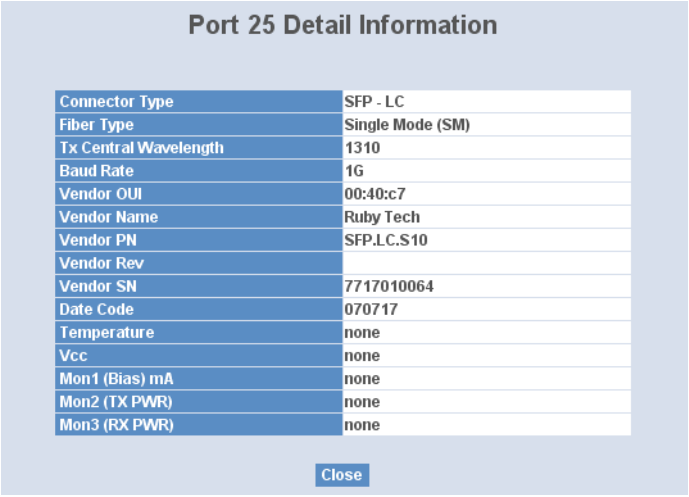
  Default: Keiner

- Tx Pause:

  Das Verfahren beim Versenden von PAUSE-Frames. Wenn diese Option aktiviert ist, versendet der Port die PAUSE-Frames, anderenfalls versendet er keine solchen Frames.

  Default: Keiner

DE



- **Detail-Information für SFP-Ports:**
  - Connector Type:

    Zeigt den Typ des verbundenen Kabels an, z.B. UTP, SC, ST oder LC.
  - Fiber Type:

    Gibt den Modus des optischen Kabels an, also z.B. Multi-Mode, Single-Mode.
  - Tx Central Wavelength:

    Gibt die zentrale Wellenlänge des Glasfaserkabels an, z.B. 850 nm, 1310 nm, 1550 nm etc.
  - Baud Rate:

    Zeigt die maximal unterstützte Baud-Rate des Glasfasermoduls an. Zum Beispiel 10M, 100M, 1G etc.
  - Vendor OUI:

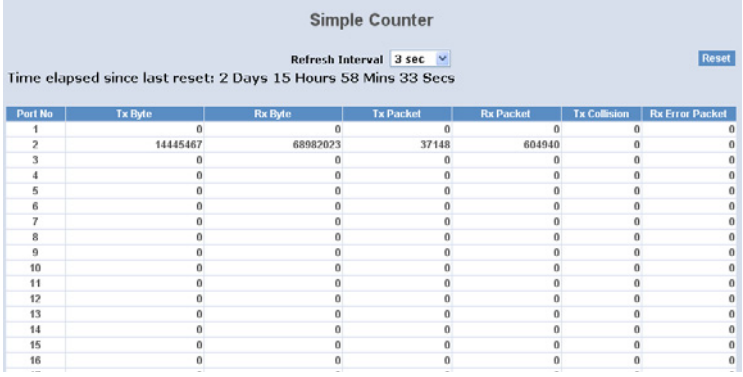
    Hier können Sie den Hersteller-OUI-Code ablesen, der von der IEEE verliehen wird.
  - Vendor Name:

    Hier können Sie den Hersteller-Namen des Modul-Herstellers ablesen.
  - Vendor P/N:

    Zeigt an, wie der Modul-Hersteller das Modul bezeichnet.

- Vendor Rev (Revision):
  Zeigt die Revisions-Nummer des Moduls.
- Vendor SN (Serial Number):
  Hier können Sie die Seriennummer des Moduls ablesen. Sie wird vom Modul-Hersteller festgelegt.
- Date Code:
  Zeigt das Herstellungs-Datum des Moduls.
- Temperature:
  Hier finden Sie die aktuelle Temperatur des Moduls.
- Vcc:
  Zeigt die Gleichstrom-Spannung an, die am Modul anliegt.
- Mon1(Bias) mA:
  Zeigt die Vorspannung des Moduls.
- Mon2(TX PWR):
  Zeigt den Übertragungsstrom des Moduls.
- Mon3(RX PWR):
  Zeigt die Empfangsleistung des Moduls.

4.3.3 Simple Counter



Port No	Tx Byte	Rx Byte	Tx Packet	Rx Packet	Tx Collision	Rx Error Packet
1	0	0	0	0	0	0
2	14445467	68982023	37148	604940	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0
11	0	0	0	0	0	0
12	0	0	0	0	0	0
13	0	0	0	0	0	0
14	0	0	0	0	0	0
15	0	0	0	0	0	0
16	0	0	0	0	0	0

Der einfache Zähler (Simple Counter) zeichnet alle Pakete, die die Ports durchlaufen auf, sowohl fehlerfreie als auch fehlerhafte.

In der Abbildung sehen Sie wie alle Zähler für einen Port gleichzeitig angezeigt werden können. Dabei kann jedes Datenfeld mit einem 20-Digit langen

DE

Datenstring gefüllt sein. Wenn der Zähler ein bestimmtes Maximum überschreitet, wird er wieder zurückgesetzt und beginnt das Zählen von Neuem. Sie können das Interval (zwischen 3 und 10 Sekunden) festlegen, indem die Daten aktualisiert werden. Default-Einstellung ist 3 Sekunden.

Simple Counter

Zeigt Ihnen eine Zusammenfassung des Datenverkehrs für einen Port an. Es werden die Zähler für Tx-Byte, Rx-Byte, Tx-Pakete, Rx-Pakete, Tx-Kollisionen und Rx-Fehler-Pakete dargestellt.

- Parameters:
  - Tx Byte:
    Insgesamt gesendete Bytes.
  - Rx Byte:
    Insgesamt empfangene Bytes.
  - Tx Packet:
    Die Anzahl der versandten Pakete.
  - Rx Packet:
    Die Anzahl der empfangenen Pakete.
  - Tx Collision:
    Anzahl der beim Senden festgestellten Datenpaket-Kollisionen.
  - Rx Error Packet:
    Anzahl der empfangenen fehlerhaften Pakete.

4.3.4 Detail Counter

Der Detail-Zähler (Detail Counter) zeichnet allen Datenverkehr für einen Port auf. Auch hier wird die gesamte Menge der Datenpakete angezeigt, unabhängig ob sie fehlerfrei waren oder nicht.

Wie Sie in der Abbildung sehen können, wird hier stets nur ein Port gleichzeitig angezeigt. Um den angezeigten Port zu wechseln, klicken Sie in der "Select"-Dropdown-Liste auf einen anderen Port.

Dabei kann jedes Datenfeld mit einem 20-Digit langen Datenstring gefüllt sein. Wenn der Zähler ein bestimmtes Maximum überschreitet, wird er wieder zurückgesetzt und beginnt von neuem das Zählen. Sie können das Interval (zwischen 3 und 10 Sekunden) festlegen, indem die Daten aktualisiert werden. Default-Einstellung ist 3 Sekunden.

Detail Counter

Zeigt Ihnen detailierte Zähler-Informationen für jeden Port an. Es kann stets nur ein Port gleichzeitig dargestellt werden.

- Parameter
  - Rx Packets:
    Die Anzahl der empfangenen Pakete.
  - Rx Octets:
    Insgesamt empfangene Bytes.
  - Rx Errors:
    Anzahl der empfangenen fehlerhaften Pakete.
  - Rx Unicast Packets:
    Die Anzahl der empfangenen Unicast-Pakete.
  - Rx Broadcast Packets:
    Zeigt Ihnen die Anzahl der empfangenen Broadcast-Pakete.
  - Rx Multicast Packets:
    Die Anzahl der empfangenen Multicast-Pakete.
  - Rx Pause Packets:
    Gibt Ihnen die Anzahl der empfangenen "PAUSE"-Pakete an.
  - Tx Collisions:
    Anzahl der beim Senden festgestellten Datenpaket-Kollisionen.
  - Tx Single Collision: Anzahl der gesendeten Pakete, die genau eine Kollision hatten.

DE

- Tx Multiple Collision:
  Anzahl der gesendeten Pakete, die mehr als eine Kollision hatten.
- Tx Drop Packets:
  Anzahl der wegen zu vieler Kollisionen, späten Kollisionen oder wegen des Alters des Pakets verworfenden Pakete.
- Tx Deferred Transmit:
  Anzahl der wegen Überlastung des Mediums beim Senden verzögerten Pakete.
- Tx Late Collision:
  Anzahl der späten Kollisionen. Dabei ist eine Kollision nach der ersten 512-Bit-Anzahl des Sendens aufgetreten.
- Tx Excessive Collision:
  Anzahl der Pakete/Frames, die nicht gesendet wurden, weil bereits 16 Versuche des Sendens gescheitert sind.
- Packets 64 Octets:
  Anzahl der empfangenen 64-Byte Frames/Pakete.
- Packets 65-127 Octets:
  Anzahl der empfangenen 65- bis 127-Byte Frames/Pakete.
- Packets 128-255 Octets:
  Anzahl der empfangenen 128- bis 255-ByteFrames.
- Packets 256-511 Octets:
  Anzahl der 256- bis 511-Byte-Frames, die empfangen wurden.
- Packets 512-1023 Octets:
  Anzahl der empfangenen 512- bis 1023-Byte-Frames.
- Packets 1024- 1522 Octets:
  Anzahl der empfangenen 1024- bis 1522-Byte-Frames.
- Tx Packets:
  Insgesamt versandte Pakete.
- TX Octets: Insgesamt versandte Datenmenge in Bytes.
- Tx Unicast Packets:
  Die Anzahl der versandten Unicast-Pakete.
- Tx Broadcast Packets:
  Gibt Ihnen die Anzahl der versandten Broadcast-Pakete an.

- Tx Multicast Packets:
  Die Anzahl der versandten Multicast-Pakete.
- Tx Pause Packets:
  Hier sehen Sie, wieviele "PAUSE"-Pakete von diesem Port gesendet wurden.
- Rx FCS Errors:
  Anzahl der fehlerhaften FSC-Pakete.
- Rx Alignment Errors:
  Anzahl der Pakete mit einem Alignment-Fehler.
- Rx Fragments:
  Anzahl der kurzen Frames (unter 64 Bytes) mit einem ungültigen CRC (Cyclic Redundancy Check).
- Rx Jabbers:
  Anzahl der langen Frames (wie im tomax_length Register angegeben) mit einem gescheiterten CRC.
- Rx Drop Packets:
  Wegen Fehlen eines ausreichenden Empfangs-Buffers verworfende Frames.
- Rx Undersize Packets:
  Anzahl der kurzen Frames (unter 64 Bytes) mit bestandenen CRC.
- Rx Oversize Packets:
  Anzahl der großen Frames (nach dem Wert im max_length Register) mit gültigen CRC.

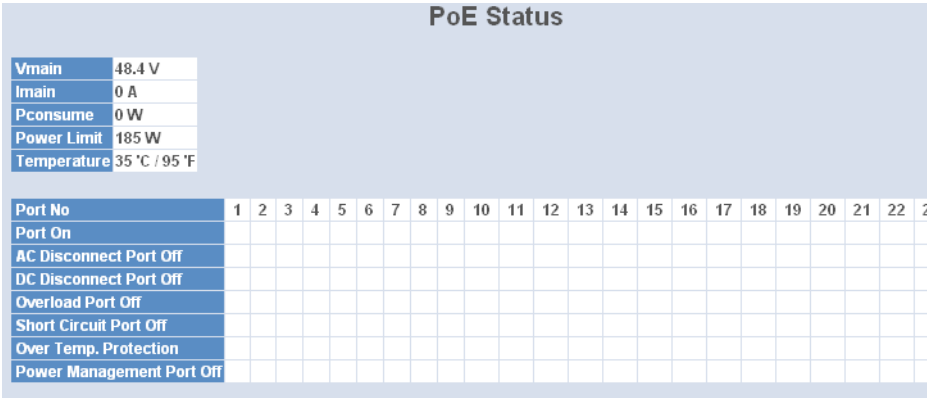
4.4 PoE (Power over Ethernet)

Nur für LANCOM ES-2126P

PoE Status

Zeigt Informationen über den PoE-Status an.

DE



- Parameter
  - Vmain:
    Die Spannung in Volt wird vom PoE vorgegeben.
  - Imain:
    Die Summe aller Ströme, die die Ports liefern.
  - Pconsume:
    Die Summe der von allen Ports verbrauchten Leistung.
  - Power Limit:
    Die maximale Leistung, die ein Switch liefern kann (Read Only).
  - Temperature:
    Die Temperatur des Chips bei eingeschaltetem PoE.
  - Port No:
    Port Nummer.
  - Port On:
    Zeigt an, ob der Port dem PD (Powered Device) Leistung zur Verfügung stellt, oder nicht.
  - AC Disconnect Port Off:
    Der Port ist wegen der "AC Disconnect function" abgeschaltet.
  - DC Disconnect Port Off:
    Der Port ist wegen der "DC Disconnect function" abgeschaltet.

- Overload Port Off:

  Der Switch wird einen Port nicht mehr mit Leistung versorgen, wenn das damit verbundene PD mehr Leistung verlangt als seine Klassen-einstellung zulässt.

- Short Circuit Port Off:

  Der Switch wird einen Port nicht mehr mit Leistung versorgen, wenn das damit verbundene PD kurzgeschlossen ist.

- Over Temp. Protection:

  Der Port des Switches wird abgeschaltet, sollte die Temperatur schnell auf 240°C oder langsam auf 200°C ansteigen.

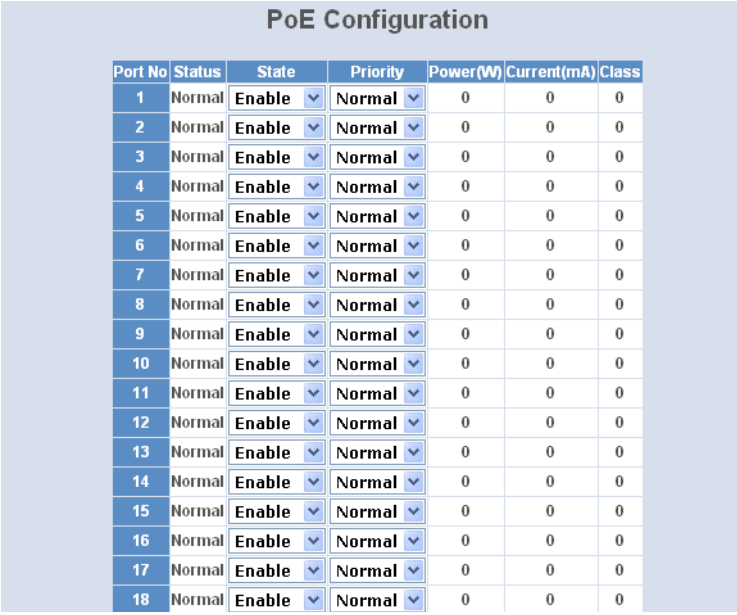
- Power Management Port Off:

  Falls die von allen Ports angeforderte Leistung das Leistungslimit des Switches übersteigt, wird er nach Priorität geordnet aufhören diesen Port mit Leistung zu versorgen.

PoE Configuration

In der "PoE Management function" können Sie die Einstellungen für PoE vornehmen.

Der Switch ist mit dem IEEE 802.3af Protokoll kompatibel und in der Lage automatisch zu erkennen, ob es sich bei einem angeschlossenem Gerät um ein PD (Powered Device) handelt. Der Switch wird auch automatisch die Energieversorgung des Gerätes gemäß dessen Klasse sicherstellen, bzw. unterbrechen, wenn das PD mehr Leistung benötigt als seine Klasse definiert, es kurzgeschlossen ist oder eine Überhitzung auftritt.



PoE Configuration

Port No	Status	State	Priority	Power(W)	Current(mA)	Class
1	Normal	Enable	Normal	0	0	0
2	Normal	Enable	Normal	0	0	0
3	Normal	Enable	Normal	0	0	0
4	Normal	Enable	Normal	0	0	0
5	Normal	Enable	Normal	0	0	0
6	Normal	Enable	Normal	0	0	0
7	Normal	Enable	Normal	0	0	0
8	Normal	Enable	Normal	0	0	0
9	Normal	Enable	Normal	0	0	0
10	Normal	Enable	Normal	0	0	0
11	Normal	Enable	Normal	0	0	0
12	Normal	Enable	Normal	0	0	0
13	Normal	Enable	Normal	0	0	0
14	Normal	Enable	Normal	0	0	0
15	Normal	Enable	Normal	0	0	0
16	Normal	Enable	Normal	0	0	0
17	Normal	Enable	Normal	0	0	0
18	Normal	Enable	Normal	0	0	0

- Parameter
  - Status:

    Kann entweder "Normal" oder "Active" sein. Dabei bedeuet Ersteres das der Port bereit ist mit einem PD (Powered Device) verbunden zu werden bzw. es mit Leistung zu versorgen. "Active" bedeutet, dass der Port bereits verbunden ist und Leistung an ein Gerät liefert.
  - State:

    "Enable" beschreibt die Fähigkeit des Ports ein PD mit Leistung zu versorgen. "Disable" dagegen bedeutet, dass bei diesem Port die Fähigkeit abgeschaltet ist.
  - Priority:

    Sie können zwischen drei Optionen wählen: "Normal", "Low" und "High". "Normal" ist die Default-Einstellung. Sollte die insgesamt von den Ports verlangte Leistung die maximal vom Switch leistbare Leistung überschreiten, wird der Switch die Ports nach der hier angegebenen Priorität (Low|Normal|High) abschalten. Sollten alle Ports dieselbe Priorität haben, wird der Switch sie bei der höchsten Port Id beginnend abschalten (12|1).

- Power(W):
  Die vom Port verbrauchte Leistung.
- Current(mA):
  Die vom Port an das PD gelieferte Strommenge.
- Class:
  Die Klasse des PDs, das mit dem Port des Switches verbunden ist.

4.5 Loop Detection

Die Loop Detection wird benutzt um den Datenverkehr zu erfassen. Wenn der Switch Datenpaketen mit der selben MAC-Adresse, wie die des Ports empfängt (Looping-Detection-Datenpakete), zeigt die Loop-Detection diese Aktivität an. Der Port ist gesperrt, wenn er die Loop-Detection-Datenpakete empfangen hat. Wenn Sie den Port wieder entsperren wollen, müssen Sie den Looping-Pfad finden und ausschalten. Wählen Sie dann den gesperrten Port aus und klicken Sie auf "resume" um ihn wieder zu aktivieren.

- Loop Detection
  Zeigt an, ob die Loop-Detection aktiv ist.
- Parameter:
  - Port No:
    Zeigt die Portnummer an, diese liegt zwischen 1 - 24.
  - Detection Port - Enable:
    Wenn die Portnummer ausgewählt ist und die Loop-Detection eingeschaltet ist, kann der Port Loops erfassen. Wenn der Port Loops erfasst, wird er gesperrt. (Wenn keine Loops auftreten, bleibt der Port ungesperrt.)
  - Locked Port - Resume:
    Wenn die Portnummer ausgewählt ist, die Loop-Detection eingeschaltet ist und der Port Loops erfasst, wird er gesperrt. Wenn Resume gewählt wird, wird der gesperrte Port wieder entsperrt. (Wenn Resume nicht gewählt wird, bleibt der Port gesperrt.)

4.6 SNMP

Jedes Network-Management-System (NMS), dass das Simple-Network-Management-Protocol (SNMP) beherrscht, kann die mit SNMP-Agenten ausgerüsteten Geräte, unter der Vorraussetzung, dass auf den Geräten die

DE

Management-Information-Base (MIB) korrekt installiert ist, kontrollieren. Das SNMP ist ein Protokoll um den Informationstransfer zwischen SNMP-Manager und SNMP-Agent zu kontrollieren und vermittelt die Object-Identity (OID) der Management-Information-Base (MIB) in der Form einer SMI-Syntax (Structure Management Information). Auf dem Switch läuft ein SNMP-Agent um auf die Anfragen eines SNMP-Managers zu reagieren.

Grundsätzlich bleibt der Agent passiv bis auf das Senden der Trap-Information. Der SNMP-Agent lässt sich auf dem Switch ein- und ausschalten. Wenn Sie den Schalter SNMP auf "Enable" stellen, wird der SNMP-Agent gestartet. Alle unterstützten MIB-OIDs, inklusive RNOM-MIB, sind dann für einen SNMP-Manager verfügbar. Wenn der Schalter auf "Disable" gestellt ist, wird der SNMP-Agent deaktiviert und der bzw. die damit verbundene Community-Name, Trap-Host, IP-Adresse sowie alle MIB-Zähler in Zukunft ignoriert.

SNMP Configuration

Hier können Sie Einstellungen am SNMP, Community-Namen, Trap-Host and Public-Traps sowie an der SNMP-Drossel vornehmen. Ein SNMP-Manager muss sich durch Angeben beider Community-Namen authentifizieren, um Zugriff auf die MIB-Informationen auf dem Zielgerät zu erhalten. Also müssen beide Parteien den selben Community-Namen erhalten. Sobald die Einstellungen vorgenommen sind, klicken Sie auf <Apply> um sie zu aktivieren.

- Parameter:
  - SNMP:

    Hier können Sie SNMP ein- bzw. ausschalten. In der Default-Einstellung ist SNMP eingeschaltet ("Enable").

Bitte beachten Sie, dass der LANmonitor keine Informationen über den LANCOM Switch anzeigen kann, wenn die SNMP-Unterstützung ausgeschaltet ist.

  - Get/Set/Trap Community:

    Der Community-Name wird als Passwort genutzt um sicher zustellen, dass ein Network-Management-Unit derselben Community wie das Zielgerät angehört. Sollte es einen anderen Community-Namen haben, gehört es einer anderen Gruppe an, und kann deshalb nicht

auf das Zielgerät via SNMP zugreifen. Wenn beide den selben Community-Namen haben, können sie miteinander kommunizieren.

Den Community-Namen können Sie einstellen. Er darf maximal 15 beliebige Zeichen (aber ohne Leerzeichen) betragen und die Groß- und Kleinschreibung muss beachtet werden.

Den Community-Namen müssen Sie für jede Funktion einzeln festlegen. Er lässt sich nicht für mehrere Funktionen verwenden (d.h. der Community-Name für GET lässt sich nicht nochmal für SET vergeben).

Default SNMP function : Enable

Default community name for GET: public

Default community name for SET: private

Default community name for Trap: public

Default Set function : Disable

Default trap host IP address: 0.0.0.0

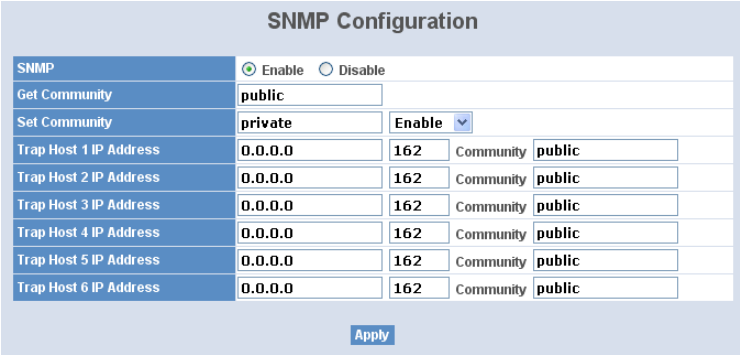
Default port number :162

- Trap:

  Der Switch unterstützt bis zu 6 Trap-Hosts. Sie können jedem davon eine eigene IP-Adresse und einen eigenen Community-Namen zuweisen. Um einen Trap-Host aufzusetzen, müssen Sie einen Trap-Manager erstellen, indem Sie eine IP-Adresse als Host einer Trap-Message zuweisen. Der Trap-Host ist eine Network-Management-Unit des SNMP-Managers, welche die Trap-Message eines SNMP-Agenten empfängt. 6 Trap-Hosts können den Verlust einer wichtigen Trap-Message effektiv verhindern.

  Für jede Public-Trap unterstützt der Switch die Trap-Events Cold Start, Warm Start, Link Down, Link Up und Authentication Failure Trap. Jedes dieser Events können Sie im Menü Alarm > Events individuell ein- und ausschalten. Wenn sie eingeschaltet sind, wird die jeweilige Trap aktiv eine Nachricht (Trap Message) an den Trap-Host schicken wenn sie auftritt. Sollten alle öffentlichen Traps ausgeschaltet sein, wird keine öffentliche Trap Message gesendet. Die Enterprise-Trap ist als Private-Trap klassifiziert, und ist daher im Kapitel über Trap Alarm Conifguration erklärt.

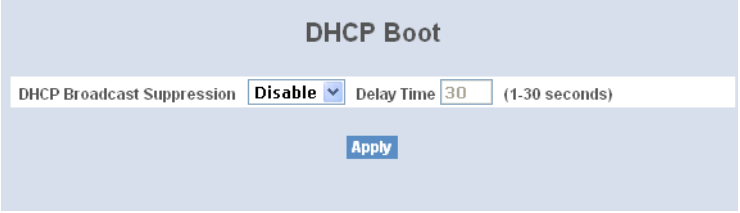
  Die Default Einstellung für alle Public-Traps ist “Enable”.



4.7 DHCP Boot

Die DHCP-Boot-Funktion (DHCP = Dynamic Host Configuration Protocol) dient dazu, die anfragendenen Broadcast-Pakete in einem größeren Zeitfenster zu verteilen, um einem Stau vorzubeugen. Dieser könnte zwischen mehreren Broadcast-Paketen von verschiedenen Netzwerkgeräten entstehen, die das NMS (NC-Management-System), den Boot-Server, den DHCP-Server oder eine der vielen anderen voreingestellten Verbindungen sucht, wenn das System nach dem herunterfahren neu bootet und sich wiederherstellt. Wenn das System neu bootet, suchen die Switches oder auch die anderen Netzwerkgeräte im LAN den Server und werden deswegen viele Broadcast-Pakete versenden.

Der Switch unterstützt eine willkürliche Delay Time (Verzögerungszeit) für DHCP und bootet jedes Gerät zeitverzögert. Dies vermeidet eine große Menge an Broadcast-Pakteten, die auftreten würden, wenn alle Geräte zur gleichen Zeit booten würde. Die Delay Time kann von Ihnen eingestellt werden und beträgt maximal 30 Sekunden. Wenn die DHCP-Broadcasting-Unterdrückung aktiv ist, wird die Delay Time in einem Bereich von 0 bis 30 Sekunden willkürlich eingestellt. Die exakte Delay Time berechnet der Switch. Default ist “disable”.



DE

4.8 IGMP Snooping

Die Funktion IGMP Snooping dient zur Organisation von Multicast-Gruppen. IGMP Snooping sendet die Multicast-Pakete zu den Ports der VLAN-Gruppe. Durch IP-Multicast-Pakete im Netzwerk wird die Bandbreite nicht unnötig belastet. Das liegt daran, dass ein Switch, der kein IGMP oder IGMP-Snooping unterstützt, Multicast- und Broadcast-Pakete nicht unterscheiden kann. Ohne IGMP Snooping unterscheidet sich das Senden von Multicast-Paketen daher nicht vom Senden von Broadcast-Paketen.

Ein Switch unterstützt IGMP Snooping mit den folgenden Funktionen: Anfragen, Anmelden und Verlassen. Ein Paket-Typ, der zwischen einem IP-Multicast-Router bzw. einem Switch und einem IP-Multicast-Host ausgetauscht wird, kann die Informationen des Multicast-Table updaten, wenn ein Mitglied (Port) zu einer IP-Multicast-Zieladresse hinzukommt oder sie verlässt. Wenn der Switch ein IP-Multicast-Paket bekommt, kann er es mit dieser Funktion an die Mitglieder senden, die vorher in eine bestimmte IP-Multicast-Gruppe eingetreten sind. IGMP Snooping verwirft die Pakete, wenn der Benutzer Multicast-Pakete zu einer Multicast-Gruppe schickt, die nicht im Vorfeld erstellt wurde.

4.8.1 IGMP Snooping Status

IGMP wird dazu benutzt den Status der IP-Multicast-Gruppe herauszufinden und die damit verbundenen Informationen im getaggten und ungetaggten VLAN Netzwerk anzuzeigen. Mit IGMP, entweder im passiven oder im aktiven Modus, können Sie die IGMP-Snooping-Information kontrollieren, diese enthält die Multicast-Mitgliederliste, VID und die Mitglieder-Ports.

DE

- Parameter
  - IGMP snooping mode selection:

    Der Switch unterstützt drei Zustände von IGMP Snooping "passive", "active" und "disable".

    Disable: Setzen Sie die Funktion auf "disable", wenn Sie die IGMP Snooping- Funktion ausschalten möchten. Default ist "disable".

    Active: Im Modus "active" sendet der Switch regelmäßig eine Anfrage bezüglich der Mitgliedschaft an alle angeschlossenen Hosts und erfasst die Antworten über die Mitgliedschaft, um die Database des Multicast-Table upzudaten. (Anmerkung: Dies reduziert unnötigen Multicast-Traffic.)

    Passive: Im Modus "passive" befragt IGMP Snooping nicht regelmäßig die Hosts der Gruppe über ihre Mitgliedschaft, sondern nur, wenn diesbezüglich eine Anfrage vom Router kommt.
  - IP Address:

    Gibt alle IP-Adressen von Multicast-Gruppen an, die in diesem Gerät registriert sind.
  - VLAN ID:

    Gibt die VLAN-ID für jede Multicast-Gruppe an.
  - Member Port:

    Gibt die Mitglieder-Ports an (einen oder mehrere), die in jeder Multicast-Gruppe sind.

4.8.2 Allowed Group

Mit der Allowed-Group-Funktion richtet IGMP Snooping, nach den von Ihnen angegebenen Bedingungen, die IP-Multicast-Tabelle ein. IGMP meldet Pakete an, die die von Ihnen eingestellten Items enthalten und fügt sie einer Multicast-Gruppe hinzu bzw. erstellt eine neue Multicast-Gruppe.

- Parameter
  - IP Range:

    Der Switch bietet zwei Möglichkeiten an, um den gültigen IP-Range einzustellen "any " und "custom". Default ist "any". Wenn Sie "custom" wählen, können Sie einen IP-Bereich vergeben. Der gültige Bereich liegt zwischen 224.0.0.0~239.255.255.255.

  - VID:

    Der Switch bietet zwei Möglichkeiten an, um gültiges VLAN VID einzustellen "any" und "custom". Default ist "any". Wenn Sie "custom" wählen, können Sie eine VID Nummer eingeben, der gültige Bereich liegt zwischen 1~4094.

  - Port:

    Der Switch bietet zwei Möglichkeiten an, um den gültigen Port-Bereich einzustellen "any" und "custom". Default ist "any". Wenn Sie "custom" wählen, können Sie die arbeitenden Ports in der Allowed-Group Configuration (erlaubte Gruppen-Konfiguration) beschränken bzw. auswählen.

  - Add:

    Eine neue Eingabe bezüglich einer erlaubten Gruppen-Konfiguration können Sie erstellen, nachdem Sie die oben genannten Parameter eingegeben haben und anschließend <add> wählen.

  - Edit:

    Die bestehende Eingabe kann verändert werden, nachdem Sie <edit> ausgewählt haben.

- Delete:

  Entfernt die bestehende Eingabe der erlaubten Gruppen-Konfiguration der erlaubten Gruppe.

4.9 VLAN

Der Switch unterstützt sowohl Tag-basierte VLAN (802.1g) als auch Port-basierte VLAN. Es können bis zu 256 aktive VLANs mit den VLAN-IDs (Identitäten) 1 bis 4094 erstellt werden. Mit den VLAN-Einstellungen können Sie Ihr Netzwerk in kleinere, leichter überschaubare Teil-Netzwerke einteilen. Sie können durch eine optimale Einstellung neben einem Gewinn an Perfomance- und Sicherheit auch die Notwendigkeit des Netzwerk-Managements reduzieren.

4.9.1 VLAN Mode

VLAN Mode Setting

Hier können Sie zwischen dem Port- und Tag-basierten VLAN-Modus entscheiden. Ihre Änderungen werden nach dem Betätigen des <Apply>-Buttons sofort übernommen und angewandt.

- Parameter
  - VLAN Mode:

    Tag-based:

    Dies ist die Default-Einstellung.

    Ein Tag-basiertes VLAN identifiziert seine Mitglieder an deren VID. Sollten zusätzlich noch ein- und ausgehende Filter-Listen angelegt worden sein, werden diese Filter auch zusätzlich angewendet um festzustellen, ob ein Paket weitergeleitet wird. Der Switch unterstützt den 802.1q-Standard.

    Jedes von Ihnen erstellte Tag-basierte VLAN muss einen VLAN-Namen und eine VLAN-ID zugewiesen bekommen. Die ID muss zwischen 1 und 4094 liegen. Sie können insgesamt 256 VLAN-Gruppen erstellen.

    Port-based:

    Port-basiertes VLAN legt die Mitglieder über den Port fest. Alle Pakete von oder zu einem Mitglieder-Port werden akzeptiert. Bestehende Filterregeln werden nicht angewandt. Einziges Krite-

rium für die Weiterleitung eines Pakets ist die physikalische Verbindung zu einem der Mitglieder-Ports. So kann in ein port-basiertes VLAN aus den Ports 1,2,3 und 4 nur einer dieser Ports mit den anderen Mitglieder-Ports kommunizieren. Der Port 5 etwa wäre von der Interaktion ausgeschlossen. Jedes port-basierte VLAN muss von Ihnen mit einem Namen versehen werden. Dieser Switch unterstützt maximal 26 Port-basierte VLANs.

- Symmetric Vlan:

  Dies ist ein Filter für eingehende Daten (1. Zugangs-Regel: "Es werden nur Pakete weitergeleitet, deren VIDs zum VID des jeweiligen Ports passen"). Sollte also zum Beispiel der Port 1 ein getaggtes Paket mit VID=100 empfangen, wird der Switch überprüfen, ob Port 1 zum VLAN 100 gehört. Sollte das nicht der Fall sein, wird das Paket verworfen.

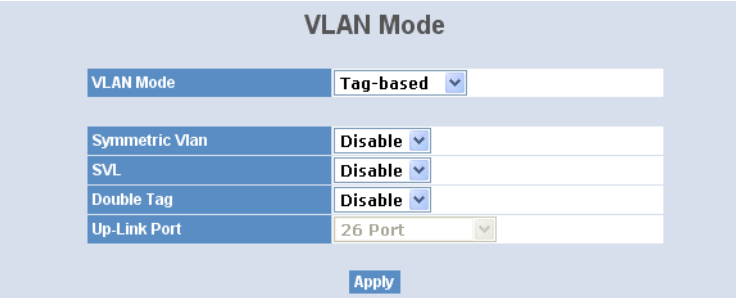
Wenn symmetrisches VLAN aktiviert ist und zum Beispiel Port 1 ein nicht-getaggtes Paket empfängt, wird der Switch die PVID des Ports als Tag vergeben und es weiterleiten. Sollte die PVID des Ports 1 allerdings nicht 100 sein, wird das Paket verworfen.

- SVL (Shared VLAN Learning):

  Alle VLANs werden dieselbe Filter-Datenbank verwenden um die Mitgliedschaft zu einem VLAN bekanntzugeben und nachzuschlagen, wenn Sie hier SVL aktivieren. Wenn SVL nicht aktiv ist, wird jedes VLAN seine eigene Datenbank benutzen um die Mitgliedschaft zu einem VLAN zu speichern oder nachzusehen. Diese Methode nennt man IVL (Independent VLAN Learning).

- Double Tag:

  Der Doppel-Tag-Modus wird nur bei Tag-basierten VLAN benutzt. In diesem Modus werden alle Pakete zunächst als nicht-getagged behandelt. Deswegen werden allen Paketen die jeweilige PVID als neues Tag hinzugefügt. Diese Pakete werden dann als Tag-basiertes VLAN weitergeleitet. Sollte ein Paket bereits ein Tag haben, wird hierdurch "doppelt-getaggt".



4.9.2 Tag-based Group

Tag-based Group Configuration

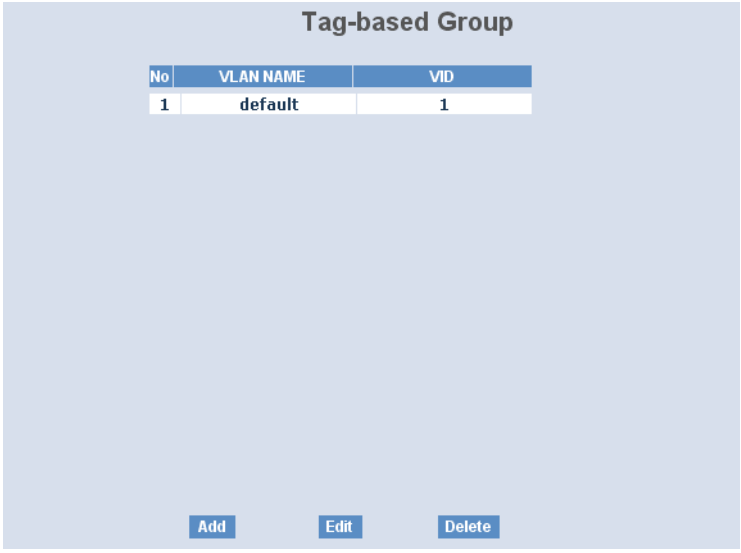
Hier finden Sie Informationen zu bereits bestehenden Tag-basierten VLANs. An dieser Stelle können Sie auch Tag-basierte VLAn komfortabel erstellen, bearbeiten oder löschen.

- Parameter:
  - VLAN Name:

    Sie können dem VLAN hier einen Namen zuweisen. Beachten Sie dabei, dass der Name nur aus den Buchstaben A-Z (Klein- und Großbuchstaben) den Ziffern 0-9, sowie den Trennzeichen "-" und "_". Der Name darf maximal 15 Zeichen lang sein.
  - VID:

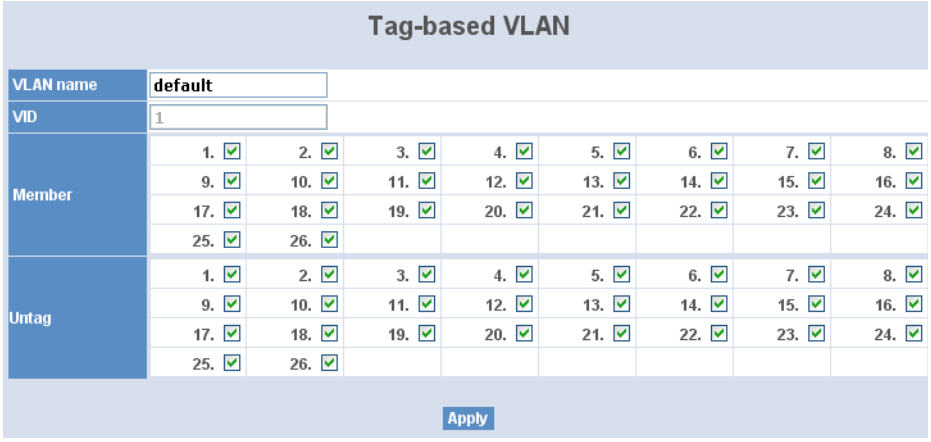
    Die sogenannte VLAN-ID(Identität). Jedes Tag-basierte VLAN hat eine einzigartige VID. Diese Option erscheint nur im Tag- oder Doppel-Tag-basierten Modus.
  - Member:

    Hier können Sie die Mitglieder eines neu geschaffenen VLANs festlegen. Dabei beschreibt "Enable", dass ein Port Mitglied des entsprechenden VLANs ist. Durch das Abhaken der Checkbox neben einem Port setzen Sie den Wert für diesen Port auf "Enable" und machen ihn zu einem Mitglied des VLANs.



- Add Group:

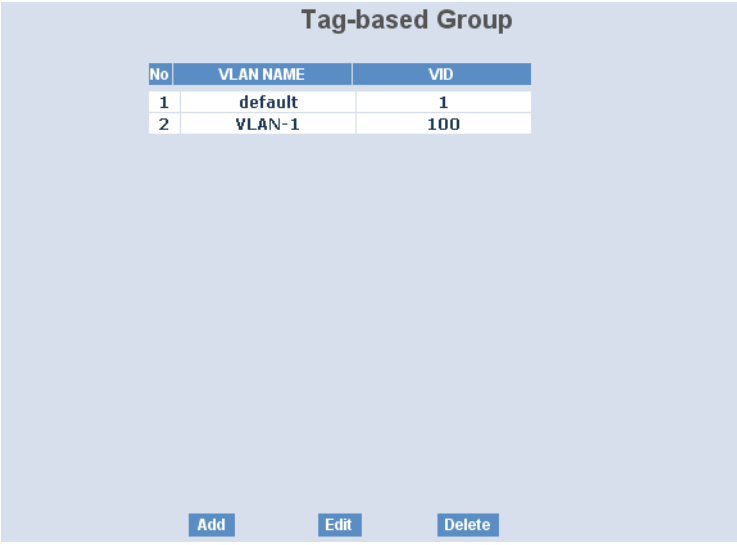
  Geben Sie dem neuen Tag-basierten VLAN einen Namen und eine VID und wählen Sie dann durch Abhaken der Checkboxen neben den Ports die Mitglieder. Der "Untag"-Parameter beschreibt eine Regel für abgehende Pakete. Wenn Sie diesen Parameter für einen Port setzen, werden aus den Paketen, die von diesem Port ausgehen, die Tags entfernt.



DE

- Delete Group:

  Durch das Klicken des <Delete>-Buttons können Sie das ausgewählte Tag-basierte VLAN löschen.



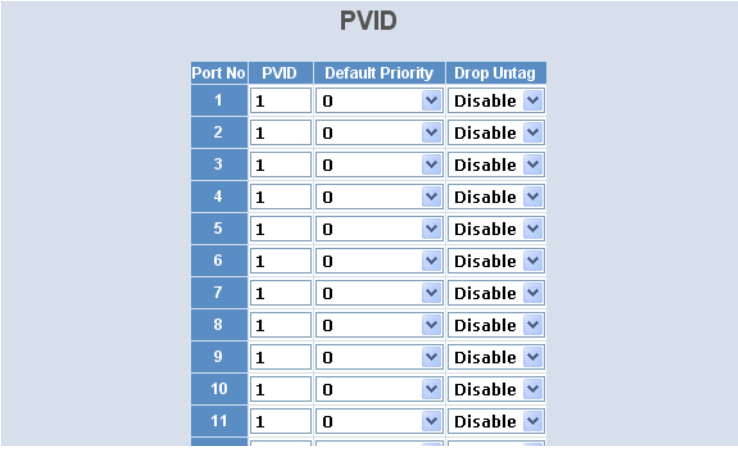
- Edit a group:

  Wenn Sie eine VLAN-Gruppe ausgewählt haben, können Sie durch das Klicken des <Edit>-Buttons Einstellungen an der Gruppe wie etwa die Gruppen-Beschreibung oder ihre Mitglieder vornehmen.

4.9.3 PVID

- PVID

  Weisen Sie hier jedem Port eine VID zwischen 1 und 4094 zu. Sie können hier auch einen Filter für eingehende Daten (2. Zugangsregel: "Alle nicht-getaggten Pakete werden verworfen.") aktivieren. Wenn dieser Filter aktiv ist, werden alle nicht-getaggten Pakete, die dieser Port empfängt verworfen.



PVID

Port No	PVID	Default Priority	Drop Untag
1	1	0	Disable
2	1	0	Disable
3	1	0	Disable
4	1	0	Disable
5	1	0	Disable
6	1	0	Disable
7	1	0	Disable
8	1	0	Disable
9	1	0	Disable
10	1	0	Disable
11	1	0	Disable

- Parameter:
  - Port 1-26:

    Port Nummer.
  - PVID:

    Die PVID muss zwischen 1 und 4094 liegen. Bevor Sie einem Port die PVID x zuweisen können müssen sie ein Tag-basiertes VLAN mit einer VID x erstellen. Sollte also etwa ein Port x ein nicht-getaggtes Paket erhalten, wird der Switch diesem Paket die Port VLAN ID (PVID, also z. B. VID y) vom Port x als Tag verleihen. Das Paket wird dann weitergeleitet als Paket mit der VID y.
  - Default Priority:

    Diese Einstellung basiert auf 802.1p QoS (Quality of Service) und betrifft nicht-getaggte Pakete. Wenn ein Paket den Switch erreicht wird ihm an Hand dieser und der 802.1p-QoS-Einstellung eine Prioritäts-Reihenfolge zugewiesen. Sollten Sie also zum Beispiel die Default-Priorität von Port 2 auf 2 setzen und dann nicht-getaggte Pakete an Port 2 senden, werden diese Pakete wegen des 802.1p-Prioritäts-Mapping eine Prioritäts-Reihenfolge von 2 haben und in Queue 1 verschoben.
  - Drop Untag:

    Sie können einen Port anweisen alle Pakete zu akzeptieren, oder nur Pakete mit einem entsprechenden VLAN-Tag. Sollten sie Letzeres einstellen, werden Pakete ohne VLAN-Tag verworfen.

DE

4.9.4 Port-based Group

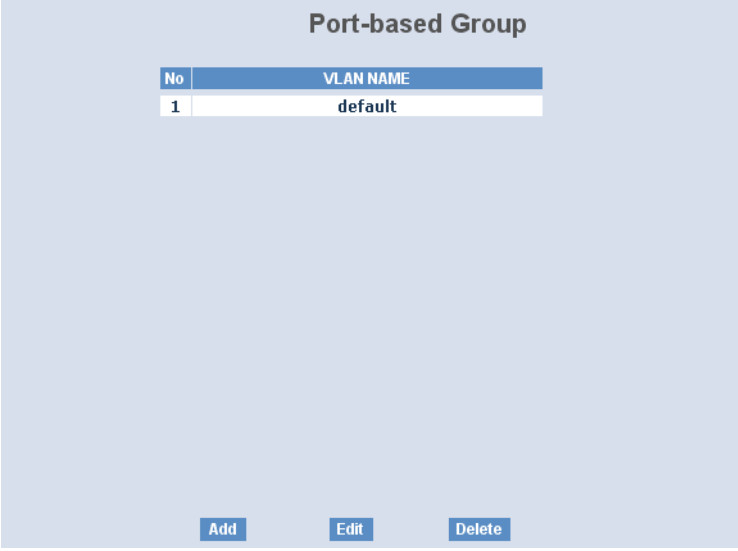
Port-based Group Configuration

Hier finden Sie Informationen zu den bereits bestehenden Port-basierten VLANs sowie die Möglichkeit komfortabel neue VLANs zu erstellen und bestehende zu bearbeiten oder zu löschen.

- Parameter
  - VLAN Name:

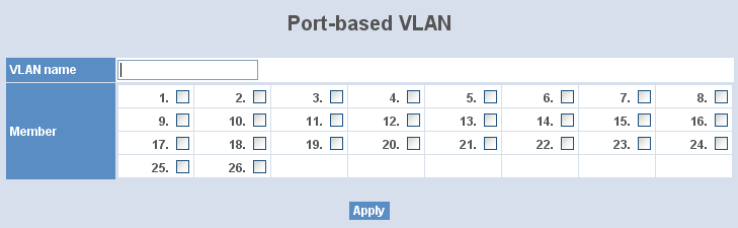
    Hier können Sie dem VLAN einen Namen zuweisen. Beachten Sie dabei, dass der Name nur aus den Buchstaben A-Z (Klein- und Großbuchstaben) den Ziffern 0-9, sowie den Trennzeichen "-" und "_". Der Name darf maximal 15 Zeichen lang sein.
  - Member Port:

    Hier können Sie die Mitglieder eines neu geschaffenen VLANs festlegen. "Enable" beschreibt, dass ein Port Mitglied des entsprechenden VLANs ist. Durch das Abhaken der Checkbox nebem einem Port setzen Sie den Wert für diesen Port auf "Enable" und machen ihn zu einem Mitglied des VLANs.



- Add Group:

  Geben Sie dem neuen Port-basierten VLAN einen Namen und eine VID und wählen Sie dann durch Anhaken der Checkboxen neben den Ports die Mitglieder.



- Delete Group:

  Klicken Sie auf die Schaltfläche <Delete>, um den gewählten Eintrag aus der Liste zu entfernen.

- Edit a group:

  Wählen Sie einen Eintrag aus und wählen Sie die Schaltfläche <Edit>, um die Beschreibung der Gruppe und die Mitglieder zu bearbeiten.

DE

4.10 MAC Table

Die MAC-Tabellen-Konfiguration beinhaltet viele Funktionen, z. B. die MAC-Tabellen-Information, MAC-Tabellen-Wartung, Static und MAC-Alias, die nicht zu einem bestimmten Funktionstypen zugeordnet werden können. Alle Funktionen werden im Folgenden beschrieben.

- MAC Table Information

  Zeigt den statischen oder dynamischen MAC-Lerneintrag und den Status des ausgewählten Ports.

- Parameter:
  - Port:

    Wählt den Port aus, bei dem Sie anfragen wollen.
  - Search:

    Erstellt den MAC-Eintrag, bei dem Sie anfragen wollen. Default ist ??-??-??-??-??-??.
  - MAC:

    Zeigt die MAC-Adresse eines Eintrags, den Sie aus der MAC-Tabelle ausgewählt haben.
  - Alias:

    Stellt den Alias für den gewählten MAC-Eintrag ein.
  - Set Alias:

    Speichert den Alias für den MAC-Eintrag, den Sie erstellt haben.
  - Search:

    Findet den Eintrag für Ihre Einstellungen.
  - Previous Page:

    Sie gelangen auf die vorherige Seite.
  - Next Page:

    Sie gelangen auf die nächste Seite.
  - Alias:

    Der Alias des gesuchten Eintrags.
  - MAC Address:

    Die MAC-Adresse des gesuchten Eintrags.
  - Port:

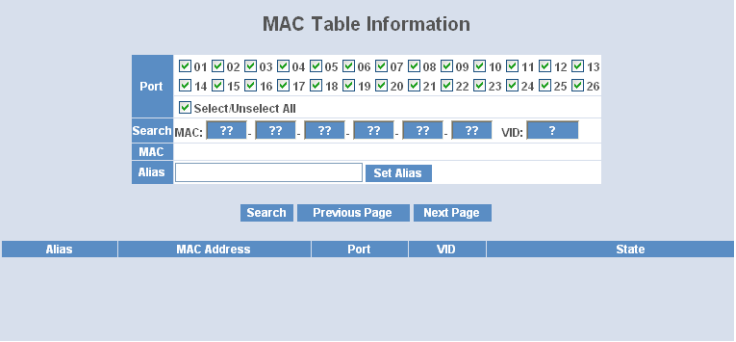
    Der Port des gesuchten MAC-Eintrags.

- VID:

  VLAN Gruppe, damit ein MAC-Eintrag besteht.

- State:

  Zeigt das Verfahren des MAC-Eintrags “dynamic MAC” oder “static MAC”.



MAC Table Maintenance

Diese Funktion ermöglicht Ihnen das Verhalten der MAC-Tabelle einzustellen. Eine inaktive MAC-Adresse, welche die Age-out-Time der MAC-Adresse übersteigt, wird aus der MAC-Tabelle gelöscht. Der Bereich der Age-out-Time liegt zwischen 10 - 1.000.000 Sekunden. Diese Einstellung hat keine Auswirkungen auf die statische MAC-Adresse.

Zusätzlich kann das Lernlimit der MAC-Maintenance die Anzahl der MACs begrenzen, die jeder Port lernen kann.

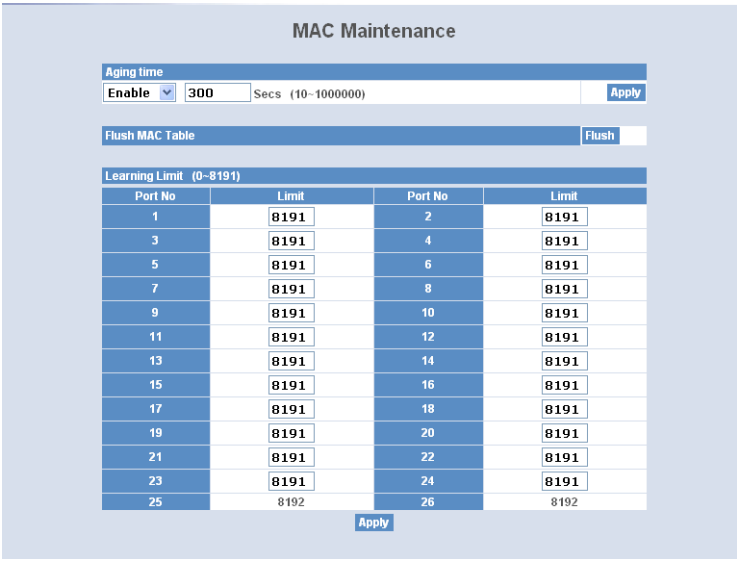
Parameter:

- Aging Time:

  Löscht eine für diese Zeit inaktive MAC-Adresse aus der MAC-Tabelle. Dies hat keine Auswirkungen auf die statische MAC-Adresse. Der Bereich der Aging-Time der MAC-Adresse liegt zwischen 10 - 1000000 Sekunden. Default Aging-Time beträgt 300 Sekunden.

- Learning Limit:

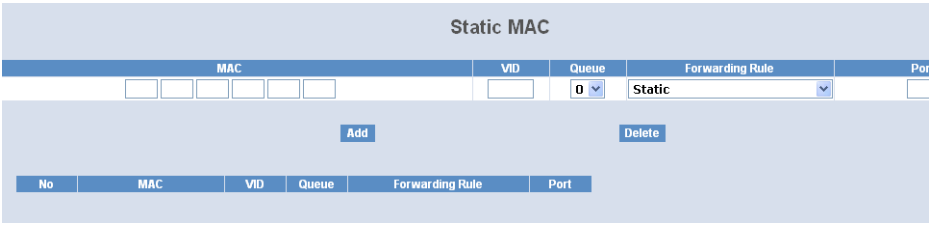
  Stellt die maximale Anzahl von MACs ein, die jeder Port lernen kann. Der gültige Wert für das Lernlimit der Ports 1-24 liegt zwischen 0 - 8.191. Für Port 25 und Port 26 gilt der festgelegte Wert 8.192, dieser kann nicht von Ihnen verändert werden.



- Static Setting

  Die Funktion Static wird dazu benutzt, die Einstellungen des MACs im Inneren des Switches zu konfigurieren. Es gibt drei Einstellungstypen: “static”, “static with destination drop” und “static with source drop”, die im Folgenden erklärt werden.

  - Wenn Sie “static” wählen, können Sie eine MAC-Adresse für einen bestimmten Port bestimmen. Die gesamten Daten des Switches, die an diese MAC-Adresse gesendet werden, werden an diesen Port weitergeleitet.
  - Wenn Sie “static with destination drop” wählen, wird das Paket verworfen, wenn seine Ziel-Adresse (Destination Address) mit dem eingestellten Wert übereinstimmt. Da dies eine allgemeine Einstellung ist, betrifft sie den Datentransport von allen Ports.
  - Wenn Sie “static with source drop” wählen, verfällt das Paket, wenn seine Quell-Adresse (Source Address) mit dem eingestellten Wert übereinstimmt. Da dies eine allgemeine Einstellung ist, betrifft sie den Datentransport von allen Ports.



- Parameter:
  - MAC:

    MAC ist eine sechs Byte lange Hardware-Adresse, die gewöhnlich hexadezimal geschrieben und mit Bindestrichen getrennt wird, z. B. 00 – 40 - C7 - D6 – 00 - 01 .
  - VID:

    VLAN Identifier. Dieser wird nur in Anspruch genommen, wenn tagged VLAN benutzt wird. Der gültige Bereich ist 1 - 4094.
  - Queue (Priority):

    Stellt die Priorität (0 - 3) für den MAC ein.
  - Forwarding Rule (Drop Policy):

    Static: Eine MAC-Adresse wird einem bestimmten Port zugeteilt und die gesamten Daten des Switches, die zu dieser MAC-Adresse gesendet werden, werden an diesen Port weitergeleitet.

    Static with destination drop: Das Paket wird verworfen, wenn seine Ziel-Adresse mit dem Wert übereinstimmt, den Sie eingestellt haben.

    Static with source drop: Das Paket wird verworfen, wenn seine Quell-Adresse mit dem Wert übereinstimmt, den Sie eingestellt haben.
  - Port:

    Hier können Sie den Port (1-26) auswählen, den Sie im Switch einstellen wollen.

- MAC Alias

  Mit der MAC-Alias-Funktion können Sie der MAC-Adresse einen Namen zuteilen. Damit können Sie z. B. einen unerlaubten Vorgang einer MAC-Adresse einem Benutzer zuzuordnen. Am Anfang werden alle Paare bestehender Alias-Namen und MAC-Adressen angezeigt.

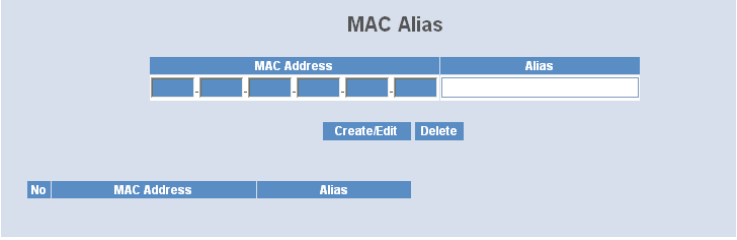
  Es gibt drei MAC-Alias-Funktionen in dieser Funktion, MAC Alias Add, MAC Alias Edit und MAC Alias Delete. Klicken Sie auf die Schaltfläche

<Create/Edit> um einen neuen Alias-Namen zu einer bestimmten MAC-Adresse hinzuzufügen, einen bestehenden Eintrag zu verändern oder um ihn zu löschen. Sie können einen Alias-Namen mit den Buchstaben A-Z, a-z und den Zahlen 0-9 mit einer maximalen Länge von 15 Stellen erstellen.

- MAC Alias Create/Edit or Delete

  In der MAC-Alias-Funktion dient die Add-Edit-Funktion dazu, dass Sie eine Verbindung zwischen einer MAC-Adresse und einem Namen herstellen können. Klicken Sie auf den <Create/Edit> Button, um einen neuen Eintrag zu erstellen.

  Mit der MAC-Alias-Löschfunktion können Sie eine bestehende MAC-Adresse oder einen Alias-Namen auswählen und löschen.



- Parameter:
  - MAC Address:

    Die MAC-Adresse ist eine sechs Byte lange Hardware-Adresse, gewöhnlich hexadezimal geschrieben und mit Bindestrichen getrennt, z. B. 00 – 40 - C7 - D6 – 00 - 02
  - Alias:

    Der von Ihnen erstellte MAC-Alias-Name.

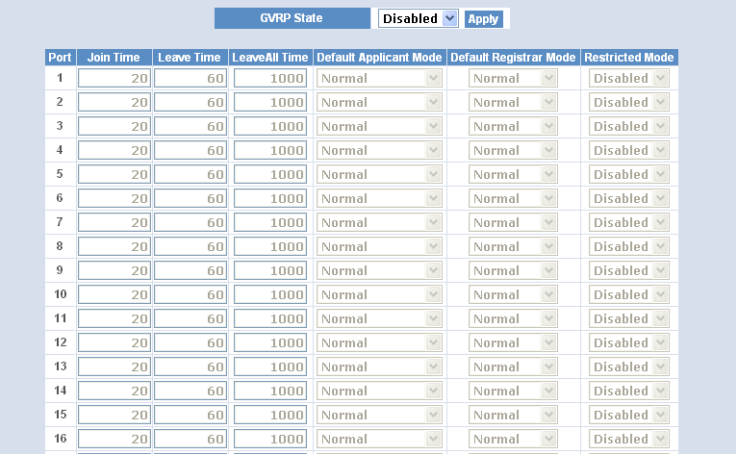
    Hinweis: Wenn die MAC-Tabelle zu viele MAC-Adressen aufgenommen hat, empfehlen wir Ihnen die MAC-Adresse und den Alias-Namen direkt einzugeben.

4.11 GVRP

GVRP (Generic VLAN Registration Protocol) ist eine auf dem Generic-Attribute-Registration-Protocol (GARP) basierende Anwendung, die hauptsächlich dafür benutzt wird, die Gruppenmitgliedschaft der VLANs automatisch und dynamisch zu warten. Die GVRP bringt die Möglichkeit mit, den VLAN-Registrationsservice durch eine GARP-Anwendung auszuführen. Dabei greift

sie auf die GARP-Information-Declaration (GID) zurück um die mit der Attribute-Datenbank verknüpften Ports zu erhalten, sowie auf die GARP-Information-Propagation (GIP) um mit Switches und Endstationen zu kommunizieren. Mit GID und GIP erhalten Maschinen im GVRP-Zustand die Inhalte der Dynamic-VLAN-Registration für jedes VLAN und verbreiten diese Informationen zu anderen GVRP-fähigen Geräten. Dadurch werden deren Wissensdatenbanken, sowie die Sets der mit gerade aktiven Mitgliedern verknüpften VLANs und die jeweiligen Ports, durch die diese Mitglieder zu erreichen sind, aufgesetzt und aktuell gehalten.

In den GVRP Einstellungen sind drei Funktionen unterstützt, die im Folgenden erklärt werden: GRVP-Config, GRVP-Counter und GVRP-Group.



4.11.1 Config

GVRP Config

Die GVRP-Konfiguration wird benutzt um den GVRP-Operationsmodus jedes Portes einzustellen. Hierfür müssen Sie sieben Parameter einstellen, die im Folgenden beschrieben werden.

- Parameter:
  - GVRP State Setting:

    Hier können Sie den GVRP-Zustand auf einfache Art und Weise ein- bzw. ausschalten. Sie können die Liste mit der Maus oder mit dem "Nach-Unten-Pfeil" nach unten scrollen um dann zwischen "Enable" oder "Disable" entscheiden. Danach können Sie mit dem "Apply"-Button die Änderung übernehmen, die dann sofort aktiv wird.

- Join Time:

  Hier können Sie die Join-Time in Hundertstelsekunden festlegen. Möglicher Einstellungsrahmen: 20-100 Hundertstelsekunden, Default 20 Hundertstelsekunden.

- Leave Time:

  Die Leave-Time lässt sich im Rahmen von 60-300 Hundertstelsekunden einstellen. Die Default-Einstellung ist auf 60 Hundertstelsekunden eingestellt.

- Leave All Time:

  Nach einer Zeitspanne wird angekündigt, dass alle Geräte die angemeldet sind, abgemeldet werden. Falls dennoch ein Gerät neu angemeldet wird, wird die Anmeldung im Switch gespeichert. Lässt sich im Bereich von 1.000-5.000 Zeiteinheiten einstellen, die Default-Einstellung ist auf 1.000 Zeiteinheiten festgelegt.

- Default Applicant Mode:

  Dieser Modus beschreibt den Typus des Teilnehmers. Sie können zwischen zwei Modi wählen: Normal und Non-Participant.

  Normal:

  In diesem Modus nimmt der Switch in vollen Umfang am GARP-Protokoll-Austausch teil. Dies ist die Default-Einstellung.

  Non-Participant:

  Der Switch wird keine GARP-Nachrichten beantworten und auch selber keine senden. Er wird nur Nachrichten empfangen und auf GVRP-BPDU (Bridge Protocol Data Unit) reagieren.

- Default Registrar Mode:

  Es gibt drei Modi für den Registrar, zwischen denen Sie wählen können: Normal registrar, Fixed Registrar und Forbidden Registrar.

  Normal:

  Der Registrar antwortet normal auf eingehende GARP-Nachrichten. Dies ist die Default-Einstellung.

  Fixed:

  Der Registrar ignoriert alle GARP-Nachrichten und alle Mitglieder verbleiben im registrierten (IN) Zustand.

  Forbidden:

  Der Registrar ignoriert alle GARP-Nachrichten und alle Mitglieder bleiben im unregistrierten (EMPTY) Zustand.

- Restricted Mode:

  Hier können Sie das Erstellen von dynamischen VLANs beschränken. Es gibt zwei Einstellungen, zwischen denen Sie wählen können: Enabled und Disabled.

  Disabled:

  Sollte der Switch eine GVRP-PDU (Protocol Data Unit) empfangen, wird er ein dynamisches VLAN erstellen. Dies ist die Default-Einstellung.

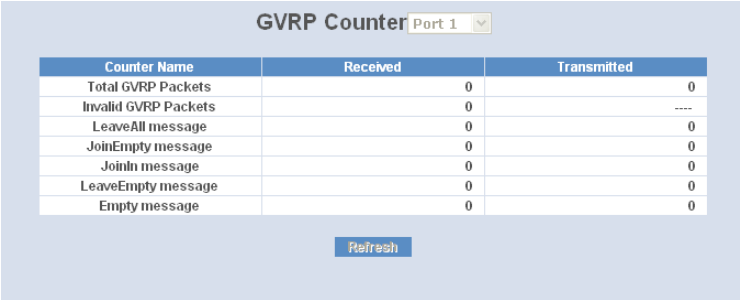
  Enabled:

  Der Switch wird kein dynamisches VLAN erstellen, wenn er eine GVRP-PDU empfängt. Sollte die dynamische GVRP-PDU zu einem existierenden statischen VLAN passen, wird der Switch diesen Port VLAN Gruppenmitgliedern hinzufügen.

4.11.2 Counter

GVRP Counter

Alle GVRP-Zähler sind grundsätzlich in empfangene (received) und gesendete (transmitted) GARP-Pakete aufgeteilt, damit Sie die GVRP-Vorgänge überwachen können.



- Parameter:
  - Received:

    Total GVRP Packets:

    Insgesamt empfangene GVRP-BPDUs der GVRP-Anwendung.

    Invalid GVRP Packets:

    Anzahl der ungültigen GARP-BPDUs, die die GVRP-Anwendung erhalten hat.

    LeaveAll Message Packets:

    Anzahl der GARP-BPDUs mit der "LeaveAll"-Nachricht, die die GARP-Anwendung empfangen hat.

    JoinEmpty Message Packets:

    Anzahl der GARP-BPDUs mit der "JoinEmpty"-Nachricht, die die GARP-Anwendung empfangen hat.

    JoinIn Message Packets:

    Anzahl der GARP-BPDUs mit der "JoinIn"-Nachricht, die die GARP-Anwendung empfangen hat.

    LeaveEmpty Message Packets:

    Anzahl der GARP-BPDUs mit der "LeaveEmpty"-Nachricht, die die GARP-Anwendung empfangen hat.

    Empty Message Packets:

    Anzahl der leeren GARP-BPDUs, die die GARP-Anwendung empfangen hat.

- Transmitted:

  Total GVRP Packets:

  Insgesamt gesendete GARP-BPDUs der GVRP-Anwendung.

  Invalid GVRP Packets:

  Anzahl der ungültigen GARP-BPDUs, die die GVRP-Anwendung gesendet hat.

  LeaveAll Message Packets:

  Anzahl der GARP-BPDUs mit der "LeaveAll"-Nachricht, die die GVRP-Anwendung gesendet hat.

  JoinEmpty Message Packets:

  Anzahl der GARP-BPDUs mit der "JoinEmpty"-Nachricht, die die GVRP-Anwendung gesendet hat.

  JoinIn Message Packets:

  Anzahl der GARP-BPDUs mit der "JoinIn"-Nachricht, die die GVRP-Anwendung gesendet hat.

  LeaveEmpty Message Packets:

  Anzahl der GARP-BPDUs mit der "LeaveEmpty"-Nachricht, die die GVRP-Anwendung gesendet hat.

  Empty Message Packets:

  Anzahl der von der GVRP-Anwendung empfangenen leeren GARP-BPDUs.

4.11.3 Group

GVRP Group Information

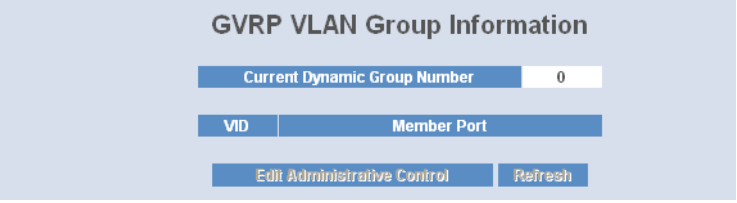
Zeigt die dynamischen Gruppenmitglieder und deren Informationen.

- Parameter
  - Current Dynamic Group Number:

    Die Anzahl der GVRP-Gruppen, die erstellt wurden.
  - VID:

    VLAN-Identifier. Wenn eine GVRP-Gruppe ein dynamisches VLAN erstellt, so wird jeder dynamischen VLAN-Gruppe ein VID zwischen 1 und 4.094 zugewiesen.

- Member Port:
  Die Mitglieder derselben dynamischen VLAN-Gruppe.
- Edit Administrative Control:
  Hier können Sie beim Erstellen einer GVRP-Gruppe den "Applicant Mode" und den "Registrar Mode" mittels der Administrative-Control-Function ändern.
- Refresh:
  Durch das Aktualisieren können Sie den aktuellen Status erfassen.



4.12 STP

Das Spanning Tree Protocol (STP) ist eine standardisierte Methode (IEEE 802.1D) um Schleifen in geswitchten Netzwerken zu vermeiden. Wenn STP aktiv ist, sollten Sie sicherstellen, dass zu einem Zeitpunkt nur eine Verbindung zwischen zwei Knotenpunkten des Netzwerks aktiviert ist. Sie können das Spanning Tree Protocol mit Hilfe des Web-Managements aktivieren und dort auch weiterführende Einstellungen vornehmen. Es wird empfohlen, dass Sie STP in allen Switches aktivieren, um sicher zu sein, dass es immer nur eine aktive Verbindung im Netzwerk gibt.

4.12.1 Status

- STP Status
  Im Spanning Tree Status können Sie 12 Parameter einsehen, um den aktuellen Stand des STP zu erfahren. Im Folgenden werden die Eigenschaften der 12 Parameter beschrieben.
- Parameter:
  - STP State:
    Zeigt den aktuellen STP Stand "enable" oder "disable". Default ist "enable".

- Bridge ID:

  Zeigt die Bridge-ID des Switches, welche auch die MAC-Adresse ist.

- Bridge Priority:

  Zeigt die aktuelle Einstellung der Bridge-Priority. Default ist 32.768.

- Designated Root:

  Zeigt die ID der Root-Bridge dieses Netzwerksegments. Wenn dieser Switch eine Root-Bridge ist, wird der Designated-Root die Bridge-ID des Switchs anzeigen.

- Designated Priority:

  Zeigt die aktuelle Root-Bridge-Priority.

- Root Port:

  Zeigt die Root-Port-Number mit den niedrigsten Verbindungskosten für Verbindungen zur Root-Bridge an.

- Root Path Cost:

  Zeigt die Verbindungskosten zwischen dem Root-Port und dem vorgesehenen Port der Root-Bridge.

- Current Max. Age:

  Aktuelle Angabe der maximum age time (maximale Lebensdauer) der Root-Bridge. Maximum age time wird benutzt, wenn die STP Topologie verändert werden soll. Wenn eine Bridge eine Nachricht zur Betriebsbereitschaft (Hello-Message) von der Root-Bridge nicht empfängt bis die maximum age time auf 0 heruntergezählt hat, wird die Root-Bridge als nicht funktionionstüchtig angesehen. Die Bridge sendet dann eine Topology Change Notification (TCN) BPDU an alle anderen Bridges.

  Alle Bridges im LAN können neu entscheiden und sich merken wer die Root-Bridge ist. Die maximum age time wird von der Root-Bridge in Sekunden bestimmt. Default ist 20 Sekunden.

- Current Forward Delay:

  Zeigt die aktuelle Forward-Delay-Time der Root-Bridge (Verzögerung beim Senden einer Nachricht). Der Wert der Forward-Delay-Time wird beim Rooten bestimmt. Die Forward-Delay-Time ist die Zeit die verstreicht vom Listening-State bis zum Learning-State oder vom Learning-State zum Forwarding-State eines Bridge-Ports.

DE

- Hello Time:

  Zeigt die aktuelle Hello-time der Root-Bridge. Die Hello-time ist ein Zeitintervall, welches von der Root-Bridge bestimmt wird. Es wird dazu benutzt, um über einen bestimmten Zeitraum alle anderen Bridges aufzufordern, jede Hello-Time-Sekunde Hello-Messages zu der Bridge mit dem zugewiesenen Designated-Port zu senden.

- STP Topology Change Count:

  STP Topology Change Count gibt die Zeit in Sekunden an, die vom Beginn des Spanning Tree Topology Change bis zum Ende der STP Konvergenz benötigt wird. Wenn der STP-Wechsel einmal umgewandelt ist, wird der Topologiewechsel auf 0 zurück gestellt. Die dafür auf dem Bildschirm angegebene Zeit wird exakt oder fast exakt wiedergegeben .

- Time Since Last Topology Change:

  Time Since Last Topology Change gibt die akkumulierte Zeit in Sekunden an, die seit dem letzten STP Topologiewechsel vergangen ist. Wenn ein Topologiewechsel ausgelöst wird, stellt sich der Zähler zurück auf 0. Er fängt erneut an zu zählen, wenn eine STP Topology Change abgeschlossen ist.

STP Status

STP State	Disabled
Bridge ID	00:A0:57:13:FA:7E
Bridge Priority	32768
Designated Root	00:A0:57:13:FA:7E
Designated Priority	32768
Root Port	0
Root Path Cost	0
Current Max. Age(sec)	20
Current Forward Delay(sec)	15
Hello Time(sec)	2
STP Topology Change Count	0
Time Since Last Topology Change(sec)	0

4.12.2 Konfiguration

Das Spanning Tree Protocol (STP), beinhaltet RSTP. In der Spanning Tree Konfiguration gibt es sechs Parameter, die Sie konfigurieren können. Im Folgenden werden die Eigenschaften der Parameter beschrieben.

- STP Configuration

  Sie können die folgenden Spanning Tree Parameter auf “enable” oder “disable” einstellen um die STP Funktion zu kontrollieren. Wählen Sie den

RSTP/STP Modus und beeinflussen Sie den STP Status der Maschine um BPDU zu senden. Default setting des Spanning Tree Protocol ist "disable".

- Parameter:
  - Spanning Tree Protocol:

    802.1W Rapid STP Funktion kann auf "enable" oder "disable" eingestellt werden. Default ist "disable".

  - Bridge Priority:

    Je niedriger der hier eingestellte Wert ist, desto höhere Priorität hat die Bridge. Normalerweise ist die Bridge mit der höchsten Priorität die Root-Bridge. Wenn Sie den LANCOM Switch als Root-Bridge benutzen wollen, können Sie ihren Wert niedriger wählen, als den Wert der Bridge im LAN. Gültige Werte liegen zwischen 0 ~ 61.440. Default ist 32.768.

  - Hello Time:

    Hello-Time wird benutzt, um die Zeit, für das Senden von einem normalen BPDU, von bestimmten Ports über Bridges zu begrenzen. Die Hello-Time entscheidet, wie lange eine Bridge eine Nachricht zu einer anderen Bridge schicken sollte und darüber, ob sie funktionstüchtig ist. Wenn zum Beispiel der LANCOM Switch die Root-Bridge des LANs ist, werden alle anderen Bridges wie vom Switch zugewiesen die Hello-time benutzen um miteinander zu kommunizieren. Die gültigen Werte liegen zwischen 1 ~ 10 in Sekunden. Default ist 2 Sekunden.

  - Max. Age:

    Wenn der LANCOM Switch die Root-Bridge ist, wird das ganze LAN die Einstellung des maximum age time des Switches übernehmen. Wenn eine Bridge eine BPDU von der Root-Bridge erhält und die age time dieser Nachricht das Maximum der Root-Bridge übersteigt, wird die Bridge die Root-Bridge als nicht funktionstüchtig ansehen und eine Topology Change Notification (TCN) BPDU an alle anderen Bridges senden. Alle anderen Bridges im LAN können sowohl bestimmen, als auch sich merken, wer die Root-Bridge ist. Der gültige Wert für das maximum age liegt zwischen 6 ~ 40 Sekunden. Default ist 20 Sekunden.

  - Forward Delay:

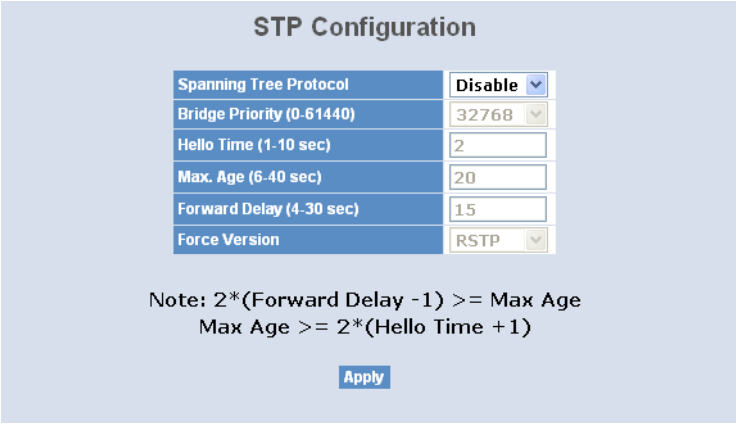
    Sie können die Forward-Delay-Time der Root-Bridge einstellen. Diese Einstellungsmöglichkeit gibt es nur bei der Root-Bridge. Die Forward-Delay-Time ist die Zeit, die ein Bridge-Port benötigt, um vom Liste-

DE

ning-State in den Learning-State oder vom Learning-State in den Forwarding-State zu gelangen. Die Forward-Delay-Time besteht aus zwei Phasen, die erste Phase ist der Übergang vom Listening-State zum Learning-State und die zweite Phase ist vom Learning-State zum Forwarding-State. Es wird angenommen, dass die Forward-Delay-Time pro Phase 15 Sekunden und somit insgesamt 30 Sekunden beträgt. Dies steht im Zusammenhang mit der STP-Convergent-Time. Gültige Werte liegen zwischen 4 ~ 30 Sekunden. Default ist 15 Sekunden.

- Force Version:

  Für den STP Algorithmus werden Ihnen zwei Optionen angeboten, RSTP und STP. Wenn Sie STP wählen, wird RSTP nachrangig angesehen. Der Switch unterstützt RSTP (802.1w), welches rückwärts kompatibel mit STP (802.1d) ist.



4.12.3 Port

- STP Port Setting

  Zur Einstellung des STP-Ports stehen Ihnen verschiedene Parameter zur Verfügung. Sie können jeden Port aktivieren oder deaktivieren, indem Sie den Port-Status bestimmen. Sie können ebenfalls die Verbindungskosten und die Priorität der einzelnen Ports einstellen, indem Sie den jeweiligen Wert eintragen und Admin-Edge-Port oder Admin-Point-to-Point einstellen.

- Parameter:

- Port Status:

  Gibt den aktuellen Status des Ports an. Es gibt nach der 802.1w Spezifikation drei mögliche Zustände.

  "Discarding State" bedeuted, dass dieser Port weder Pakete schicken noch erlerntes Wissen einbringen kann.

  Beachten Sie: Drei andere Status ("disable state", "blocking state" und "listening state") werden nach der 802.1d Spezifikation alle durch den "discarding state" vertreten.

  "Learning state" bedeuted, dass der Port sein gelerntes Wissen einbringen, aber keine Pakete versenden kann.

  "Forwarding state" bedeuted, dass der Port sowohl sein erlerntes Wissen einbringen, als auch Pakete verschicken kann.

- Path Cost Status:

  Dies ist der Wert der Verbindung vom Port zur Root-Bridge. Der STP Algorithmus bestimmt die beste Verbindung zur Root-Bridge, indem er die Summe der Verbindungskosten von allen Ports für diese Verbindung berechnet. So ist wahrscheinlicher, dass ein Port mit geringeren Verbindungskosten Root-Port wird.

- Configured Path Cost:

  Der Bereich geht von 0 - 200.000.000. Wenn die Verbindungskosten auf Null eingestellt sind, wird das STP den empfohlenen Wert aus der Auto-Verhandlung des entsprechenden Links bekommen und diesen Wert im Path Cost Status anzeigen. Wenn dies nicht der Fall ist, wird der Wert angezeigt, den der Administrator im Configured-Path-Cost und Path-Cost-Status eingegeben hat.

  Der empfohlene Wert für 802.1w RSTP liegt zwischen 1 - 200.000.000.

  10 Mbps : 2.000.000

  100 Mbps : 200.000

  1 Gbps : 20.000

  Default : 0

- Priority:

  In diesem Fall ist die Priorität des Ports gemeint. Die Priorität und die Nummer des Ports ergeben zusammen die ID des Ports. Port-IDs wer-

den oft verglichen, um zu bestimmen welcher Port einer Bridge Root-Port wird. Der Bereich umfasst 0 - 240. Default ist 128.

- Admin Edge Port:

  Wenn Sie die Einstellung "yes" wählen, wird der Port ein Edge-Port. Ein Edge-Port ist ein Port, der mit einem Gerät verbunden ist, dass das STP oder RSTP nicht beherrscht. Normalerweise ist das verbundene Gerät dann eine Endpunkt. Edge-Ports gelangen sofort in einen Forwarding-State und überspringen den Listening- und Learning-State, weil der Edge-Port keine Bridging-Loops im Netzwerk erstellen kann. Dies beschleunigt die Konvergenz. Wenn der Link des Edge-Ports umschaltet, wird die STP-Topologie nicht verändert. Im Gegensatz zu einem Designated-Port oder einem Root-Port, schaltet der Edge-Port auf einen normalen Spanning-Tree-Port um, sobald er ein BPDU empfängt. Default ist "no".

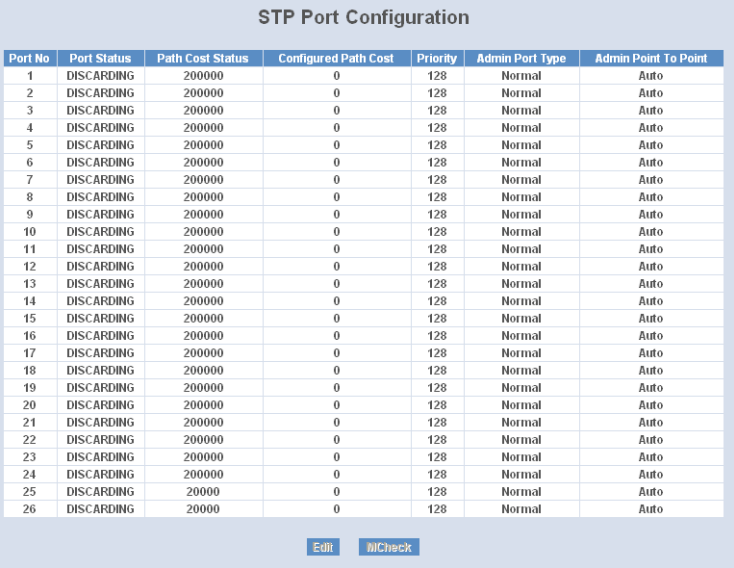
- Admin Point To Point:

  Aus der Sicht des RSTP ist ein Port ein Point-to-Point-Link, wenn er im vollduplexen Modus ist und ein Shared-Link, wenn er im halbduplexen Modus ist. Schnelle RSTP-Konvergenz kann nur in Point-to-Point-Links und in Edge-Ports stattfinden. Da der Port schnell in einen Forwarding-State gelangt, kann die Konvergenz beschleunigt werden.

  Es gibt drei Parameter "auto" "true" und "false", die dazu benutzt werden den Typ des Point-to-Point-Links zu bestimmen. Wenn Sie diesen Parameter auf "auto" einstellen, befindet sich RSTP im duplexen Modus. In den heutzutage geswitchten Netzwerken laufen die meisten Links im vollduplexen Modus. Manchmal kann das Ergebnis auch halbduplex sein. In diesem Fall wird der Port nicht in den Forwarding-State umschalten. Wenn Sie die Einstellung "true" wählen, wird der Port von RSTP als Point-to-Point-Link angesehen und bedingungslos in den Forwarding-State gebracht. Wenn Sie "false" wählen, wird die Umwandlung zum Forwarding-State nicht vorkommen. Default ist "auto".

- M Check

  Der Migration-Check zwingt den Port ein RSTP BPDU anstelle eines nachrangigen STP BPDU bei der nächsten Übertragung zu senden. Der Vorteil dieses Vorgangs ist, dass der Port schnell wieder zum RSTP-Port wird. Klicken Sie <M Check> um ein RSTP BPDU von dem, von Ihnen ausgewählten, Port zu senden.



STP Port Configuration

Port No	Port Status	Path Cost Status	Configured Path Cost	Priority	Admin Port Type	Admin Point To Point
1	DISCARDING	200000	0	128	Normal	Auto
2	DISCARDING	200000	0	128	Normal	Auto
3	DISCARDING	200000	0	128	Normal	Auto
4	DISCARDING	200000	0	128	Normal	Auto
5	DISCARDING	200000	0	128	Normal	Auto
6	DISCARDING	200000	0	128	Normal	Auto
7	DISCARDING	200000	0	128	Normal	Auto
8	DISCARDING	200000	0	128	Normal	Auto
9	DISCARDING	200000	0	128	Normal	Auto
10	DISCARDING	200000	0	128	Normal	Auto
11	DISCARDING	200000	0	128	Normal	Auto
12	DISCARDING	200000	0	128	Normal	Auto
13	DISCARDING	200000	0	128	Normal	Auto
14	DISCARDING	200000	0	128	Normal	Auto
15	DISCARDING	200000	0	128	Normal	Auto
16	DISCARDING	200000	0	128	Normal	Auto
17	DISCARDING	200000	0	128	Normal	Auto
18	DISCARDING	200000	0	128	Normal	Auto
19	DISCARDING	200000	0	128	Normal	Auto
20	DISCARDING	200000	0	128	Normal	Auto
21	DISCARDING	200000	0	128	Normal	Auto
22	DISCARDING	200000	0	128	Normal	Auto
23	DISCARDING	200000	0	128	Normal	Auto
24	DISCARDING	200000	0	128	Normal	Auto
25	DISCARDING	20000	0	128	Normal	Auto
26	DISCARDING	20000	0	128	Normal	Auto

Edit MCheck

4.13 Trunk

In den Port-Trunking-Einstellungen können Sie entscheiden, wie bei Link-Bündelung verfahren werden soll. Sie können mehr als einen Port mit derselben Geschwindigkeit, Full-Duplex und derselben MAC-Adresse als einen logischen Port zusammenfassen, dem dann die gebündelte Bandbreite dieser Ports zur Verfügung steht. Damit können Sie mit ihrer bestehenden Ethernet-Infrastruktur höhere Bandbreiten verwirklichen. Beispielsweise erreichen Sie durch das Zusammenfassen von drei Ports zu einem logischen Port die dreifache Bandbreite.

Der Switch unterstützt zwei Methoden des Port-Trunking:

1. LACP:

   Ports mit dem "Link Aggregation Control Protocol" nach IEEE 802.3ad (LACP, Link-Bündelungs-Kontroll-Protokoll) als Port-Trunking-Methode können eine eindeutige "LACP-GroupID" (Zwischen 1 und 3) (LACP-Gruppen-Identität) festlegen um einen logischen Port zu bilden. Der Vorteil dieser Methode ist, dass ein Port sich mit dem Gegenport abstimmt bevor er ein aktives Mitglied (auch Aggregator genannt) einer Trunk-

Gruppe, also eines logischen Ports wird. Das LACP ist daher die sicherere Trunking-Methode.

Port-Trunking wird in folgenden Fällen nicht funktionieren:

- Link-Bündelung über mehrere Switches
- Bündelung mit nicht IEEE 802.3-MAC-kompatibelen Links
- Operieren im Half-Duplex Modus
- Das Bündeln von Ports mit verschiedenen Datenraten

2 Static Trunk:

Wenn Sie für Ports die Static-Trunk-Methode (Statische Trunks) wählen, müssen Sie ihnen eine bestimmte "Static-GroupID" (Ebenfalls 1-3, die Statische-Gruppen-Identität kann diesselbe sein, wie die einer LACP-Gruppe) zuweisen. Der Vorteil dieser Methode ist, dass ein Port sofort als aktives Mitglied eines logischen Ports funktioniert, ohne sich vorher mit der Gegenseite abstimmen zu müssen. Dies ist gleichzeitig allerdings auch ein Nachteil, da die jeweiligen gegenüberliegenden Ports eventuell nicht als logischer Port konfiguriert sind. Deshalb sollten Sie in diesem Fall auf beiden Seiten Static-Trunk als Methode wählen. Beachten Sie bitte auch, dass Links mit niedriger Geschwindigkeit bei dieser Methode nicht aktive Mitglieder eines logischen Ports werden, wenn man sie mit Links höherer Geschwindigkeit bündelt.

Der Switch erlaubt es, bis zu drei Static-Trunk- und LACP-Gruppen in der Management-Ansicht festzulegen. Es können jedoch nur drei logische Ports gleichzeitig aktiv sein. Eine LACP-Gruppe mit mehr als einem aktiven Mitglied wird als aktiver logischer Port verstanden, während eine LACP-Gruppe mit nur einem aktiven Mitglied nicht als solcher unterstützt wird. Jede Statische Trunk-Gruppe ist automatisch ein aktiver logischer Port.

Jede Trunk-Gruppe, gleich welcher Methode, kann maximal vier aktive Mitglieder haben. Bitte beachten Sie, dass einige Entscheidungen automatisch vom System getroffen werden, während Sie Einstellungen zum Bündeln von Ports vornehmen. Es gibt vier Trunk-Einstellungsregeln:

① Maximal 3 Gruppen sind möglich

② Eine Gruppe kann maximal 4 aktive Mitglieder bzw. Ports enthalten.

③ Die Ports 25 und 26 können nicht Mitglied der Gruppen 1 und 2 sein.

④ Die Gruppe 3 kann nicht die Ports 1-24 enthalten.

4.13.1 Port

Trunk Port Setting/Status

Hier können Sie die Zugehörigkeit zu einer Trunk-Gruppe für jeden Port einsehen und konfigurieren.

- Parameter:

  - Method: Legen Sie hier die Methode fest, die der Port nutzen soll um mit anderen Ports gebündelt zu werden.

    None: Der Port wird sich nicht mit anderen Ports bündeln.

    LACP: Das LACP wird benutzt um den Port mit anderen Ports zu einem logischen Port zu bündeln.

    Static: Der Port wird Static-Trunk als Methode verwenden um sich mit anderen Ports, die ebenfalls Static-Trunk nutzen, zu bündeln.

  - Group:

    Alle Ports, die dieselbe Methode verwenden, müssen einer eindeutigen Gruppen-Identität (zwischen 1 und 3) zugeordnet werden, wenn sie als logischer Port gebündelt werden.

  - Active LACP:

Dieses Feld wird nur dann angezeigt, wenn die Trunking-Methode für diesen Port LACP ist.

Active:

Ein aktiver LACP Port wird mit dem Senden einer LACPDU(LACP-Paket) an sein Gegenüber beginnen, sobald die LACP Entität die Kontrolle über diesen Port übernommen hat.

Passive:

Ein passiver LACP Port wird nicht von sich aus eine LACPDU senden, bevor er nicht ein solches Paket von seinem Gegenüber erhalten hat.

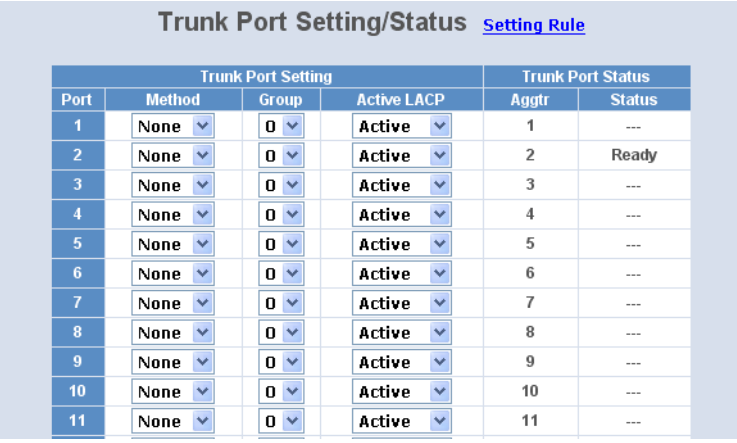
  - Aggtr:

    Aggtr ist eine Abkürzung für “Aggregator”. Jeder Port ist auch ein Aggregator, und seine Aggregator-ID ist dieselbe wie seine Port-Nummer. Einen Aggregator können wir als Repräsentant seiner Trunking-Gruppe betrachten. Alle Ports mit derselben Gruppen-Identität und Trunk-Methode lassen sich zu einem bestimmten Aggregator-

Port zusammen bündeln. Der Aggregator-Port ist normalerweise der Port mit der niedrigsten Port-Nummer innerhalb der Trunk-Gruppe.

- Status:

  Dieses Feld zeigt Ihnen den Trunk-Status eines Ports an, der an der Port-Bündelung teilnimmt. Ports, die nicht an der Port-Bündelung teilnehmen, erscheinen als "not ready"(Nicht bereit).



4.13.2 Aggregator View

Aggregator View

Zeigt Ihnen die aktuellen Trunk-Informationen aus Sicht eines Aggregators an.

- Parameter:
  - Aggregator:

    Hier finden Sie die Aggregator-ID (1-26) für jeden Port, die mit der generellen Port-Nummer bzw. -ID übereinstimmt, da jeder Port potentiell ein Aggregator ist.

  - Method:

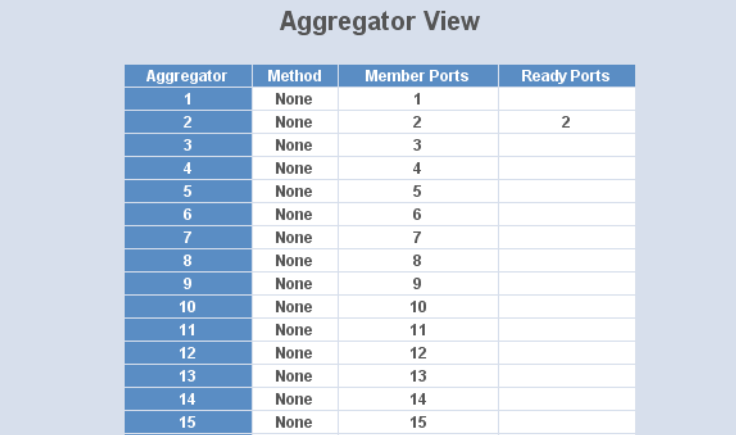
    Zeigt Ihnen die Methode an, die ein Port verwendet um sich mit anderen Ports zu bündeln.

  - Member Ports:

    Alle Port-Mitglieder eines Aggregators werden Ihnen hier angezeigt.

- Ready Ports:

  Nur die aktiven Mitglieder eines Aggregators werden angezeigt.



Aggregator View

Aggregator	Method	Member Ports	Ready Ports
1	None	1	
2	None	2	2
3	None	3	
4	None	4	
5	None	5	
6	None	6	
7	None	7	
8	None	8	
9	None	9	
10	None	10	
11	None	11	
12	None	12	
13	None	13	
14	None	14	
15	None	15	

LACP Detail (LACP Aggregator Detailed Information)

Zeigt Ihnen detailierte Information über die LACP-Gruppe an.

- Parameter
  - Actor:

    Derjenige Switch, von dem Sie die Einstellungen betrachten.
  - Partner:

    Das gegenüberliegende (Partner-)System aus Ihrer Sichtweise.
  - System Priority:

    Zeigt die Systemprioritäts-Teil einer System-ID an.
  - MAC Address:

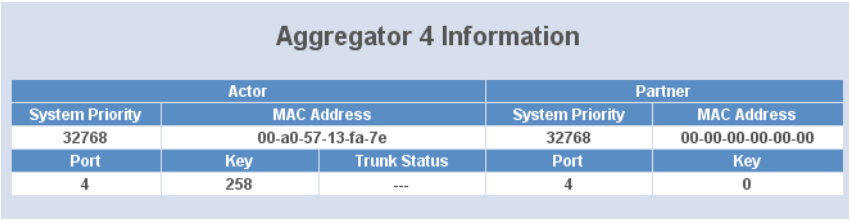
    Hier können Sie den MAC-Adressen-Teil einer System-ID ablesen.
  - Port:

    Der Port-Nummern-Teil der LACP-Port-ID kann hier von Ihnen abgelesen werden.
  - Key:

    Zeigt den Wert des Feldes "Key"(Schlüssel) des Aggregators. Dieser Wert wird von dem LACP festgelegt und lässt sich nicht durch die Konfigurations-Oberfläche einstellen.

- Trunk Status:

  Zeigt den Trunk-Status eines einzelnen Ports an. Dabei bedeutet "---" das der Port nicht bereit bzw. nicht aktiv ist.



4.13.3 LACP System Configuration

LACP System Configuration

In den LACP-System-Einstellungen können Sie den Prioritätsteil der LACP-System-ID festlegen. Das LACP wird nur Ports zusammenbündeln, deren Partner sich ebenfalls auf nur einem System befinden. Jedes System, dass das LACP unterstützt bekommt dazu eine eindeutige, globale System-ID zugewiesen. Diese System-ID besteht aus einem 64-Bit Feld, das wiederrum aus einer 48-Bit MAC-Adresse und einem 16-Bit Prioritätswert besteht.

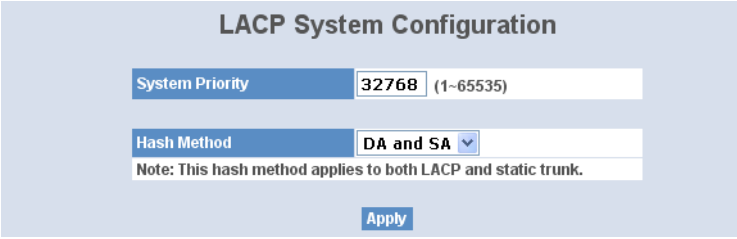
- Parameter
  - System Priority:

    Die Systempriorität lässt sich zwischen 1 und 65.535 festlegen. Die Default-Einstellung ist 32.768.

  - Hash Method:

    DA+SA, DA und SA sind drei angebotene Hash-Methoden für die Link-Bündelung auf dem Switch. Der Hash-Modus entscheidet, welchen Weg die Pakete zum Senden nehmen.

    Default-Einstellung: DA+SA

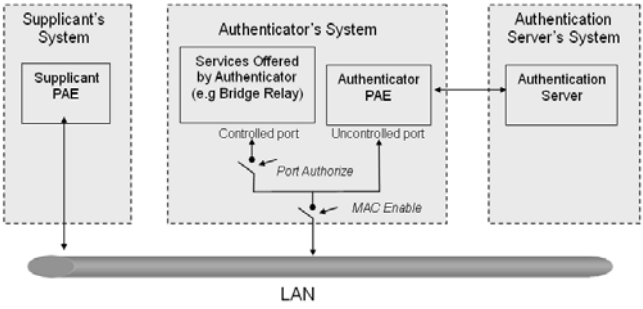


DE

4.14 802.1x Konfiguration

Die 802.1x Port-basierte Netzwerkzugangs-Verwaltung ist eine Methode bestimmte Benutzer auf bestimmte Netzwerkressourcen zu beschränken, indem man ihre Benutzerinformation authentizifiert. Dadurch ist der Netzwerkzugang durch einen 802.1x-fähigen Port ohne Authentizifierung ausgeschlossen. Sollte ein Benutzer das Netzwerk durch einen solchen Port betreten wollen, muss er zunächst seinen Accountnamen eingeben und dann auf die Authentizifierungsbestätigung warten bevor er über den 802.1x-fähigen Port Packete senden oder schicken kann.

Damit Geräte und Endstationen Netzwerkressourcen unter 802.1x-Kontrolle nutzen können, müssen sie eine Authentizifierungs-Anfrage für diese kontrollierten Ports an den Authenticator senden. Der Authenticator reicht diese Anfrage dann an den Authentizifierungs-Server weiter, der sie bearbeitet und verifiziert und dann die Nutzung der Ports gestattet oder ablehnt.



Nach dem IEEE802.1x-Standard sind drei Komponenten implimentiert: Der Authenticator, Supplicant und der Authentizifierungs-Server.

- Supplicant:

  Diese Entität wird dafür, benutzt auf Anfrage des Authenticators dessen PAE (Port Access Entity) die Authentizifierungs-Informationen zu kommunizieren.

- Authenticator:

  Eine Entität für die Kontrolle sowohl authentizifierter, als auch nicht-authentizifierter Ports. Sie authentizifiert die Supplicant-Entität je nachdem wie der Austausch der Authentizifierungs-Nachricht zwischen ihr und dem Supplicant-PAE abgelaufen ist. Sie können eine Zeit festlegen nach der der Authenticator eine Re-Authentizifierung des Supplicant ver-

langt. Während der Re-Authentizifierung bleibt der Port (bis zum eventuellen Scheitern des Authenzifierungs-Vorgangs) in einem authentizifierten Zustand.

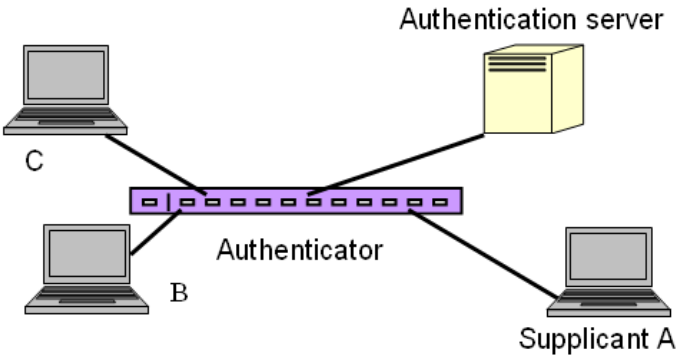
Einen als Authenticator fungierenden Port können Sie sich als zwei logische Ports vorstellen, einen kontrollierten und einen unkontrollierten. Der kontrollierte Port kann nur dann Packete passieren lassen, wenn der PAE des Authenticators dies gestattet; Während der unkontrollierte Port alle Packete mit einer PAE-Gruppen-MAC-Adresse mit dem Wert 01-80-c2-00-00-03 zu jeder Zeit passieren lassen wird.

- Authentication server:

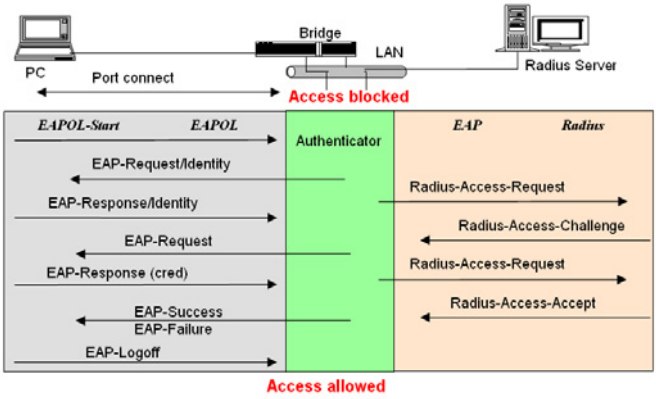
  Dieses Gerät leistet den Authentizifierungs-Service durch EAP für den Authenticator. Dabei nutzt es Authentizifierungs-Zertifikate, die vom Supplicant geliefert wurden, um dessen Zugangsberechtigung zum Netzwerk festzustellen.

Wenn die Supplicant-PAE eine Authentizifierungs-Anfage an die Authenticator-PAE richtet, wird diese den Supplicant um das Senden der Authentizifierungs-Nachricht bitten. Diese Nachricht sendet der Authenticator dann an den RADIUS-Server weiter um die Informationen zu verifizieren. Der RADIUS-Server wird dann die Anfrage gestatten oder abweisen und entsprechend antworten.

Während des Authentizifierungs-Prozesses werden die Nachrichtenpakete zwischen Supplicant und Authenticator durch das Extensible-Authentication-Protocol-over-LAN (EAPOL) eingekapselt. Auch die Kommunikation zwischen Authenticator und Authentizifierungs-Server nutzt das EAPOL. Vor einer erfolgreichen Authentizifierung kann der Supplicant den Authenticator nur für den Authentizifierungs-Nachrichtenaustausch erreichen, oder auf das Netzwerk über den unkontrollierten Port zugreifen.



Die Abbildung zeigt eine typische Konfiguration: Ein einzelner Supplicant, ein Authenticator und ein Authentizifierungs-Server. B und C sind im internen Netzwerk, D ist ein Authentizifierungs-Server, auf dem RADIUS ausgeführt wird. Der zentrale Switch fungiert als Authenticator, zu dem PC A verbunden ist. A ist ein Computer ausserhalb des kontrollierten Ports und führt eine Supplicant-PAE aus. Angenommen, PC A möchte Zugriff auf die Ressourcen auf den Geräten B und C, dann muss er zunächst eine Authentizifierungs-Nachricht mit dem Authenticator durch ein EAPOL-Packet austauschen. Der Authenticator wird dann die Authentizifierungs-Zertifikate dem Authentizifierungs-Server vorlegen. Sollte dieser der Authentizifierung zustimmen, sendet er diese Information dem Authenticator, der dann dem PC A den Zugang auf die Geräte B und C durch den Switch gestattet. Sollte es zwei direkt miteinander verbundene Switches geben, hat der Verbindungs-Port zwischen den beiden möglicherweise sowohl die Rolle einen Supplicants, als auch eines Authenticators, da der Verkehr hier bidirektional ist.



Die Abbildung zeigt den Ablauf einer 802.1x Authenzifierung. Die Login-Schritte basieren auf 802.1x Port-Zugangs-Kontrollmanagement. Auf der linken Seite kommt das EAPOL-, auf der rechten das EAP-Protokoll zum Einsatz.

1. Zu Beginn des Prozesses ist der Supplicant A nicht authentifiziert und auch der Port am Switch, der als Authenticator fungiert, ist im nicht autorisierten Zustand. Der Zugang ist also in diesem Schritt noch geblockt.

2. Sowohl Authenticator als auch Supplicant können einen Nachrichtenaustausch initiieren. Wenn der Supplicant den Austausch beginnt, sendet er eine EAPOL-Start-Nachricht an den Authenticator, auf die dieser sofort mit einem EAP-Request/Identiy-(EAP-Identitätsanfrage) Paket antworten wird.

3. Der Authenticator sendet regelmässig EAP-Request/Identity-Pakete an den Supplicant um eine Re-Authentizifierung der Identität anzufragen.

4. Sollte der Authenticator den Austausch nicht durch das Senden des EAP-Request/Identiy-Pakets beginnen, wird der Supplicant durch das Senden des EAPOL-Pakets den Prozess starten.

5. Als nächstes wird der Supplicant ein EAP-Response/Identity-(EAP-Identitätsantwort) Paket als Antwort an den Authenticator schicken. Der Authenticator wird dann die Benutzer-ID in den RADIUS-Access-Request-(RADIUS-Zugang)Befehl einbetten und diesen an den Authentizifierungs-Server senden um so die Identität des Benutzers zu bestätigen.

6. Nach dem Empfangen des RADIUS-Access-Request-Befehls wird der Authentizifierungs-Server ein RADIUS-Access-Challenge-(RADIUS-Indentitätsanforderung) Paket an den Supplicant senden, indem er ihn auffordert sein Benutzerpasswort durch die Authenticator-PAE einzugeben.

7. Der Supplicant wird sein Benutzerpasswort in die Zertifikatsinformationen konvertieren (z. B. im MDF- oder OPT-Format) und antwortet diese Zertifikationsinformationen sowie den spezifischen Authentizifierungsalgorithmus als EAP-Response-Paket an den Authentizifierungs-Server durch die Authenticator-PAE. Durch den Wert des entsprechenden Feldes der Nachricht-PDU weiß der Authentizifierungs-Server, welchen Algorithmus er anwenden muss um die Zertifikatsinformation zu verfizieren, z. B. EAP-MD5 (Message Digest 5), EAP-OTP (One Time Password) oder einen anderen Algorithmus.

8. Wenn Benutzer-ID und Passwort korrekt eingegeben wurden, wird der Authentizifierungs-Server ein RADIUS-Access-Accept-(RADIUS-Zugangsbestätigung) Befehl an den Authenticator senden. Sollten die Benutzereingaben nicht korrekt sein wird er entsprechend ein RADIUS-Access-Reject-(RADIUS-Zugangsverweigerung) Paket senden.

9. Der Authenticator wird ein EAP-Success-(EAP-Erfolg) Paket an den Supplicant senden, wenn es ein RADIUS-Acces-Accept-Paket vom Authentizifierungs-Server erhält. Gleichzeitig wechselt der Port unter 802.1x-Kontrolle des Supplicants in den authorisierten Zustand. Der Supplicant und andere Geräte an diesem Port können nun auf das Netzwerk zugreifen. Sollte der Authenticator dagegen ein RADIUS-Access-Reject-Paket erhalten, wird dem Supplicant ein EAP-Failure-(EAP-Scheitern) Befehl weitergegeben. Dies bedeutet, dass die Authentizifierung fehlgeschlagen ist und der entsprechende Port im unauthorisierten Zustand bleibt, d.h. der Supplicant und andere an diesen Port angeschlossene Geräte haben keinen Zugriff auf das Netzwerk.

10. Der Supplicant kann eine EAP-Logoff-Nachricht an den Server senden. Dies löst ein Wechseln des entsprechenden Ports in den unauthorisierten Zustand aus.

MultiHost 802.1X ist die einzige Authentizifierungsmethode, die der Switch unterstützt. Diese Methode gestattet es nur korrekt authentizifierten Geräten, die über einen solchen Port verbunden sind, auf das Netzwerk zuzugreifen.

Die Port-basierte 802.1X Netzwerkzugangs-Kontrollfunktion des Switches unterstützt ausschließlich Basis-MultiHost-Modus. Dieser kann zwischen der MAC-Adresse und der VID eines Gerätes unterscheiden. Die folgende Gegenüberstellung zeigt zusammenfassend die Kombination von Authentizifierungs- und Portstatus im Vergleich zum Portmodus-Status, den sie im 802.1x Port-Modus einstellen können,und dem Portkontrolle-Status, den Sie in den Port-Einstellungen setzen können. Dabei bedeuet Zugangsberechtigung, dass der jeweilige MAC-Zugang authorisiert wurde.

Port Mode	Port Control	Authentication	Port Status
Disable	Don't Care	Don't Care	Port Uncontrolled
Multihost	Auto	Successful	Port Authorized
Multihost	Auto	Failure	Port Unauthorized
Multihost	ForceUnauthorized	Don't Care	Port Unauthorized
Multihost	ForceAuthorized	Don't Care	Port Authorized

802.1x State Setting

Hier können Sie die globalen Parameter für die RADIUS Authentifizierung der 802.1x-Port-Sicherheitsanwendung einstellen.

- Parameter
  - Radius Server:

    Die IP-Adresse des RADIUS-Authentizifierungs-Servers.

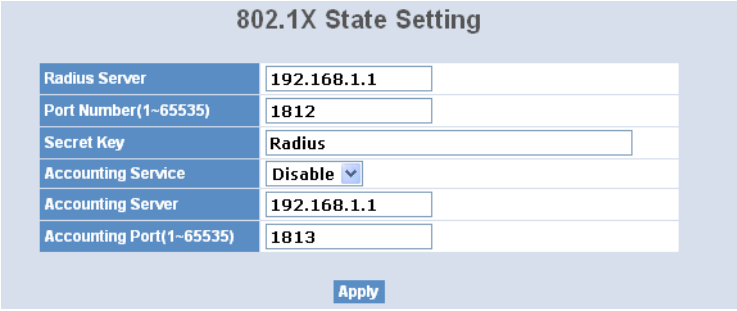
    Default-Einstellung: 192.168.1.1
  - Port Number:

    Der Port auf dem der RADIUS-Server erreichbar ist. Zugelassen sind alle Ports zwischen 1-65.535.

    Default-Einstellung ist auf Port 1812.
  - Secret Key:

    Hier können Sie den Sicherheits-Schlüssel festlegen, den Authentifizierungs-Server und Authenticator zum kommunizieren verwenden. Sie können eine Zeichenkette zwischen 1-31 Buchstaben sowie die Zahlen 0-9 verwenden, allerdings kein Leerzeichen. Die Groß- und Kleinschreibung wird beachtet.

    Default-Einstellung: Radius



802.1x Mode Setting

Hier können Sie für jeden Port individuell entscheiden, ob er den 802.1x Modus verwendet.

- Parameter
  - Port Number:

    Geben Sie hier an, welchen Port Sie verwenden um den 802.1x Modus zu konfigurieren.
  - 802.1x Mode:

    Hier können Sie den 802.1x Modus einstellen. Sie haben die Wahl zwischen den folgenden Werten für den 802.1x-Modus:

    Disable:

    Der Port erfordert keine Authentifizierung über 802.1x.

    Normal:

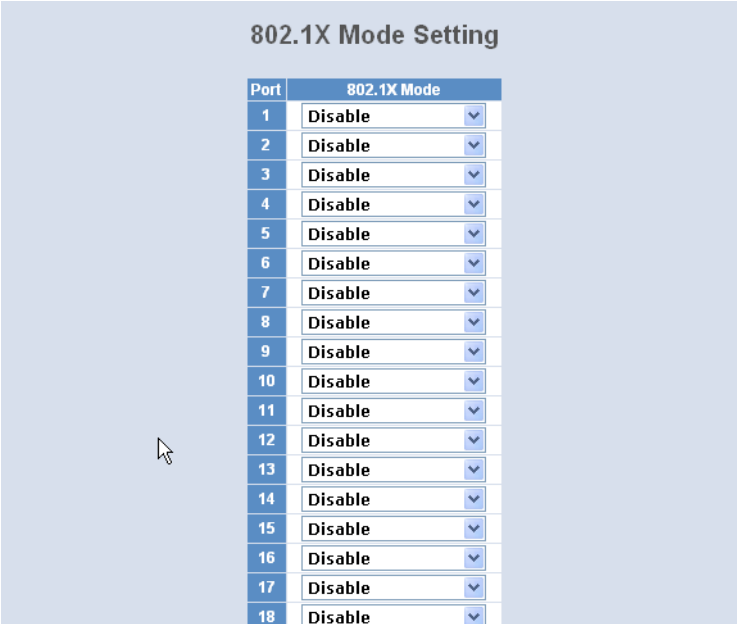
    Ein an diesem Port angeschlossenes Gerät muss über 802.1x authentifiziert werden, um Zugang zum Netzwerk zu erhalten.

    Advanced 802.1x:

    Diese Einstellung wird verwendet, wenn an dem Port ein Hub oder Switch im Downlink angeschlossen ist. Alle an diesem Hub/Switch angeschlossenen Geräte müssen dann über 802.1x authentifiziert werden, um Zugang zum Netzwerk zu erhalten.

  Die Default-Einstellung ist “Disable”.

DE



Port Security Management

Zeigt Ihnen den Status für jeden Port an. Wenn MultiHost eingeschaltet ist, können Sie hier auch sehen, ob ein Port authorisiert oder unautorisiert ist.

- Parameter
  - Disable Mode:

    Wenn Sie hier "Disabled"(Aus) wählen, wird der Port nicht durch einen 802.1x-Authenticator geschützt. Jedes über diesen Port verbundene Gerät kann ohne Zustimmung des 802.1x Authenticatos auf das Netzwerk zugreifen.
  - Port Number:

    Hier können Sie auswählen, für welchen Port zwischen 1-26 Sie den Status der 802.1x Authentizifierung angezeigt haben möchten.
  - Port Status:

    Der aktuelle 802.1x-Status des Portes. Wenn Sie 802.1x für den Port abgeschaltet haben, ist dieses Feld nicht aktiv.

- 802.1x with Multihost mode:

  Sie können festlegen, dass Geräte nur dann mit dem Netzwerk über diesen Port verbinden dürfen, wenn der jeweilige Authenticator dies nach erfolgreicher Authentizifierung zulässt. Wenn über diesen Port der Zugriff auf das Netzwerk gestattet ist, wird der Port-Status auf "authorized"(autorisiert) stehen, dementsprechend auf "unauthorized"(nicht autorisiert), wenn der Zugriff verweigert wurde.

Param. Setting

Hier können Sie Parameter für individuelle Ports in der 802.1x Anwendung festlegen. Details finden Sie im Folgenden.

- Parameter
  - Port:

    Hier können Sie festlegen welchen Port Sie verwenden möchten um die jeweiligen, folgenden 802.1x Parameter zu konfigurieren.

  - Port Control:

    Hier können Sie den Authentifizierungs-Modus auswählen. Sie haben die Wahl zwischen drei Modi: "ForceUnauthorized"(Authentizifierung

Verbieten), "ForceAuthorized"(Authentifizierung Erzwingen) und "Auto"(Automatik).

ForceUnauthorized:

Der kontrollierte Port ist gezwungen im nicht authorisierten Zustand zu verbleiben.

ForceAuthorized:

Der kontrollierte Port ist gezwungen im authorisierten Zustand zu bleiben.

Auto:

Ob der Port authorisiert oder nicht authorisiert wird, hängt vom Ergebnis des Authentifizierungs-Prozesses zwischen Authentifizierungs-Server und Supplicant ab.

Default-Einstellung: Auto

- reAuthMax(1-10):

  Hier können Sie festlegen nach wievielen erfolglosen Authentifizierungsversuchen der Port als nicht authorisiert eingestuft wird.

  Default-Einstellung: 2

- txPeriod(1-65.535 s):

  Die Zeitspanne in Sekunden, in der die EAPOL-PDU zwischen Authenticator und dem Supplicant gesendet werden muss.

  Default-Einstellung: 30 Sekunden

- Quiet Period(0-65.535 s):

  Die Zeitspanne in Sekunden, in der nicht versucht wird auf den Supplicant zuzugreifen.

  Default-Einstellung: 60 Sekunden

- reAuthEnabled:

  Hier können Sie entscheiden, ob an diesem Port reguläre Authentifizierung stattfinden soll oder nicht.

  Default-Einstellung: ON (Ein)

- reAuthPeriod(1-65.535 s):

  Hier können Sie die Zeitspanne in Sekunden festlegen, nach der sich ein Supplicant erneut authentifizieren muss. Sie darf nicht Null betragen.

Default-Einstellung: 3.600 Sekunden

- max. Request(1-10):

  Legen Sie hier fest, wie oft der Authenticator einen auf diesem Port verbundenden Supplicant zur Authentifizierung mit dem EAP-Request-Packet auffordert, bevor er die Sitzung schließt.

  Default-Einstellung: 2

- suppTimeout(1-65.535 s):

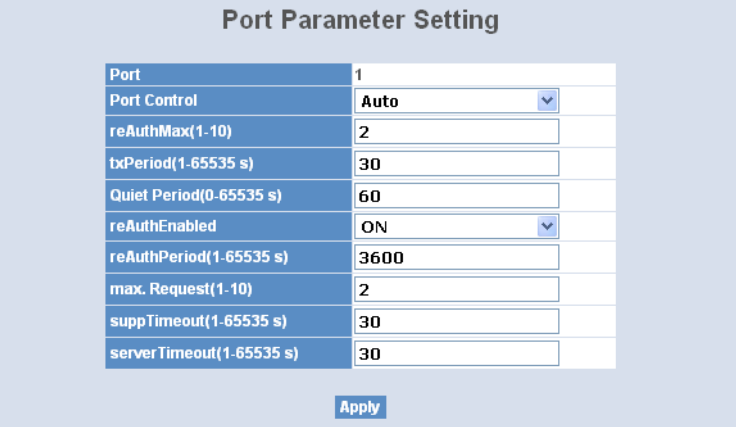
  Legen Sie hier fest, welche Verzögerung in Sekunden zwischen Authenticator und Supplicant maximal auftreten kann, bevor die Sitzung abgebrochen wird.

  Default-Einstellung: 30 Sekunden

- serverTimeout(1-65.535 s):

  Hier können Sie festlegen, welche maximale Verzögerung in Sekunden zwischen Authenticator und Authentifizerungs-Server auftreten kann, bevor die Sitzung geschlossen wird.

  Default-Einstellung: 30 Sekunden



4.15 TACACS+

4.15.1 Einleitung

Nur für LANCOM ES-2126+

TACACS+ (Terminal Access Control Access Control Server) ist ein Protokoll für Authentifizierung, Authorisierung und Accounting (AAA), es stellt also den

DE

Zugang zu Netzwerkkomponenten nur für bestimmte Nutzer sicher, regelt die Berechtigungen der Benutzer und überträgt Daten für die Protokollierung der Netzwerknutzung. TACACS+ ist also eine Alternative zu anderen AAA-Protokollen wie RADIUS.

Der Einsatz von TACACS+ ist eine Voraussetzung für die Einhaltung der PCI-Compliance (Payment Card Industry).

Die Regelung der Zugriffsmöglichkeiten für die Anwender stellt in modernen Netzwerken mit zahlreichen Diensten und Netzwerkkomponenten eine große Herausforderung dar. Gerade in größeren Szenarien ist es kaum noch möglich, die Zugangsdaten der Benutzer auf jedem Gerät bzw. in jedem Dienst einzutragen und auf Dauer konsistent zu halten. Aus diesem Grund bietet sich die zentrale Bereitstellung der Benutzerdaten auf einem entsprechenden Server an.

In einem einfachen Anwendungsbeispiel möchte sich ein Anwender auf einem Router anmelden und übermittelt dazu seine Zugangsdaten (User-ID) an den Router. Der Router fungiert in diesem Fall als Network Access Server (NAS): er überprüft die Zugangsdaten nicht selbst, sondern leitet diese an den zentralen AAA-Server weiter, der die Daten nach der Prüfung mit einen positiven Bestätigung (Accept) oder einer Ablehnung (Reject) beantwortet.

4.15.2 Konfiguration der TACACS+-Parameter

Mit den folgenden Parametern wird TACACS+ konfiguriert:

- **State**

  Konfiguriert die TACACS+-Server und legt das Kennwort für die Verschlüsselung der Datenübertragung über das TACACS+-Protokoll fest.

  - Server 1: Adresse des TACACS+-Server, an den die Anfragen für Authentifizierung, Authorisierung und Accounting weitergeleitet werden sollen.

    Der Wert 0.0.0.0 deaktiviert diesen Eintrag.

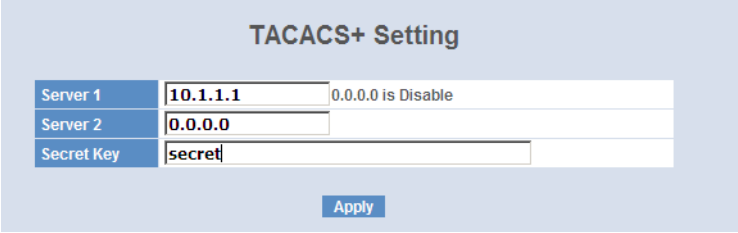
  - Server 2: Hier können Sie optional eine zweite TACACS+-Server-Adresse konfigurieren. Wenn der erste TACACS+-Server nicht erreichbar ist, leitet das Gerät die Anfragen nach Erreichen der

maximal fehlgeschlagenen Login-Versuche an den zweiten TACACS+-Server weiter. Die maximale Anzahl der Fehlversuche wird als "Access Retry" im Menüpunkt "Access" festgelegt.

Der Wert 0.0.0.0 deaktiviert diesen Eintrag.

- Secret Key: Das Kennwort für die Verschlüsselung der Kommunikation zwischen NAS und TACACS+-Server.

Das Kennwort muss im LANCOM und im TACACS+-Server übereinstimmend eingetragen werden. Eine Nutzung von TACACS+ ohne Verschlüsselung ist nicht zu empfehlen.



Authentication

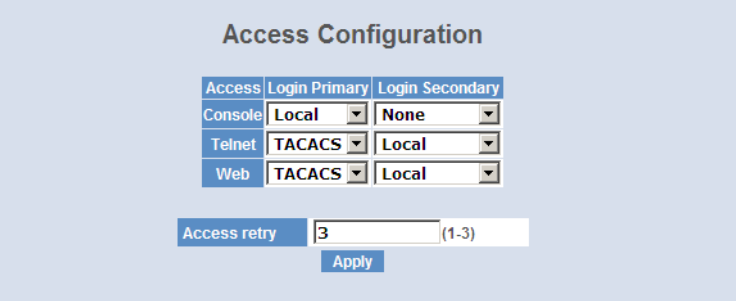
Der Zugang zum Gerät zur Konfiguration kann über die serielle Schnittstelle (Console), über das LAN mit Telnet bzw. SSH oder mit einem Browser erfolgen. Für jede dieser drei Zugangsarten kann separat eingestellt werden, ob für die Zugangsprüfung die lokalen Benutzerkonten im Gerät selbst oder die Benutzerkonten auf einem TACACS+-Server verwendet werden sollen. Für den Fall, dass die Zugangsprüfung über das ausgewählte Benutzerkonto mehrmals fehlschlägt, kann eine zweite Anmeldemöglichkeit definiert werden.

- Login Primary: "TACACS" für die Anmeldung über den TACACS+-Server, "Local" für die Anmeldung über die lokalen Benutzerkonten.
- Login Secondary: "TACACS" und "Local" wie oben. Dabei kann nur der Wert ausgewählt werden, der nicht als "Login Primary" eingestellt ist. Mit der zusätzlichen Option "None" kann die sekundäre Anmeldemöglichkeit ausgeschaltet werden.

Der Rückgriff auf lokale Benutzerkonten stellt ein Sicherheitsrisiko dar, wenn kein Root-Kennwort gesetzt ist. Daher kann die TACACS+-Authentifizierung mit Rückgriff auf lokale Benutzerkonten nur aktiviert werden, wenn ein Root-Kennwort definiert ist.

DE

- Access retry: Gibt an, nach wievielen erfolglosen Anmeldeversuchen auf die sekundäre Anmeldemöglichkeit gewechselt werden soll. Wenn TACACS+ als "Login Primary" eingestellt ist, wird nach der eingestellten Anzahl von Fehlversuchen auf dem primären TACACS+-Server zunächst der sekundäre TACACS+-Server verwendet. Erst wenn auch auf diesem Server die maximale Anzahl von Fehlversuchen erreicht wurde, wird die als "Login Secondary" eingestellte Anmeldemöglichkeit verwendet.



Authorization

- State: Aktiviert die Authorisierung über einen TACACS+-Server. Wenn die TACACS+-Authorisierung aktiviert ist, werden alle Authorisierungs-Anfragen über das TACACS+-Protokoll an den konfigurierten TACACS+-Server übertragen.

Im TACACS+-Server kann die Authorisierung für die folgenden Kommandos separat definiert werden:

- 802.1X
- Account
- Alarm
- Autologout
- Bandwidth
- Config-file
- DHCP-boot
- Diagnostics
- Firmware
- GVRP
- Hostname
- IGMP-Snooping

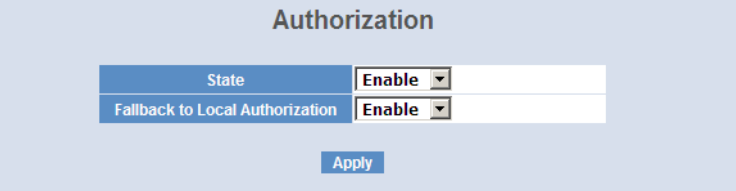
- IP
- Log
- Loop detection
- MAC-table
- Management
- Port
- QoS
- Reboot
- Security
- SNMP
- STP
- System
- TACACS+
- TFTP
- Time
- Trunk
- VLAN
- Virtual Stack.

Für jedes Kommando können die Argumente “show” und “set” separat erlaubt oder gesperrt werden.

Für den Admin-Account müssen alle nicht definierten Kommandos erlaubt werden, z.B. mit den Optionen "Permit Unmatched Commands" und "Permit Unmatched Args" in der Konfiguration des TACACS+-Servers.

Die TACACS+-Authorisierung wird nur dann aktiviert, wenn ein erreichbarer TACACS+-Server definiert ist.
Wenn die TACACS+-Authorisierung aktiviert ist, wird für jedes Kommando beim TACACS+-Server eine Anfrage gestellt, ob der Benutzer diese Aktion ausführen darf. Dementsprechend erhöht sich der Datenverkehr bei der Konfiguration, außerdem müssen die Rechte für die Benutzer im TACACS+-Server definiert sein.
Die Vergabe der Rechte erfolgt hier auf der obersten Menüebene – so kann z.B. der komplette Konfigurationsbereich “Account” für einen Benutzer erlaubt oder gesperrt werden.

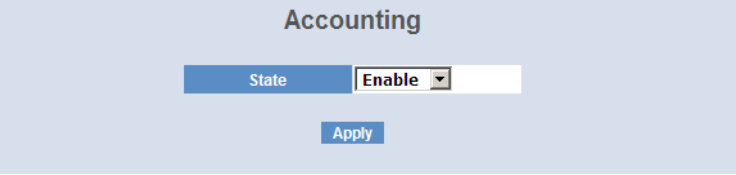
- Fallback to Local Authorization: Aktiviert den Rückfall auf lokale Authorisierungs-Methoden, sollte die Anmeldung über TACACS+ scheitern.



Accounting

- State: Aktiviert das Accounting über einen TACACS+-Server. Wenn das TACACS+-Accounting aktiviert ist, werden alle Accounting-Daten über das TACACS+-Protokoll an den konfigurierten TACACS+-Server übertragen.

Das TACACS+-Accounting wird nur dann aktiviert, wenn ein erreichbarer TACACS+-Server definiert ist.



Bitte beachten Sie, dass bei der Konfiguration über Telnet oder das Webinterface ggf. unterschiedliche Einträge im Accounting für die gleiche Konfiguration zu finden sind. Werden z. B. die Werte für "Location", "Contact" und "Decive Name" über Telnet neu gesetzt, werden im Accounting-Server drei Aktionen verzeichnet. Im Webinterface sind die drei Werte auf einer Webseite zusammengefasst, daher wird auch nur ein Accounting-Eintrag erzeugt.

4.16 Alarm

4.16.1 Events

Events Konfiguration

Die Trap-Event-Konfiguration wird benutzt um den Switch zu veranlassen Trap-Informationen zu senden, wenn bestimmte Trap-Events auftreten.

Sie haben die Möglichkeit zu definieren wie mit 22 verschiedenen Trap-Events umgegangen wird. Die Trap-Informationen über eine aufgetretene Trap können über verschiedene Wege an Sie gesendet werden: Per E-Mail und als Trap an den SNMP-Manager. Die Nachricht wird entsprechend Ihrer Auswahl gesendet.

- Parameter:
  - Trap:

    Cold Start, Warm Start, Link Down, Link Up, Authentication Failure (Authentifizierung gescheitert), User login (Benutzer angemeldet), User logout (Benutzer abgemeldet).
  - STP:

    STP Topology Changed (STP-Topologie geändert), STP Disabled (STP Ausgeschaltet), STP Enabled (STP Eingeschaltet).
  - LACP:

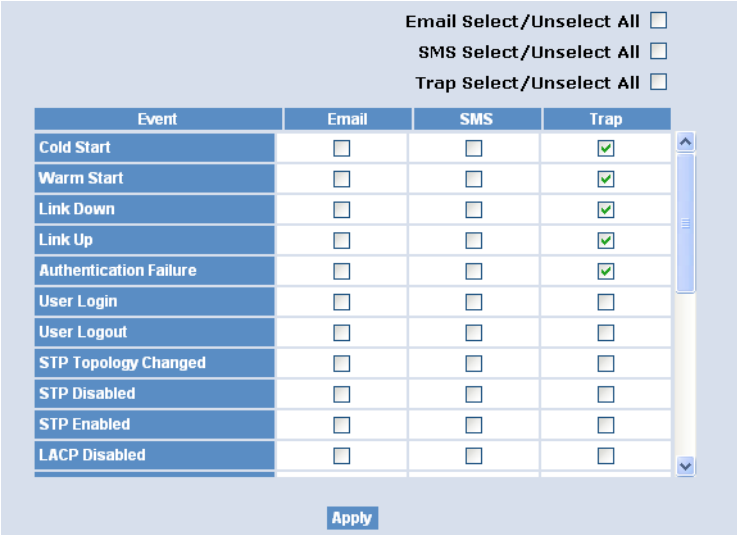
    LACP Disabled (LACP Ausgeschaltet), LACP Enabled (LACP Eingeschaltet), LACP Member Added (LACP Mitglied hinzugefügt), LACP Port Failure (LACP Port-Fehler).
  - GVRP:

    GVRP Disabled (GVRP Ausgeschaltet), GVRP Enabled (GVRP Eingeschaltet).
  - VLAN:

    Port-based VLAN Enabled (Port-basiertes VLAN aktiviert), Tag-based VLAN Enabled (auf Tags basierendes VLAN aktiviert).
  - Module Swap:

    Module Inserted (Modul eingesetzt), Module Removed (Modul entfernt), Dual Media Swapped (Dual Media Port getauscht).
  - PoE:

    PoE Failure (PoE Fehler).



4.16.2 Email

E-Mail

In der Alarmkonfiguration können Sie festlegen, welche Personen über eine aufgetretene Trap per E-Mail informiert werden sollen. Sie können maximal 6 E-Mail-Adressen angeben. Die 22 Trap-Events werden an den SNMP Manager gesendet, sollte eine Trap auftreten. Nach dem Auswählen der Trap-Events können Sie die gewünschten E-Mail-Adressen eintragen. Klicken Sie anschließend <Apply>(Bestätigen) und die neuen Einstellungen werden in wenigen Sekunden übernommen.

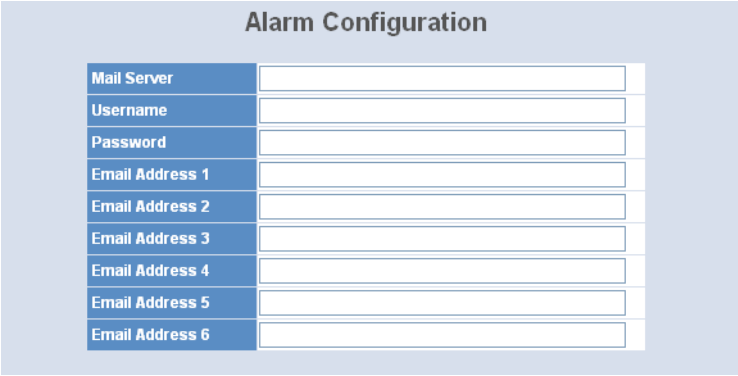
- Parameter:
  - E-Mail:

    Mail Server: Die IP-Adresse des Servers, der ihre E-Mail überträgt.

    Username: Ihr Benutzername auf dem Mail-Server.

    Password: Ihr Passwort auf dem Mail-Server.

    E-Mail Address 1 – 6: E-Mail-Adressen, die die Alarm-Nachricht erhalten sollen.



4.17 Security

Mirror Configuration

Die Mirror Configuration (Spiegelkonfiguration) dient dazu, den Datenverkehr im Netzwerk zu überwachen. Wenn zum Beispiel Port A der überwachende Port und Port B der zu überwachende Port ist, dann wird der Datenverkehr, der bei Port B eintrifft, auf Port A kopiert und überwacht.

- Parameter
  - Mode:

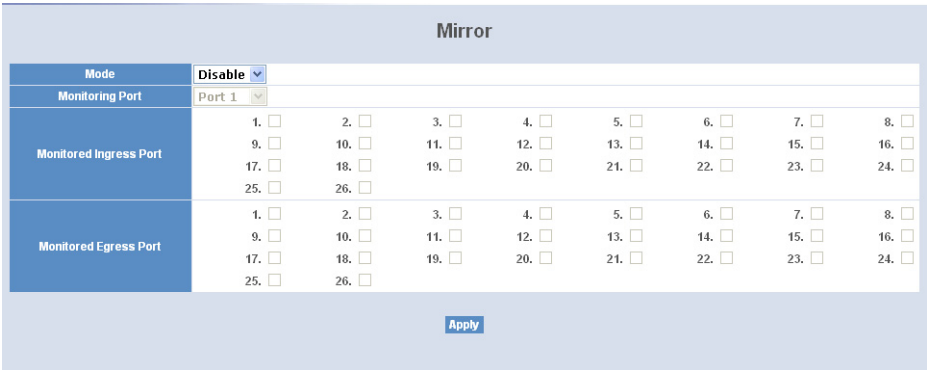
    Aktiviert oder deaktiviert die Port-Spiegel-Funktion. Default ist: Deaktiviert.
  - Monitoring Port:

    Bestimmt den Port, der überwachen soll. Gültige Ports liegen im Bereich von 1 - 26. Default ist Port 1.
  - Monitored Ingress Port:

    Stellt den zu überwachenden Port ein. Es werden nur die empfangenen Pakete des von Ihnen ausgewählten Ports überwacht. Hierfür klicken Sie einfach die Box neben dem ausgewählten Port an. Gültige Ports liegen im Bereich von 1 - 26.
  - Monitored Egress Port:

    Stellt den zu überwachenden Port ein. Es werden nur die gesendeten Pakete des von Ihnen gewählten Ports überwacht. Hierfür klicken Sie einfach die Box neben dem ausgewählten Port an. Gültige Ports liegen im Bereich von 1 - 26.

Function name:



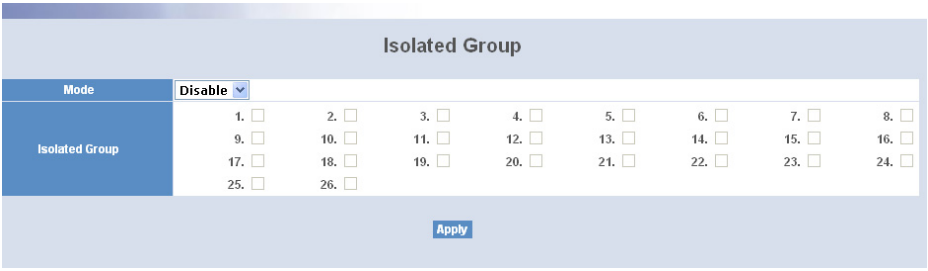
Isolated Group

Die Isolated Group Function (Isolierte Gruppenfunktion) sorgt dafür, dass der Port unabhängig von den anderen Ports in der isolierten Gruppe bleibt, da die Ports nicht miteinander kommunizieren sollen. Die Ports der isolierten Gruppe können jedoch immer noch mit den Ports der nicht isolierten Gruppe kommunizieren. Mit dieser Einstellung kann der Administrator den Port, der Schleifenprobleme im Netzwerk verursacht, sofort finden.

- Parameter
  - Mode:

    Aktiviert oder deaktiviert die Isolated Group Function. Default ist disable.
  - Isolated Group:

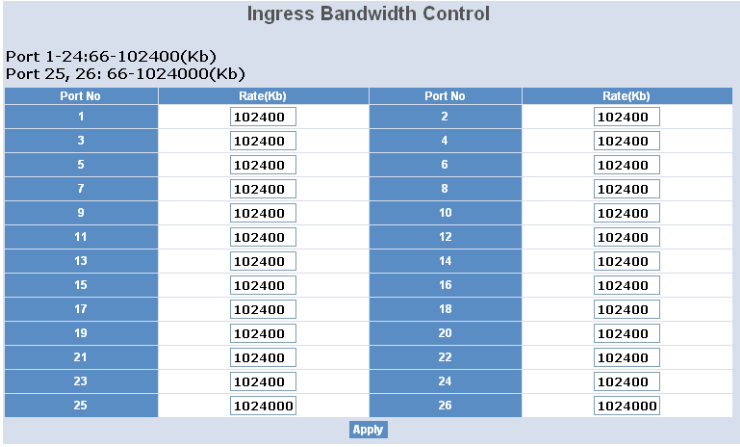
    Sie können jeden Port zu einem Mitglied dieser Gruppe bestimmen. Hierfür klicken Sie einfach die Box neben dem ausgewählten Port an. Gültige Ports liegen im Bereich von 1 - 26. In dieser Gruppe können sich die Mitglieder-Ports untereinander keine Pakete senden. Wenn alle Ports Mitglieder der isolierten Gruppe werden, kann der Switch keine Pakete versenden .



4.18 Bandwidth Management

Ingress Bandwidth Setting

Hier können Sie das Limit der eingehenden Bandbreite für jeden Port einzeln festlegen.



- Parameter
  - Port No.:

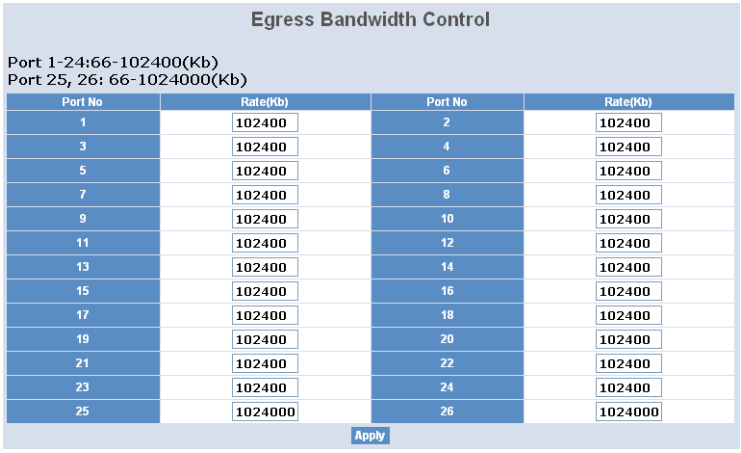
    Suchen Sie hier den Port aus, den Sie einstellen möchten. Sie können alle Ports von 1 bis 26 auswählen.
  - Rate:

    Setzen Sie hier das Limit der eingehenden Bandbreite für den ausgewählten Port. Hereinkommender Datenverkehr wird abgelehnt, sollte die Datenmenge das von Ihnen hier festgelegte Limit übersteigen. Sollten Sie die Flusskontrolle aktiviert haben, werden auch Pause-Fra-

mes generiert. Bei den Ports 1-24 haben Sie die Möglichkeit einen Wert von 66-102.400, bei den Ports 25 und 26 sogar von 66-1.024.000, in Einer-Schritten einzustellen. Die Default-Einstellung für die Ports 1 bis 24 ist 102.400, für Port 25 und 26 ist sie 1.024.000.

Egress Bandwidth Setting

Hier können Sie ein Limit für jeden Port bezüglich der ausgehenden Bandbreite festlegen.



- Parameter
  - Port No.:

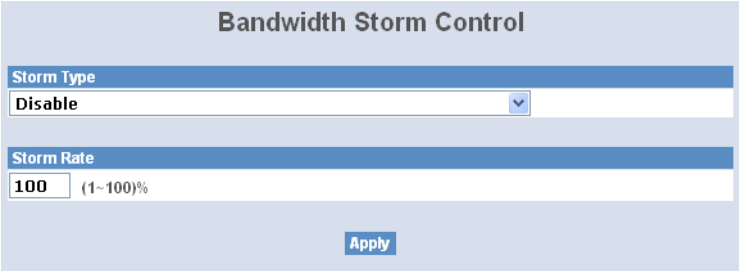
    Wählen Sie hier den Port aus, auf den Sie das Limit anwenden möchten.
  - Rate:

    Legen Sie hier das Limit für die ausgehende Bandbreite für diesen Port fest. Wenn die Datenmenge das Limit übersteigt, setzt das Senden von Paketen aus. Wenn die ausgehenden Puffer voll sind, können Daten verloren gehen. Das Format der Pakete ist auch hier auf Unicast, Broadcast und Multicast festgelegt. Die Ports 1 bis 24 unterstützen ein Limit von 66-102.400, die Ports 25 und 26 sogar von 66-1.024.000. Sie können die Einstellung in Einer-Schritten verändern. Die Default-Einstellung ist bei den Ports 1 bis 24 bei 102.400, und bei den Ports 25 und 26 entsprechend 1.024.000.

DE

Storm Setting

Mit der Funktion "Strom Control" können Sie einen gemeinsamen Grenzwert für den zulässigen Anteil der Brodcast-, Multicast- oder Unicast-Pakete am gesamten Traffic definieren. Wenn dieser Grenzwert erreicht wird, werden die Datenpakete des entsprechenden Typs verworfen. Die Storm Control kann für die einzelnen Typen separat aktiviert werden.



- Parameter
  - Storm Type:

    Disable:

    Schalten Sie die "Storm-Control"(Datenflut-Schutz) hier aus.

    Broadcast Storm Control:

    Aktivieren Sie die Bandbreiten-Storm-Control für Broadcast-Pakete.

    Multicast Storm Control:

    Aktivieren Sie die Bandbreiten-Storm-Control für Multicast-Pakete.

    Unknown Unicast Storm Control:

    Aktivieren Sie die Bandbreiten-Storm-Control für unbekannte Unicast-Pakete. Diese Packete sind MAC-Adressen, die den Lernprozess noch nicht abgeschlossen haben.

    Broadcast, Multicast, Unknown Unicast Storm Control:

    Hier können Sie die Storm-Control für Broadcast, Multicast und Unknown Unicast-Pakete einschalten.

  - Storm Rate:

    Hier können Sie ein Bandbreiten-Limit in Prozent der maximalen Bandbreite der Ports festlegen. Wenn die Storm Rate z.B. auf 15% festgelegt wird, werden die für Strom Control aktivierten Pakete ver-

worfen, sobald an dem Port 15% der maximalen Bandbreite durch Broadcast, Multicast bzw. Unknown Unicast verursacht werden (bei einem Port mit maximal 100 MBit/s also 15 MBit/s).

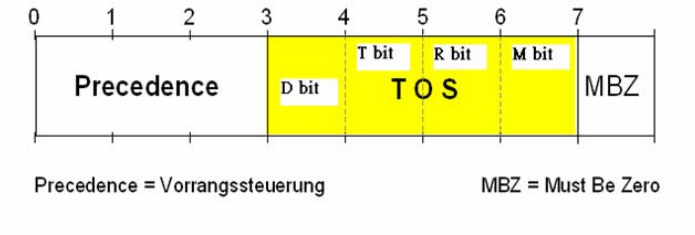
Zugelassene Einstellungen sind zwischen 1 und 100 Prozent. Nur ganze Werte sind möglich und die Default-Einstellung beträgt 100.

DE

4.19 QoS (Quality of Service) Configuration

Der Switch unterstützt fünf Arten des QoS (Quality of Service), darunter fallen die MAC-Priorität, die 802.1p-Priorität, die IP-TOS-Priorität und die DiffServ-DSCP-Priorität. Die Port-Based-Priorität hat im Switch den Namen VIP-Port. Jedes Paket, das zum VIP-Port gelangt, erhält die höchste Übertragungspriorität. Die MAC-Priorität wird durch die MAC-Zieladresse der Pakete bestimmt. Das VLAN-Tagged-Prioritätsfeld wird von der Einstellung der 802.1p Priorität beeinflusst. Die IP-TOS-Priorität beeinflusst TOS-Felder des IP-Headers und stellt Ihnen ein 8-bit Service-Type-Feld zur Verfügung, welches genauere Angaben darüber macht, wie mit dem Datagram umgegegangen werden soll. Das Feld kann in sechs Unterfelder aufgeteilt werden: PRECEDENCE (3 Bits), D-Type (Verzögerungspriorität, 1 Bit), T-Type (Durchflusspriorität, 1 Bit), R-Type (Betriebssicherheitspriorität, 1 Bit), M-Type (Finanzielle Priorität, 1Bit), und UNUSED (1 Bit).

Sie können diese Felder kontrollieren, um spezielle QoS-Ziele zu erreichen. Wenn Sie die Bits D, T, R oder M einstellen, erfordert das D-Bit eine niedrige Verzögerung, das T-Bit eine hohe Durchflussleistung, das R-Bit eine hohe Verlässlichkeit und das M-Bit niedrige Kosten.



DiffServ-DSCP-Priorität arbeitet an dem DSCP-Feld des IP-Header. In den späten Neunzigern definierte die IETF (Internet Engineering Task Force) die Bedeutung des 8-Bit Service-Type-Feldes neu, um eine Anzahl von differenzierten Diensten (DS= differentiated services) unterzubringen. Die ersten

sechs Bits dieser DS-Interpretation bestehen aus einem Codepoint, welcher manchmal mit DSCP abgekürzt wird. Die letzten beiden Bits bleiben ungenutzt.

Datenströme mit Paketen hoher Priorität werden im Switch weniger verzögert. Um mit verschiedenen Prioritäten von Paketen umzugehen, hat jeder Ausgangsport bis zu vier Warteschlangen. Jeder QoS ist beeinflusst von zwei Planungen: WRR (Weighted Round Robin) und Strict-Priorität. Wenn Sie die Einstellungen der Prioritätenverteilung der Warteschlangen beendet haben, wird die WRR-Planung gemäß der von Ihnen eingestellten Gewichtung der vier Warteschlangen die Bandbreite verteilen (Warteschlange 0 bis Warteschlange 3). Eine andere Planungsmethode ist die Strict-Priorität. Diese ist für die VIP-Port-Funktion des QoS bestimmt. Die Ports, die Sie zu VIP-Ports bestimmen, werden in der ausgehenden Warteschlange des Switches die höchste Übertragungspriorität bekommen.

Die QoS-Funktionen können zur selben Zeit aktiv sein. Beachten Sie dabei die folgenden Einstellungen der einzelnen Funktionen:

1. Wenn VIP und TOS aktiv sind, müssen Sie die Prioritäten für beide Funktionen festlegen.
2. Wenn VIP und DSCP aktiv sind, müssen Sie die Prioritäten für beide Funktionen festlegen.
3. Wenn TOS und DSCP aktiv sind, müssen Sie DSCP wählen.
4. Wenn 802.1p und TOS aktiv sind, wählen Sie TOS.
5. Wenn 802.1p und DSCP aktiv sind, wählen Sie DSCP.
6. Wenn 802.1p und TOS aktiv sind, wählen Sie DSCP.
7. Wenn 802.1p, DSCP, TOS und VIP aktiv sind, müssen Sie die Prioritäten für VIP und DSCP festlegen.

   VIP/DSCP > TOS > 802.1p (Endgültiges Ergebnis)

QoS Global Setting

Wenn Sie die QoS-Funktion nutzen wollen, aktivieren Sie zunächst den QoS-Modus. Anschließend können Sie die MAC-Priorität, die 802.1p-Priorität, die IP-TOS-Priorität, die DiffServ-DSCP-Priorität oder VIP-Port-Funktionen benutzen. Wählen Sie eine Prioritäten-Kontrolle, wie zum Beispiel 802.1p, TOS oder DSCP. Desweiteren können Sie die Warteschlangen-Methode des WRR oder der Strict-Priorität auswählen. Danach können Sie die Gewichtung der Warteschlangen null bis drei bestimmen.

DE

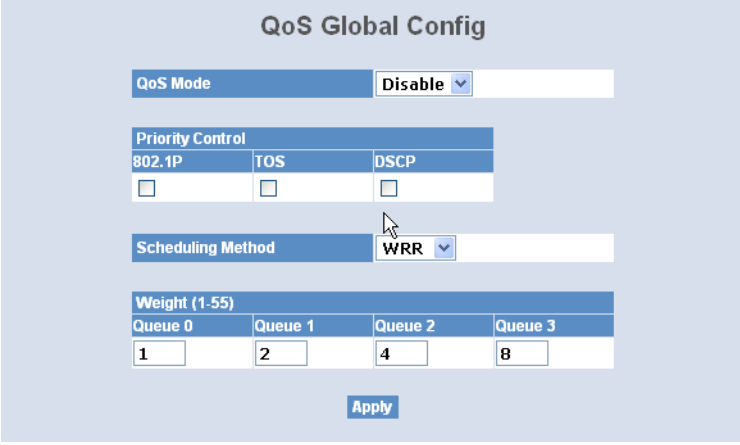
- Parameter
  - QoS Mode:

    Sie können den QoS-Modus und damit die QoS-Funktion aktivieren. Default ist disable.
  - Priority Control:

    Setzen Sie ein Häkchen in die Check-Box von 802.1p, TOS oder DSCP-QoS und klicken Sie den Apply-Button, um die Einstellungen zu übernehmen.
  - Scheduling Method:

    Es gibt zwei Planungsmethoden: WRR und Strict-Priorität. Default ist WRR. Nachdem Sie eine der Planungsmethoden gewählt haben, müssen Sie den Apply-Button drücken, um die Einstellung zu übernehmen.
  - Weight (1-55):

    Hier können Sie die Gewichtung der Warteschlangen null bis drei einstellen. Der Bereich der Werte für die Gewichtung liegt zwischen 1-55. Default des Wertes der Warteschlange null ist eins, der Warteschlange eins ist zwei, der Warteschlange zwei ist vier und der Warteschlange drei ist acht.



VIP Port Setting

Die ausgehenden Pakete haben die höchste Übertragungspriorität, wenn ein Port als VIP Port eingestellt ist. Diese Pakete werden bevorzugt zuge-

stellt. Wählen Sie die Methode der Strict-Priorität, um diese Funktion bestmöglich zu nutzen.

Beispiel:

Normalerweise werden Pakete von Port 2 und 3 gleichzeitig zu Port 1 übertragen. Dadurch kann Stau entstehen. Wenn Sie Port 2 als VIP-Port wählen, werden die Pakete von Port 3 fallen gelassen, weil die Pakete von Port 2 Vorrang haben.

- Parameter:
  - VIP Port:

    Setzen Sie ein Häkchen in die Check-Box um einen Port (1-26) zum VIP-Port zu bestimmen. Klicken Sie anschließend den Apply-Button um die Einstellungen zu übernehmen.

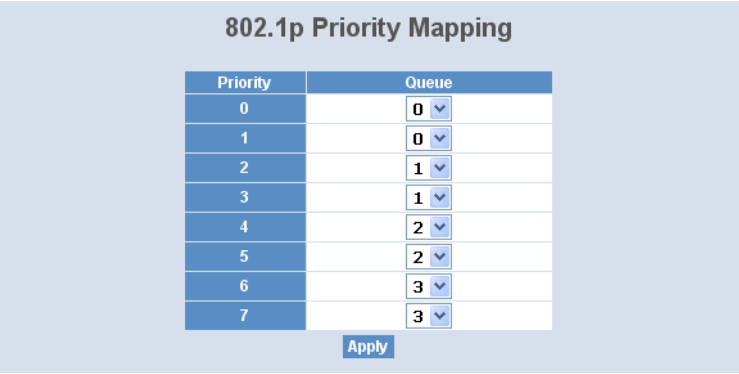
802.1p Setting

Mit dieser Einstellung können Sie die Priorität eines bestimmten VLAN-Tags setzen. Sie können eine Priorität zwischen 1 und 8 vergeben, die wieder auf 4 Warteschlangen (Queue 0-3) verweisen und einen anderen Anteil der Bandbreite innehaben, je nachdem welche Gewichtung eine Warteschlange innehat.

- Parameter:
  - 802.1p Priority Mapping:

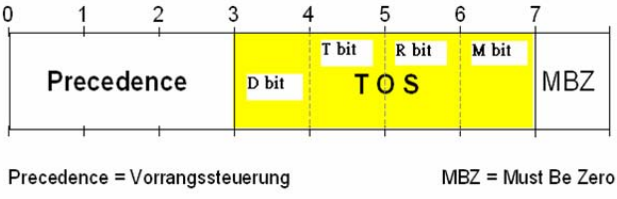
    Sie können jede Priorität einer bestimmten Warteschlange zwischen 0 und 3 zuordnen. In der Default-Einstellung sind Prioritäten 0 und 1 der Warteschlange 0 zugeordnet, die Prioritäten 2 und 3 zu Warteschlange 1, Prioritäten 4 und 5 zu Warteschlange 2 und Prioritäten 6 und 0 zu Warteschlange 3.

DE



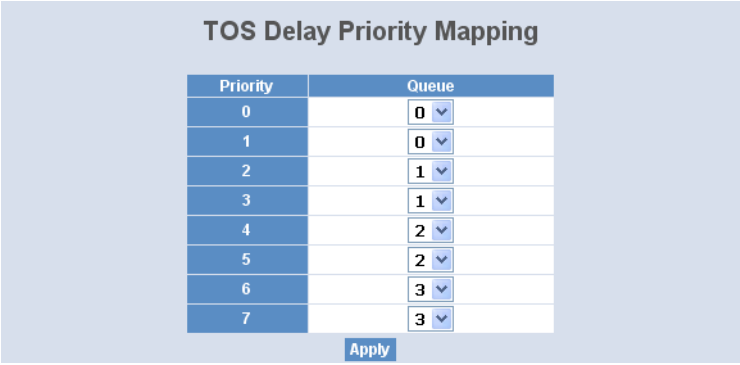
D-Type TOS

Die IP-TOS-Priorität beeinflußt Werte im Header eines Datenpaketes in Form des 8-Bit SERVICE TYPE Feldes. Dieses gibt an, wie ein Datagramm behandelt werden sollte und lässt sich in sechs Typen von Sub-Feldern unterteilen, die wie folgt lauten: PRECEDENCE (3 Bits), D-Typ (Delay Priority (Verzögerungs-Priorität), 1 Bit), T-Typ (Throughput Priority (Durchsatz-Priorität), 1 Bit), R-Typ (Reliability Priority (Verlässlichkeits-Priorität), 1 Bit), M-Typ (Monetary Cost Priority (Verbindungskosten-Priorität), 1 Bit) und UNUSED. Das PRECEDENCE-Feld kann acht Prioritäten aus dem folgenden Prioritäten-Diagramm zuordnen. Das TOS-Delay-Priority-Mapping (Mapping nach Verzögerungs-Priorität) funktioniert nur, wenn im Header einer Nachricht im T-Typ-Feld ein Wert gegeben wird.



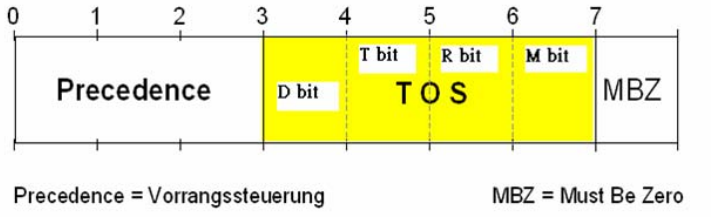
- Parameter:
  - TOS Delay Priority Mapping:

    Sie können jede Priorität einer bestimmten Warteschlange zwischen 0 und 3 zuordnen. In der Default-Einstellung sind Prioritäten 0 und 1 der Warteschlange 0 zugeordnet, die Prioritäten 2 und 3 zu Warteschlange 1, Prioritäten 4 und 5 zu Warteschlange 2 und Prioritäten 6 und 0 zu Warteschlange 3.



T-Type TOS

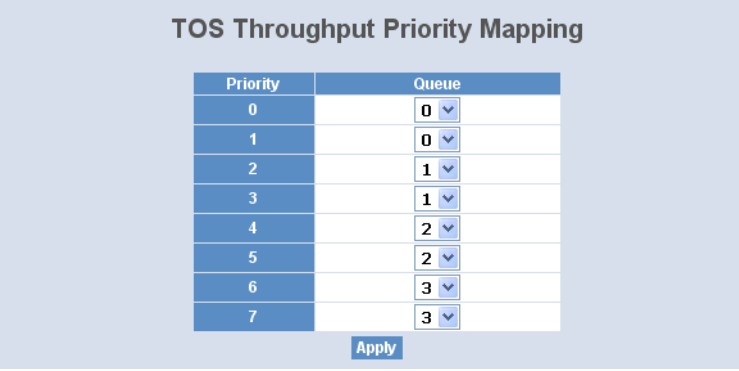
Die IP-TOS-Priorität beeinflußt Werte im Header eines Datenpaketes in Form des 8-Bit SERVICE TYPE Feldes. Dieses gibt an wie ein Datagramm behandelt werden sollte. Dieses Feld lässt sich in sechs Typen von Sub-Feldern unterteilen, die wie folgt lauten: PRECEDENCE (3 Bits), D-Typ (Delay Priority (Verzögerungs-Priorität), 1 Bit), T-Typ (Throughput Priority (Durchsatz-Priorität), 1 Bit), R-Typ (Reliability Priority (Verlässlichkeits-Priorität), 1 Bit), M-Typ (Monetary Cost Priority (Verbindungskosten-Priorität), 1 Bit) und UNUSED. Das PRECEDENCE-Feld kann acht Prioritäten aus dem folgenden Prioritäten-Diagramm zuordnen. Das TOS-Throughput-Priority-Mapping (Mapping nach Durchsatz-Priorität) funktioniert nur, wenn im Header einer Nachricht im T-Typ-Feld ein Wert gegeben wird.



- Parameter:
  - TOS Throughput Priority Mapping:

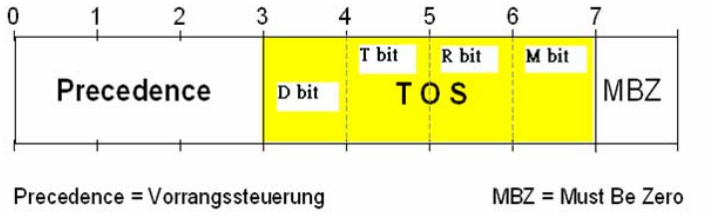
    Sie können jede Priorität einer bestimmten Warteschlange zwischen 0 und 3 zuordnen. In der Default-Einstellung sind Prioritäten 0 und 1 der Warteschlange 0 zugeordnet, die Prioritäten 2 und 3 zu Warte-

schlange 1, Prioritäten 4 und 5 zu Warteschlange 2 und Prioritäten 6 und 0 zu Warteschlange 3.



- R-Type TOS

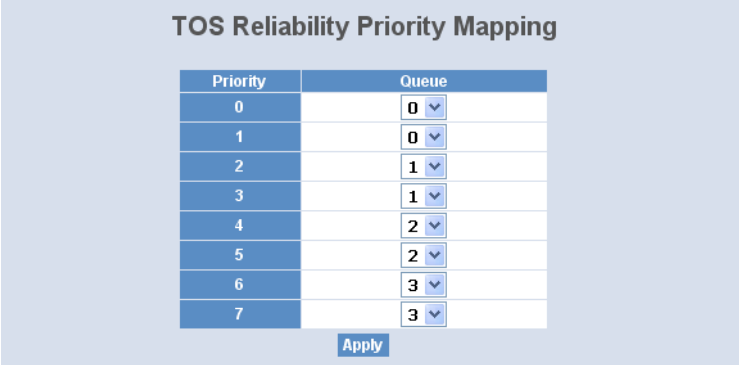
  Die IP-TOS-Priorität beeinflußt Werte im Header eines Datenpaketes in Form des 8-Bit SERVICE TYPE Feldes. Dieses gibt an wie ein Datagramm behandelt werden sollte. Dieses Feld lässt sich in sechs Typen von Sub-Felder unterteilen, die wie folgt lauten: PRECEDENCE (3 Bits), D-Typ (Delay Priority (Verzögerungs-Priorität), 1 Bit), T-Typ (Throughput Priority (Durchsatz-Priorität), 1 Bit), R-Typ (Reliability Priority (Verlässlichkeits-Priorität), 1 Bit), M-Typ (Monetary Cost Priority (Verbindungskosten-Priorität), 1 Bit) und UNUSED. Das PRECEDENCE-Feld kann acht Prioritäten aus dem folgenden Prioritäten-Diagramm zuordnen. Das TOS-Reliability-Priority-Mapping (Mapping nach Verlässlichkeit-Priorität) funktioniert nur, wenn im Header einer Nachricht im R-Typ-Feld ein Wert gegeben wird.



- Parameter:
  - TOS Reliability Priority Mapping:

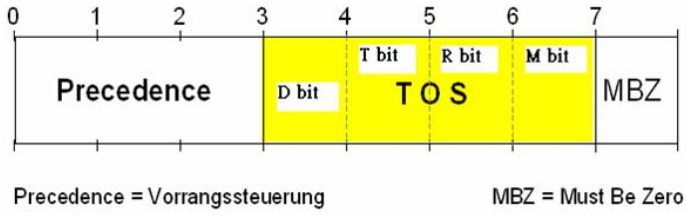
    Sie können jeder Priorität einer bestimmten Warteschlange zwischen 0 und 3 zuordnen. In der Default-Einstellung sind Prioritäten 0 und 1

der Warteschlange 0 zugeordnet, die Prioritäten 2 und 3 zu Warteschlange 1, Prioritäten 4 und 5 zu Warteschlange 2 und Prioritäten 6 und 0 zu Warteschlange 3.



M-Type TOS

Die IP-TOS-Priorität beeinflußt Werte im Header eines Datenpaketes in Form des 8-Bit SERVICE TYPE Feldes. Dieses gibt an wie ein Datagramm behandelt werden sollte. Dieses Feld lässt sich in sechs Typen von Sub-Felder unterteilen, die wie folgt lauten: PRECEDENCE (3 Bits), D-Typ (Delay Priority (Verzögerungs-Priorität), 1 Bit), T-Typ (Throughput Priority (Durchsatz-Priorität), 1 Bit), R-Typ (Reliability Priority (Verlässlichkeits-Priorität), 1 Bit), M-Typ (Monetary Cost Priority (Verbindungskosten-Priorität), 1 Bit) und UNUSED. Das PRECEDENCE-Feld kann acht Prioritäten aus dem folgenden Prioritäten-Diagramm zuordnen. Das TOS-Monetary-Cost-Priority-Mapping (Mapping nach Pfadkosten-Priorität) funktioniert nur, wenn im Header einer Nachricht im M-Typ-Feld ein Wert gegeben wird.

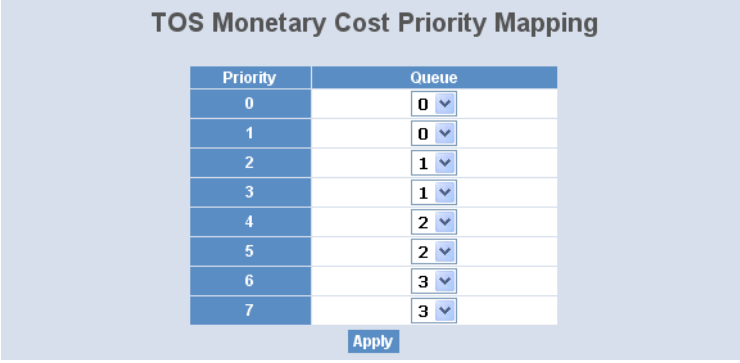


- Parameter:

DE

- TOS Monetary Cost Priority Mapping:

  Sie können jede Priorität einer bestimmten Warteschlange zwischen 0 und 3 zuordnen. In der Default-Einstellung sind Prioritäten 0 und 1 der Warteschlange 0 zugeordnet, die Prioritäten 2 und 3 zu Warteschlange 1, Prioritäten 4 und 5 zu Warteschlange 2 und Prioritäten 6 und 0 zu Warteschlange 3.



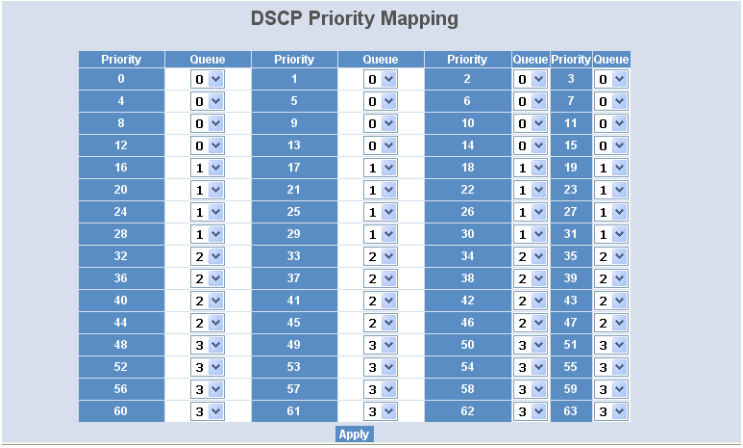
DSCP Setting

In den späten 90er Jahren des letzten Jahrtausends hat die IETF die Bedeutung des 8-Bit "SERVICE TYPE"-Feldes neu definiert um eine Anzahl neuer differenzierter Dienste aufzunehmen. Nach dieser Interpretation sind die ersten 6 Bit ein Codepoint, auch DSCP genannt. Die beiden letzten Bits bleiben unbenutzt.

Dabei kann der DSCP 64 Datenverkehrs-Klassen basierend auf den Kombinationen der Werte in diesen ersten 6 Bits definieren. Sie können jeder dieser 64 Klassen einer Warteschlange von 0 bis 3 zuweisen.

- Parameter:
  - DSCP Priority Mapping:

    Hier können Sie den oben erwähnten Klassen einer Warteschlange zuordnen. In der Default-Einstellung sind die Prioritäten 0-15 der Warteschlange 0, die Prioritäten 16-31 der Warteschlange 1, die Prioritäten 32-47 der Warteschlange 0 und die Prioritäten 48-63 ebenfalls der Warteschlange 0 zugeordnet.



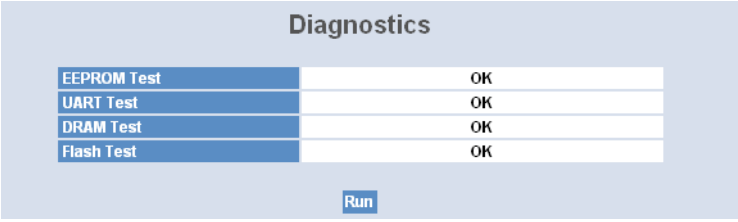
4.20 Diagnostics

Dieses Kapitel beschreibt die Funktionen zur Selbstdiagnose. Jede von ihnen wird im Folgenden der Reihe nach beschrieben.

4.20.1 Diag

Diagnostics

Sie finden hier eine Reihe von grundsätzlichen Systemdiagnose-Werkzeugen. Die EEPROM-, UART-, DRAM- und Flash-Tests sollen Ihnen bei der Entscheidung helfen, ob ein System reparaturbedürftig ist oder nicht.



4.20.2 Loopback

Loopback Test

Es gibt zwei Loopback-Tests: Einen internen und einen externen Test. Bei der internen Testlösung wird das Testsignal den Switch nicht verlassen, während bei dem externen Test ein Signal an verbundene Geräte gesendet

wird. Sollten Sie den Switch nicht mit aktiven Netzwerkgeräten verbunden haben, d.h. die Ports sind "link down", wird der externe Test auf diesen Ports als gescheitert gemeldet.

Hinweis: Egal welche Testmethode Sie wählen, beide Diagnosewerkzeuge werden den normalen Systembetrieb stören. Alle gesendeten und empfangenen Packete werden temporär gestoppt.

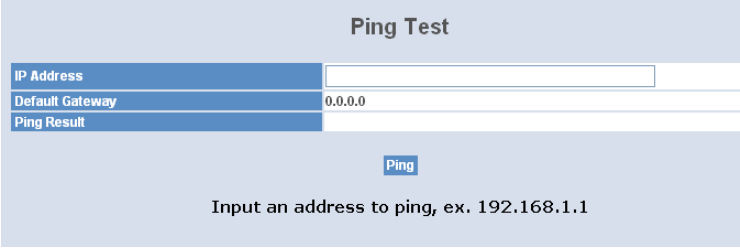
4.20.3 Ping

Ping Test

Mit dem Ping-Test können Sie durch das ICMP-Protokoll feststellen ob ein Zielgerät aktiv ist oder nicht. Geben Sie einfach eine Ihnen bekannte IP-Adresse ein und klicken Sie den <Ping>-Button. Anschließend wird Ihnen das Resultat des Tests zeigen ob das Zielgerät erreichbar ist.

- Parameter

- IP Address:
  Eine IP-Adresse der Version IPv4, also z. B. 192.168.1.1.
- Default Gateway:
  Die IP-Adresse des Default-Gateway.



4.20.4 Watchdog

- Watchdog
  Mit dem Watchdog kann überprüft werden, ob ein Netzwerkgerät noch erreichbar ist. Dazu wird regelmäßig ein Ping auf eine IP-Adresse gesendet.

Wenn nur ein Ping erfolgreich beantwortet wurde und dann alle folgenden Pings unbeantwortet bleiben, wird der Zähler zurückgesetzt und neu gestartet.

- Parameter
  - State:
    Schaltet die Watchdog-Funktion ein oder aus. Default: Disable.
  - Time Gap:
    Zeitlicher Abstand zwischen zwei Pings. Eingabe in Sekunden von 1 bis 100. Default: 10 Sekunden.
  - Host:
    IP-Adresse des Netzwerk-Geräts, an das der Ping gesendet werden soll.
  - Reset the management CPU Interface:
    Wenn die maximale Anzahl von Fehlern (nicht beantwortete Pings) erreicht wird, kann die CPU des Switches neu gestartet werden. Mit

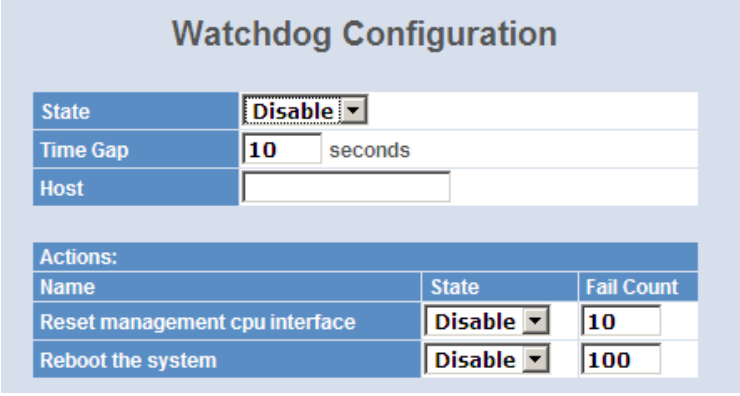
diesem Schalter aktivieren oder deaktivieren Sie diese Funktion. Default: Disable.

Fail Count: Grenzwert für den Neustart der CPU, Werte von 1 bis 20. Default: 10.

- Reboot the system:

  Wenn die maximale Anzahl von Fehlern (nicht beantwortete Pings) erreicht wird, kann der Switch neu gestartet werden. Mit diesem Schalter aktivieren oder deaktivieren Sie diese Funktion. Default: Disable.

  Fail Count: Grenzwert für den Neustart der CPU, Werte von 1 bis 1000. Default: 100.



4.21 TFTP Server

TFTP Server

Stellt eine IP-Adresse für den TFTP-Server ein.

- Parameter

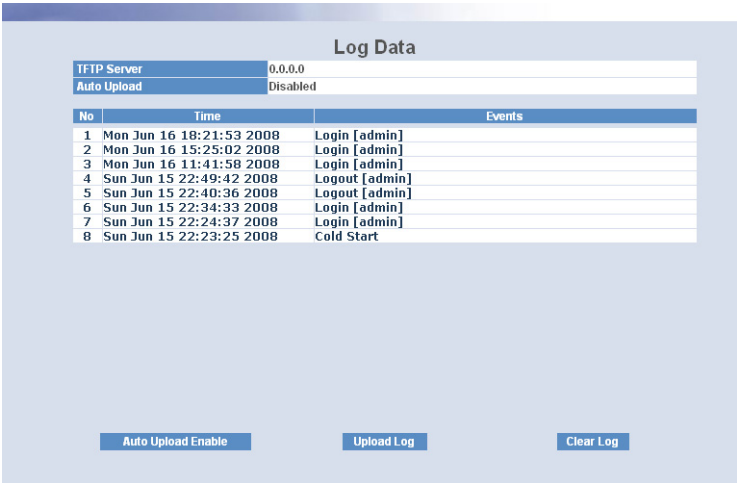
  Bestimmt die IP-Adresse des TFTP-Servers. Geben Sie die IP-Adresse Ihres TFTP-Servers ein und drücken Sie den <Apply> Button, um die Einstellungen zu übernehmen.

4.22 Log

Diese Funktion zeigt Ihnen die Log-Daten (Daten des Protokolls), die der Switch für den Benutzer bereitstellt. Es gibt 17 private Trap-Logs und 5 öffentliche Trap-Logs. Insgesamt stellt der Switch 120 Log-Einträge zur Verfügung. Mehr Details zu Log-Einträgen finden Sie in den Kapiteln über die Trap/ Alarm Konfiguration und die SNMP Konfiguration.

Log Data

Die Trap-Log-Angabe zeigt die Log-Einträge der "SNMP Private Trap events", "SNMP Public Traps" und die Benutzer-Logs die im System auftreten. In der Reporttabelle befinden sich drei Felder mit der Nummer, dem Zeitpunkt und dem Ereignis des Trap-Protokolls.



- Parameter
  - No.:

    Gibt die Ordnungsnummer des Traps an.

- Time:
  Gibt den Zeitpunkt an, wann der Trap stattgefunden hat
- Events:
  Gibt den Namen des Trap-Ereignisses an.
- Auto Upload Enable:
  Wechselt den aktiven oder deaktiven Status der Auto-Upload-Funktion.
- Upload Log:
  Führt einen Upload der Log-Daten mit Hilfe von tftp durch.
- Clear Log:
  Entfernt die Log-Daten.

4.23 Firmware Upgrade

Diese Funktion hilft Ihnen ein Upgrade der Software durchzuführen, um eine Funktion zu reparieren oder zu verbessern. Der Switch stellt einen TFTP-Klienten zur Verfügung, um ein Upgrade der Software durchzuführen. Sie können dies mit Hilfe des Ethernet bewerkstelligen.

Firmware Upgrade

Der Switch unterstützt das Software-Upgrade über TFTP. Wenn Sie ein Software-Upgrade durchführen, durchlaufen Sie zwei Schritte:

1. Geben Sie die IP-Adresse Ihres TFTP-Servers in das entsprechende Feld ein.

2. Bestimmen Sie den vollständigen Pfad und den Dateinamen. Klicken Sie dann die <Upgrade> -Schaltfläche. Sollte Ihr Download nicht erfolgreich sein, wird der Switch zu dem Punkt "Software upgrade" zurückkehren und das Software-Upgrade nicht ausführen.

   Wenn der Download erfolgreich abgeschlossen ist, beginnt der Switch mit dem Software-Upgrade. Eine Reboot-Nachricht wird nach dem Abschluss des Software-Upgrades erscheinen. Anschließend müssen Sie den Switch neu starten, damit die neue Software funktionstüchtig ist.

   Hinweis: Sorgen Sie dafür, dass die Stromversorgung während des Software-Updates keinesfalls unterbrochen wird.

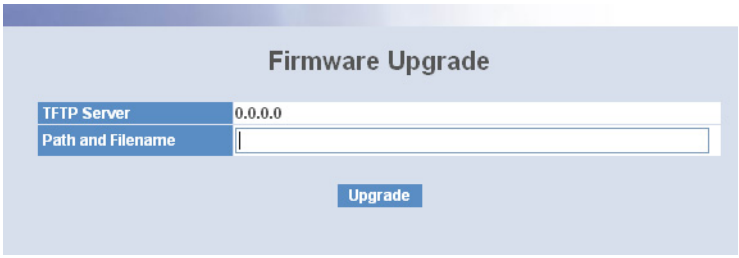
- Parameter

- TFTP Server:

  Auf dem TFTP-Server liegt die Datei, mit der Sie ein Upgrade durchführen wollen.

- Path and Filename:

  Der Dateipfad der Datei, mit der Sie ein Upgrade durchführen wollen.



4.24 Reboot

Sie können den Reset-Button in der Vorderfront des Switches betätigen, um den Switch neu zu starten. Nachdem Sie ein Software-Upgrade durchgeführt, die IP-Konfiguration oder die VLAN-Modus-Konfiguration verändert haben, müssen Sie den Switch neu starten um die veränderten Einstellungen zu übernehmen. Diesen Neustart können Sie alternativ zum Reset-Button mit Hilfe der Reboot-Funktion aus dem Hauptmenü vornehmen.

Reboot

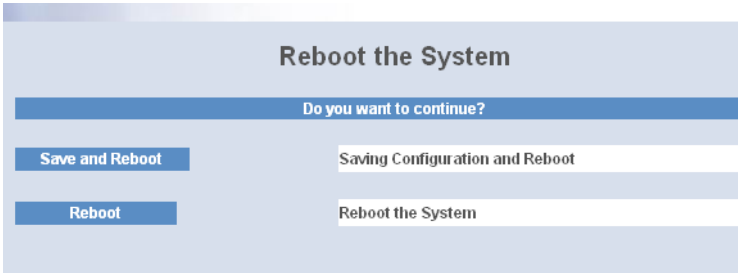
Starten Sie den Switch neu. Der Reboot hat die gleichen Auswirkungen, wie das Drücken des Reset-Buttons in der Vorderfront des Switches. Es wird ca. 30 Sekunden dauern, bis das System den Boot-Vorgang abgeschlossen hat.

- Parameter
  - Save and Reboot:

    Speichert die aktuellen Einstellungen als Startkonfiguration, bevor der Switch neu gestartet wird.

  - Reboot:

    Startet das System direkt neu.



4.25 Logout

Sie können sich mit der Logout-Funktion manuell abmelden. Sie können den Switch jedoch auch so einstellen, dass er Sie automatisch abmeldet.

Logout

Die Logout-Funktion verhindert, dass unbefugte Benutzer Zugriff auf das System haben. Wenn Sie sich nicht abmelden und den Browser verlassen, meldet der Switch Sie automatisch ab. Neben dem manuellen und impliziten Logout, können Sie den automatischen Logout ein- oder ausschalten. Der <Auto Logout> befindet sich auf der Bildschirmoberfläche rechts oben.

- Parameter:
  - Auto Logout:

    Wenn die Auto-Logout-Funktion eingeschaltet ist ("ON") und es findet über einen Zeitraum von drei Minuten weder eine Tastenbetätigung, noch eine Bildschirmbewegung statt, wird der Switch Sie automatisch abmelden. Default ist ON.

DE

5 Operation of CLI Management (englisch)

5.1 CLI Management

Refer to Chapter 2 for basic installation. The following description is the brief of the network connection.

-- Locate the correct DB-9 null modem cable with female DB-9 connector. Null modem cable comes with the management switch. Refer to the Appendix B for null modem cable configuration.

-- Attach the DB-9 female connector to the male DB-9 serial port connector on the Management board.

-- Attach the other end of the DB-9 cable to an ASCII terminal emulator or PC Com-1, 2 port. For example, PC runs Microsoft Windows HyperTerminal utility.

-- At "Com Port Properties" Menu, configure the parameters as below: (see the next section)

Baud rate	57600
Stop bits	1
Data bits	8
Parity	N
Flow control	none

5.1.1 Login

The command-line interface (CLI) is a text-based interface. User can access the CLI through either a direct serial connection to the device or a Telnet session. The default values of the managed switch are listed below:

Username: admin

Password: admin

After you login successfully, the prompt will be shown as "**#**" if you are the first login person and your authorization is administrator; otherwise it may show "**$**". See the following two figures. The former means you behave as an administrator and have the access right of the system. As to the latter, it means you behave as a guest and are only allowed to view the system without the permission to do any setting for this switch.

DE

```
Managed Switch - PSES-2126C

Login: admin
Password:

PSES-2126C#
```

Fig. 4-1

```
Managed Switch - PSES-2126C

Login: admin
Password:

PSES-2126C$
```

Fig. 4-2

5.2 Commands of CLI

```
Managed Switch - PSES-2126C

Login: admin
Password:

PSES-2126C# ?
  802.1X                Enter into 802.1X mode
  account               Enter into account mode
  alarm                 Enter into alarm mode
  autologout            Change autologout time
  bandwidth             Enter into bandwidth mode
  config-file           Enter into config file mode
  dhcp-boot             Enter into dhcp-boot mode
  diag                  Enter into diag mode
  firmware              Enter into firmware mode
  gvrp                  Enter into gvrp mode
  hostname              Change hostname
  igmp-snooping         Enter into igmp mode
  ip                    Enter into ip mode
  log                   Enter into log mode
  mac-table             Enter into mac table mode
  management            Enter into management mode
  poe                   Enter into PoE function
  port                  Enter into port mode
```

Fig. 4-3

5.2.1 Global Commands of CLI

- **end**
  - Syntax:

    end
  - Description:

    Back to the top mode.

    When you enter this command, your current position would move to the top mode. If you use this command in the top mode, you are still in the position of the top mode.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

    PSES-2126C# alarm

    PSES-2126C(alarm)# events

    PSES-2126C(alarm-events)# end

    PSES-2126C#
- **exit**
  - Syntax:

    exit
  - Description:

    Back to the previous mode.

    When you enter this command, your current position would move back to the previous mode. If you use this command in the top mode, you are still in the position of the top mode.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

    PSES-2126C# trunk

```
PSES-2126C(trunk)# exit
PSES-2126C#
```

- **help**
  - Syntax:

help

  - Description:

To show available commands.

Some commands are the combination of more than two words. When you enter this command, the CLI would show the complete commands. Besides, the command would help you classify the commands between the local commands and the global ones.

  - Argument:

None.

  - Possible value:

None.

  - Example:

```
PSES-2126C# ip
PSES-2126C(ip)# help
Commands available:
  ------------<< Local commands >>------------
  set ip               Set ip and gateway
  set dns              Set dns
  enable dhcp          Enable DHCP, and set dns auto or
manual
  disable dhcp         Disable DHCP
  show                 Show IP Configuration
  ------------<< Global commands >>------------
  exit                 Back to the previous mode
  end                  Back to the top mode
  help                 Show available commands
  history                Show a list of previously run
commands
```

```
  logout                Logout the system
  save start            Save as start config
  save user             Save as user config
  restore default       Restore default config
  restore user          Restore user config
PSES-2126C(ip)#
```

DE

- **history**
  - Syntax:

    history [#]
  - Description:

    To show a list of previous commands that you had ever run.

    When you enter this command, the CLI would show a list of commands which you had typed before. The CLI supports up to 256 records. If no argument is typed, the CLI would list total records up to 256. If optional argument is given, the CLI would only show the last numbers of records, given by the argument.
  - Argument:

    [#]: show last number of history records. (optional)
  - Possible value:

    [#]: 1, 2, 3, …., 256
  - Example:

```
PSES-2126C(ip)# history
 Command history:
  0. ?
  1. trunk
  2. exit
  3. PSES-2126C# trunk
  4. PSES-2126C(trunk)# exit
  5. PSES-2126C#
  6. trunk
  7. exit
  8. alarm
```

DE

```
 9. events
10. end
11. ip
12. help
13. history
PSES-2126C(ip)# history 3
 Command history:
12. help
13. history
14. history 3
PSES-2126C(ip)#
```

- **logout**
  - Syntax:

    logout
  - Description:

    When you enter this command via Telnet connection, you would logout the system and disconnect. If you connect the system through direct serial port with RS-232 cable, you would logout the system and be back to the initial login prompt when you run this command.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

    PSES-2126C# logout
- **restore default**
  - Syntax:

    restore default
  - Description:

    When you use this function in CLI, the system will show you the information "Do you want to restore the default IP address?(y/n)". If you choose Y or y, the IP address will restore to default "192.168.1.1". If you

choose N or n, the IP address will keep the same one that you had saved before.

If restoring default successfully, the CLI would prompt if reboot immediately or not. If you press Y or y, the system would reboot immediately; otherwise, it would be back to the CLI system. After restoring default configuration, all the changes in the startup configuration would be lost. After rebooting, the entire startup configuration would reset to factory default.

- Argument:

None.

- Possible value:

None.

- Example:

PSES-2126C# restore default

Restoring ...

Restore Default Configuration Successfully

Press any key to reboot system.

- **restore user**

  - Syntax:

  restore user

  - Description:

  To restore the startup configuration as user defined configuration. If restoring default successfully, the CLI would prompt if reboot immediately or not. If you press Y or y, the system would reboot immediately; others would back to the CLI system. After restoring user-defined configuration, all the changes in the startup configuration would be lost. After rebooting, the entire startup configuration would replace as user defined one.

  - Argument:

  None.

  - Possible value:

  None.

  - Example:

  PSES-2126C# restore user

Restoring ...

Restore User Configuration Successfully

Press any key to reboot system.

- **save start**
  - Syntax:

save start

  - Description:

To save the current configuration as the start one. When you enter this command, the CLI would save your current configuration into the non-volatile FLASH. If you want the configuration still works after rebooting, save the configuration using the command 'save start'.

  - Argument:

None.

  - Possible value:

None.

  - Example:

```
PSES-2126C# save start

Saving start...

Save Successfully

PSES-2126C#
```

- **save user**
  - Syntax:

save user

  - Description:

To save the current configuration as the user-defined configuration. When you enter this command, the CLI would save your current configuration into the non-volatile FLASH as user-defined configuration.

  - Argument:

None.

  - Possible value:

None.

  - Example:

PSES-2126C# save user

Saving user...

Save Successfully

PSES-2126C#

5.2.2 Local Commands of CLI

Please note: to use one of the local commands, you first have to change to the corresponding configuration area, e.g. `802.1x <Enter> set mode 1`.

802.1x

- **set max-request**
  - Syntax:

    set max-request <port-range> <times>
  - Description:

    The maximum number of times that the state machine will retransmit an EAP Request packet to the Supplicant before it times out the authentication session.
  - Argument:

    <port range>: syntax 1,5-7, available from 1 to 26

    <times>: max-times, range 1-10
  - Possible value:

    <port range> : 1 to 26

    <times> : 1-10, default is 2
  - Example:

    PSES-2126C(802.1x)# set max-request 2 2
- **set mode**
  - Syntax:

    set mode <port-range> <mode>
  - Description:

    To set up the 802.1X authentication mode of each port.
  - Argument:

    <port range> : syntax 1,5-7, available from 1 to 26

    <mode> : set up 802.1x mode

    0:disable the 802.1x function

1:set 802.1x to Multi-host mode

- Possible value:

<port range> : 1 to 26

<mode>: 0 or 1

- Example:

PSES-2126C(802.1x)# set mode 2 1

- **set port-control**
  - Syntax:

set port-control <port-range> <authorized>

  - Description:

To set up 802.1X status of each port.

  - Argument:

<port range> : syntax 1,5-7, available from 1 to 26

<authorized> : set up the status of each port

0:ForceUnauthorized

1:ForceAuthorized

2:Auto

  - Possible value:

<port range> : 1 to 26

<authorized> : 0,1 or 2

  - Example:

PSES-2126C(802.1x)# set port-control 2 2

- **set quiet-period**
  - Syntax:

set quiet-period <port-range> <sec>

  - Description:

A timer used by the Authenticator state machine to define periods of time during when it will not attempt to acquire a Supplicant.

  - Argument:

<port range> : syntax 1,5-7, available from 1 to 26

<sec> : timer, range 0-65535

  - Possible value:

<port range> : 1 to 26

<sec> : 0-65535, default is 60

- Example:

PSES-2126C(802.1x)# set quiet-period 2 30

- **set reAuthEnabled**
  - Syntax:

set reAuthEnabled <port-range> <ebl>

  - Description:

A constant that define whether regular reauthentication will take place on this port.

  - Argument:

<port range> : syntax 1,5-7, available from 1 to 26

<ebl> :

0:"OFF" to disable reauthentication

1:"ON" to enable reauthentication

  - Possible value:

<port range> : 1 to 26

<ebl> : 0 or 1, default is 1

  - Example:

PSES-2126C(802.1x)# set reAuthEnabled 2 1

- **set reAuthMax**
  - Syntax:

set reAuthMax <port-range> <max>

  - Description:

The number of reauthentication attempts that are permitted before the port becomes Unauthorized.

  - Argument:

<port range> : syntax 1,5-7, available from 1 to 26

<max> : max. value , range 1-10

  - Possible value:

<port range> : 1 to 26

<max> : 1-10, default is 2

- Example:

PSES-2126C(802.1x)# set reAuthMax 2 2

- **set reAuthPeriod**
  - Syntax:

set reAuthPeriod <port-range> <sec>

  - Description:

A constant that defines a nonzero number of seconds between periodic reauthentication of the supplicant.

  - Argument:

<port range> : syntax 1,5-7, available from 1 to 26

<sec> : timer, range 1-65535

  - Possible value:

<port range> : 1 to 26

<sec> : 1-65535, default is 3600

  - Example:

PSES-2126C(802.1x)# set reAuthPeriod 2 3600

- **set serverTimeout**
  - Syntax:

set serverTimeout <port-range> <sec>

  - Description:

A timer used by the Backend Authentication state machine in order to determine timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. The initial value of this timer is either suppTimeout or serverTimeout, as determined by the operation of the Backend Authentication state machine.

  - Argument:

<port range> : syntax 1,5-7, available from 1 to 26

<sec> : timer, range 1-65535

  - Possible value:

<port range> : 1 to 26

<sec> : 1-65535, default is 30

  - Example:

PSES-2126C(802.1x)# set serverTimeout 2 30

- **set state**
  - Syntax:

    set state <ip> <port-number> <secret-key>
  - Description:

    To configure the settings related with 802.1X Radius Server.
  - Argument:

    <ip> : the IP address of Radius Server, and the IP format is xxx.xxx.xxx.xxx

    <port-number> : the service port of Radius Server(Authorization port), range 1~65535

    <secret-key> : set up the value of secret-key, and the length of secret-key is from 1 to 31
  - Possible value:

    <port-number> : 1~65535, default 1812
  - Example:

    PSES-2126C(802.1x)# set state 192.168.1.115 1812 WinRadius
- **set suppTimeout**
  - Syntax:

    set suppTimeout <port-range> <sec>
  - Description:

    A timer used by the Backend Authentication state machine in order to determine timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. The initial value of this timer is either suppTimeout or serverTimeout, as determined by the operation of the Backend Authentication state machine.
  - Argument:

    <port range> : syntax 1,5-7, available from 1 to 26

    <sec> : timer, range 1-65535
  - Possible value:

    <port range> : 1 to 26

    <sec> : 1-65535, default is 30
  - Example:

    PSES-2126C(802.1x)# set suppTimeout 2 30

DE

- **set txPeriod**
  - Syntax:

    set txPeriod <port-range> <sec>
  - Description:

    A timer used by the Authenticator PAE state machine to determine when an EAPOL PDU is to be transmitted.
  - Argument:

    <port range> : syntax 1,5-7, available from 1 to 26

    <sec> : timer, range 1-65535
  - Possible value:

    <port range> : 1 to 26

    <sec> : 1-65535, default is 30
  - Example:

    PSES-2126C(802.1x)# set txPeriod 2 30
- **show mode**
  - Syntax:

    show mode
  - Description:

    To display the mode of each port.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
PSES-2126C(802.1x)# show mode
 Port      Mode
====== ============
   1     Disable
   2     Multi-host
   3     Disable
   4     Disable
   5     Disable
```

```
6       Disable
```

- **show parameter**
  - Syntax:

  show parameter
  - Description:

  To display the parameter settings of each port.
  - Argument:

  None.
  - Possible value:

  None.
  - Example:

```
PSES-2126C(802.1x)# show parameter
port  1) port control  : Auto
         reAuthMax     : 2
         txPeriod      : 30
         Quiet Period  : 60
         reAuthEnabled : ON
         reAuthPeriod  : 3600
         max. Request  : 2
         suppTimeout   : 30
         serverTimeout : 30
```

- **show security**
  - Syntax:

  show security
  - Description:

  To display the authentication status of each port.
  - Argument:

  None.
  - Possible value:

  None.
  - Example:

PSES-2126C(802.1x)# show security

```
 Port       Mode          Status
====== ============ ==============
   1      Disable
   2      Multi-host    Unauthorized
   3      Disable
   4      Disable
   5      Disable
   6      Disable
```

- **show state**
  - Syntax:

  show state
  - Description:

  To display the Radius server configuration.
  - Argument:

  None.
  - Possible value:

  None.
  - Example:

  PSES-2126C(802.1x)# show state

```
Radius Server: 192.168.1.115
Port Number  : 1812
Secret Key   : WinRadius
```

account

- **add**
  - Syntax:

  add <name>
  - Description:

  To create a new guest user. When you create a new guest user, you must type in password and confirm password.
  - Argument:

<name> : new account name

- Possible value:

<name> : A string must be at least 5 character.

- Example:

```
PSES-2126C(account)# add aaaaa
Password:
Confirm Password:
PSES-2126C(account)#
```

- **del**
  - Syntax:

del <name>

  - Description:

To delete an existing account.

  - Argument:

<name> : existing user account

  - Possible value:

None.

  - Example:

```
PSES-2126C(account)# del aaaaa
Account aaaaa deleted
```

- **modify**
  - Syntax:

modify <name>

  - Description:

To change the username and password of an existing account.

  - Argument:

<name> : existing user account

  - Possible value:

None.

  - Example:

```
PSES-2126C(account)# modify aaaaa
username/password: the length is from 5 to 15.
```

```
Current username (aaaaa):bbbbb
New password:
Confirm password:
Username changed successfully.
Password changed successfully.
```

■ **show**

□ Syntax:

show

□ Description:

To show system account, including account name and identity.

□ Argument:

None.

□ Possible value:

None.

□ Example:

```
PSES-2126C(account)# show
  Account Name       Identity
----------------- ---------------
 admin              Administrator
 guest                  guest
 bbbbb                  guest
```

alarm

<<email>>

■ **del mail-address**

□ Syntax:

del mail-address <#>

□ Description:

To remove the e-mail address.

□ Argument:

<#>: email address number, range: 1 to 6

□ Possible value:

<#>: 1 to 6

- Example:

```
PSES-2126C(alarm-email)# del mail-address 2
```

- **del server-user**
  - Syntax:

    del server-user
  - Description:

    To remove the server, user account and password.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
PSES-2126C(alarm-email)# del server-user
```

- **set mail-address**
  - Syntax:

    set mail-address <#> <mail address>
  - Description:

    To set up the email address.
  - Argument:

    <#> : email address number, range: 1 to 6

    <mail address> : email address
  - Possible value:

    <#>: 1 to 6
  - Example:

```
PSES-2126C(alarm-email)# set mail-address 1
abc@mail.abc.com
```

- **set server**
  - Syntax:

    set server <ip>
  - Description:

    To set up the IP address of the email server.

DE

- Argument:

<ip>:email server ip address or domain name

- Possible value:

None.

- Example:

```
PSES-2126C(alarm-email)# set server 192.168.1.6
```

- **set user**
  - Syntax:

set user <username>

  - Description:

To set up the account of the email server.

  - Argument:

<username>: email server account

  - Possible value:

None.

  - Example:

```
PSES-2126C(alarm-email)# set user admin
```

- **show**
  - **Syntax**:

show

  - Description:

To display the configuration of e-mail trap event.

  - Argument:

None.

  - Possible value:

None.

  - Example:

```
PSES-2126C(alarm-email)# show
Mail Server    : 192.168.1.6
Username       : admin
Password       : ***************
Email Address 1: abc@mail.abc.com
```

```
Email Address 2:
Email Address 3:
Email Address 4:
Email Address 5:
Email Address 6:
```

<<events>>

- **del all**
  - **Syntax**:

    del all <range>
  - Description:

    To disable email, sms and trap of events.
  - Argument:

    <range>:del the range of email, sms and trap of events, syntax 1,5-7
  - Possible value:

    <range>: 1~22
  - Example:

```
PSES-2126C(alarm-events)# del all 1-3
```

- **del email**
  - **Syntax**:

    del email <range>
  - Description:

    To disable the email of the events.
  - Argument:

    <range>:del the range of email, syntax 1,5-7
  - Possible value:

    <range>: 1~22
  - Example:

```
PSES-2126C(alarm-events)# del email 1-3
```

- **del sms**
  - **Syntax**:

    del sms <range>
  - Description:

To disable the sms of the events.

- Argument:

<range>:del the range of sms, syntax 1,5-7

- Possible value:

<range>: 1~22

- Example:

```
PSES-2126C(alarm-events)# del sms 1-3
```

- **del trap**
  - **Syntax**:

del trap <range>

  - Description:

To disable the trap of the events.

  - Argument:

<range>:del the range of trap, syntax 1,5-7

  - Possible value:

<range>: 1~22

  - Example:

```
PSES-2126C(alarm-events)# del trap 1-3
```

- **set all**
  - **Syntax**:

set all <range>

  - Description:

To enable email, sms and trap of events.

  - Argument:

<range>:set the range of email, sms and trap of events, syntax 1,5-7

  - Possible value:

<range>: 1~22

  - Example:

```
PSES-2126C(alarm-events)# set all 1-3
```

- **set email**
  - **Syntax**:

set email <range>

- Description:

To enable the email of the events.

- Argument:

<range>:set the range of email, syntax 1,5-7

- Possible value:

<range>: 1~22

- Example:

```
PSES-2126C(alarm-events)# set email 1-3
```

- **set sms**
  - **Syntax**:

set sms <range>

- Description:

To enable the sms of the events.

- Argument:

<range>:set the range of sms, syntax 1,5-7

- Possible value:

<range>: 1~22

- Example:

```
PSES-2126C(alarm-events)# set sms 1-3
```

- **set trap**
  - **Syntax**:

set trap <range>

- Description:

To enable the trap of the events.

- Argument:

<range>:set the range of trap, syntax 1,5-7

- Possible value:

<range>: 1~22

- Example:

```
PSES-2126C(alarm-events)# set trap 1-3
```

- **show**
  - **Syntax**:

show

□ Description:

The Show here is used to display the configuration of alarm event.

□ Argument:

None.

□ Possible value:

None.

□ Example:

```
PSES-2126C(alarm-events)# show
   Events                    Email SMS Trap
-----------------------------------------
1  Cold Start                          v
2  Warm Start                          v
3  Link Down                           v
4  Link Up                             v
5  Authentication Failure              v
6  User Login
7  User Logout
8  STP Topology Changed
9  STP Disabled
10 STP Enabled
11 LACP Disabled
12 LACP Enabled
13 LACP Member Added
14 LACP Port Failure
15 GVRP Disabled
16 GVRP Enabled
17 Port-based Vlan Enabled
18 Tag-based Vlan Enabled
19 Module Inserted
```

```
20 Module Removed
21 Moudle Media Swapped
22 PoE Failure
```

- **show (alarm)**
  - **Syntax**:

    show
  - Description:

    The Show for alarm here is used to display the configuration of Trap, SMS or E-mail.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
PSES-2126C(alarm)# show email
PSES-2126C(alarm)# show events
PSES-2126C(alarm)# show sms
```

    <<sms>>

- **del phone-number**
  - **Syntax**:

    del phone-number <#>
  - Description:

    To delete sms phone number.
  - Argument:

    <#>: mobile phone number, range: 1 to 6
  - Possible value:

    <#>: 1 to 6
  - Example:

```
PSES-2126C(alarm-sms)# del phone-number 3
```

- **del server-user**
  - **Syntax**:

    del server-user

DE

- Description:

  To delete sms server, user account and password.

- Argument:

  None.

- Possible value:

  None.

- Example:

```
PSES-2126C(alarm-sms)# del server-user
```

- **set phone-number**
  - Syntax:

    set phone-number <#> <phone-number>

  - Description:

    To add sms phone number.

  - Argument:

    <#>: mobile phone number, range: 1 to 6

    <phone-number>: phone number

  - Possible value:

    <#>: 1 to 6

  - Example:

```
PSES-2126C(alarm-sms)# set phone-number 1 0968777777
```

- **set server**
  - Syntax:

    set server <ip>

  - Description:

    To set up the IP address of sms server.

  - Argument:

    <ip>: SMS server ip address or domain name

  - Possible value:

    None.

  - Example:

```
PSES-2126C(alarm-sms)# set server 192.168.1.7
```

- **set user**
  - **Syntax**:

    set user <username>
  - Description:

    To set up user account and password of sms server.
  - Argument:

    <username>: SMS server account
  - Possible value:

    None.
  - Example:

```
PSES-2126C(alarm-sms)# set user ABC
```

- **show**
  - **Syntax**:

    show
  - Description:

    To display the configuration of SMS trap event.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
PSES-2126C(alarm-sms)# show
SMS Server      : 192.168.1.7
Username        : ABC
Password        : ****************
Mobile Phone  1: 0968777777
Mobile Phone  2:
Mobile Phone  3:
Mobile Phone  4:
Mobile Phone  5:
Mobile Phone  6:
```

DE

autologout

- **autologout**
  - Syntax:

    autologout <time>
  - Description:

    To set up the timer of autologout.
  - Argument:

    <time>: range 1 to 3600 seconds, 0 for autologout off, current setting is 180 seconds.
  - Possible value:

    <time >: 0,1-3600
  - Example:

    PSES-2126C# autologout 3600

    Set autologout time to 3600 seconds

bandwidth

- **set egress-rate**
  - Syntax:

    set egress-rate <range> <data_rate>
  - Description:

    To set up the egress-rate of the ports.
  - Argument:

    <range>:syntax 1,5-7, available from 1 to 26

    <data_rate>: 66-1024000(Kb).

    port 1-24: 66-102400(Kb); port 25-26: 66-1024000(Kb)
  - Possible value:

    <range>: 1 to 26

    <data_rate>: 66-102400(Kb) for port 1-24; 66-1024000(Kb) for port 25-26
  - Example:

    PSES-2126C(bandwidth)# set egress-rate 1-16 299
- **set ingress-rate**
  - Syntax:

set ingress-rate <range> <data_rate>

- Description:

To set up the ingress-rate of the ports.

- Argument:

<range>:syntax 1,5-7, available from 1 to 26

<data_rate>: 66-1024000(Kb).

port 1-24: 66-102400(Kb); port 25-26: 66-1024000(Kb)

- Possible value:

<range>: 1 to 26

<data_rate>: 66-102400(Kb) for port 1-24; 66-1024000(Kb) for port 25-26

- Example:

PSES-2126C(bandwidth)# set ingress-rate 1-16 100

set storm-rate

- Syntax:
- Description:

To set up the storm-rate of the ports.

- Argument:
- <range>:syntax: 1,3-5, available from 1 to 5

1: Disable 2: Broadcast Storm Control

3: Multicast Storm Control

4: Unknown Unicast Storm Control

5: Broadcast, Multicast, Unknown Unicast Storm Control

<data_rate>: 1-100. The value must be the integer.

The value 100 disables broadcast storm control.

- Possible value:

<range>: 1 to 5

<data_rate>: 1-100.

- Example:

PSES-2126C(bandwidth)# set storm-rate 2 99

show

- Syntax:

DE

- Description:

To display all current settings of the bandwidth.

- Argument:

None.

- Possible value:

None.

- Example:

```
PSES-2126C(bandwidth)# show
 Port   Ingress Rate(Kb)    Egress Rate(Kb)
====== ==================  =================
    1      102400               102400
    2      102400               102400
    3      102400               102400
              :
             :
   23      102400               102400
   24      102400               102400
   25     1024000              1024000
   26     1024000              1024000

   Broadcast Storm Control
==========================================================
==
Type: Disable
Rate: 100 %
```

config-file

- **export start**

- Syntax:

export start

- Description:

To run the export start function.

- Argument:

None.

- Possible value:

None.

- Example:

PSES-2126C(config-file)# export start

Export successful.

- **export user-conf**
  - Syntax:
  - Description:

To run the export user-conf function.

- Argument:

None.

- Possible value:

None.

- Example:

PSES-2126C(config-file)# export user-conf

Export successful.

- **import start**
  - Syntax:
  - Description:

To run the import start function.

- Argument:

None.

- Possible value:

None.

- Example:

PSES-2126C(config-file)# import start

Import successful.

- **import user-conf**
  - Syntax:
  - Description:

To run the import user-conf function.

- Argument:

None.

- Possible value:

None.

- Example:

PSES-2126C(config-file)# import user-conf

Import successful.

- **set export-path**
  - Syntax:
  - Description:

To set up the file path and filename that user would like to export.

- Argument:

<filepath>:filepath and filename

- Possible value:

<filepath>:filepath and filename

- Example:

PSES-2126C(config-file)# set export-path log/21511.txt

- **set import-path**
  - Syntax:
  - Description:

To set up the filepath and filename that user would like to import.

- Argument:

<filepath>:filepath and filename

- Possible value:

<filepath>:filepath and filename

- Example:

PSES-2126C(config-file)# set import-path log/21511.txt

- **show**
  - Syntax:
  - Description:

To display the information of the config file.

- Argument:

None.

- Possible value:

None.

- Example:

```
PSES-2126C(config-file)# show
TFTP Server IP Address: 192.168.3.111
Export Path and Filename: log/21511.txt
Import Path and Filename: log/21511.txt
```

dhcp-boot

set dhcp-boot

- Syntax:
- Description:

To set up the delay time for DHCP Boot.

- Argument:
- <sec>:range syntax: 0, 1-30. The value "0" is to disable dhcp-boot delay
- Possible value:

<sec>:0-30

- Example:

PSES-2126C(dhcp-boot)# set 30

show

- Syntax:
- Description:

To display the status of DHCP Boot.

- Argument:

None.

- Possible value:

None.

- Example:

PSES-2126C(dhcp-boot)# show

DHCP Boot : Enable

```
Second      : 30
PSES-2126C(dhcp-boot)#
```

diag

diag

- Syntax:

diag

- Description:

Diag is used to test whether EEPROM, UART, DRAM and Flash is normal or not.

- Argument:

None.

- Possible value:

None.

- Example:

```
PSES-2126C(diag)# diag
EEPROM Test : OK
UART Test   : OK
DRAM Test   : OK
Flash Test  : OK
```

Loopback

- Syntax:

loopback

- Description:

For Internal/External Loopback Test.

- Argument:

None.

- Possible value:

None.

- Example:

```
PSES-2126C(diag)# loopback
Internal Loopback Test : OK
```

```
External Loopback Test : Port 1 2 3 4 5 6 7 8 9 10 11
12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 Fail
```

- **ping**
  - Syntax:

    ping <ip>
  - Description:

    To confirm that whether the remote end-station or switch itself is alive or not.
  - Argument:

    <ip> : IP address or domain name
  - Possible value:

    IP address, e.g. 192.168.2.65 or domain name, e.g. tw.yahoo.com
  - Example:

```
PSES-2126C(diag)# ping 192.168.1.115
Gateway       : 192.168.1.253
192.168.1.115 is alive.
```

firmware

- **set upgrade-path**
  - Syntax:
  - Description:

    To set up the image file that will be upgraded.
  - Argument:

    <filepath>: upgrade file path and name
  - Possible value:

    <filepath>: upgrade file path and name
  - Example:

```
PSES-2126C(firmware)#          set          upgrade-path
FEL2SW26_ES2126_v2.05.img
```

- **show**
  - Syntax:
  - Description:

    To display the information of tftp server and upgrade-path and file name.

- Argument:

None.

- Possible value:

None.

- Example:

```
PSES-2126C(firmware)# show
TFTP Server IP Address: 192.168.3.111
Path and Filename     : FEL2SW26_ES2126_v2.05.img
```

- **upgrade**
  - Syntax:
  - Description:

To run the software upgrade function.

- Argument:

None.

- Possible value:

None.

- Example:

```
PSES-2126C(firmware)# upgrade
```

Upgrading firmware ...

gvrp

- **disable**
  - Syntax:

disable

- Description:

To disable the gvrp function

- Argument:

None.

- Possible value:

None.

- Example:

PSES-2126C(gvrp)# disable

- **enable**
  - Syntax:

    enable
  - Description:

    To enable the gvrp function.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

    PSES-2126C(gvrp)# enable
- **group**
  - Syntax:

    group <group number>
  - Description:

    To enter any of gvrp group for changing gvrp group setting. You can change the applicant or registrar mode of existing gvrp group per port.
  - **Argument:**

    <group number>: enter which gvrp group you had created, using value is vid. Available range: 1 to 4094
  - Possible value:

    <group number>: 1~4094
  - Example:

```
PSES-2126C(gvrp)# show group

GVRP group information

Current Dynamic Group Number: 1

VID  Member Port

---- ---------------------------------------------
-

2    5

PSES-2126C(gvrp)# group 2
```

PSES-2126C(gvrp-group-2)# set applicant 1-6 non-participant

DE

```
PSES-2126C(gvrp-group-2)# show
GVRP group VID: 2
Port Applicant       Registrar
---- --------------- ---------
1    Non-Participant Normal
2    Non-Participant Normal
3    Non-Participant Normal
4    Non-Participant Normal
5    Non-Participant Normal
6    Non-Participant Normal
7    Normal          Normal
8    Normal          Normal
12   Normal          Normal
13   Normal          Normal
            :
            :
23   Normal          Normal
24   Normal          Normal
25   Normal          Normal
26   Normal          Normal
PSES-2126C(gvrp-group-2)# set registrar 1-10 fixed

PSES-2126C(gvrp-group-2)# show
GVRP group VID: 2
Port Applicant       Registrar
---- --------------- ---------
1    Non-Participant Fixed
2    Non-Participant Fixed
3    Non-Participant Fixed
4    Non-Participant Fixed
```

```
5     Non-Participant Fixed
6     Non-Participant Fixed
7     Normal          Fixed
8     Normal          Fixed
9     Normal          Fixed
10    Normal          Fixed
17    Normal          Normal
              :
               :
23    Normal          Normal
24    Normal          Normal
25    Normal          Normal
26    Normal          Normal
```

- **set applicant**
  - Syntax:

    set applicant <range> <normal|non-participant>
  - Description:

    To set default applicant mode for each port.
  - **Argument:**

    <range>: port range, syntax 1,5-7, available from 1 to 26

    <normal>: set applicant as normal mode

    <non-participant>: set applicant as non-participant mode
  - **Possible value:**

    <range>: 1 to 26

    <normal|non-participant>: normal or non-participant
  - Example:

    PSES-2126C(gvrp)# set applicant 1-10 non-participant
- **set registrar**
  - Syntax:

    set registrar <range> <normal|fixed|forbidden>
  - Description:

DE

To set default registrar mode for each port.

- **Argument:**

<range>: port range, syntax 1,5-7, available from 1 to 26

<normal>: set registrar as normal mode

<fixed>: set registrar as fixed mode

<forbidden>: set registrar as forbidden mode

- Possible value:

<range>: 1 to 26

<normal|fixed|forbidden>: normal or fixed or forbidden

- Example:

PSES-2126C(gvrp)# set registrar 1-5 fixed

- **set restricted**
  - Syntax:

set restricted <range> <enable|disable>

- Description:

To set the restricted mode for each port.

- **Argument:**

<range>: port range, syntax 1,5-7, available from 1 to 26

<enable>: set restricted as enabled

<disable>: set restricted as disabled

- Possible value:

<range>: 1 to 26

<enable|disable>: enable or disable

- Example:

```
PSES-2126C(gvrp)# set restricted 1-10 enable

PSES-2126C(gvrp)# show config

GVRP state: Enable

Port Join Time Leave Time LeaveAll Time     Applicant
Registrar Restricted

---- --------- ---------- ------------- --------------
- --------- ----------
```

```
  1      20        60        1000      Normal          Normal
Enable
  2      20        60        1000      Normal          Normal
Enable
  3      20        60        1000      Normal          Normal
Enable
  4      20        60        1000      Normal          Normal
Enable
  5      20        60        1000      Normal          Normal
Enable
  6      20        60        1000      Normal          Normal
Enable
  7      20        60        1000      Normal          Normal
Enable
  8      20        60        1000      Normal          Normal
Enable
  9      20        60        1000      Normal          Normal
Enable
 10      20        60        1000      Normal          Normal
Enable
                                                 :
                                           :
                                           :
 22      20        60        1000      Normal          Normal
Disable
 23      20        60        1000      Normal          Normal
Disable
 24      20        60        1000      Normal          Normal
Disable
 25      20        60        1000      Normal          Normal
Disable
 26      20        60        1000      Normal          Normal
Disable
```

DE

- **set timer**
  - Syntax:

    set timer <range> <join> <leave> <leaveall>
  - Description:

    To set gvrp join time, leave time, and leaveall time for each port.
  - **Argument:**

    <range> : port range, syntax 1,5-7, available from 1 to 26

    <join>: join timer, available from 20 to 100

    <leave>: leave timer, available from 60 to 300

    <leaveall>: leaveall timer, available from 1000 to 5000

    Leave Time must equal double Join Time at least.
  - Possible value:

    <range> : 1 to 26

    <join>: 20 to 100

    <leave>: 60 to 300

    <leaveall>: 1000 to 5000
  - Example:

    PSES-2126C(gvrp)# set timer 2-8 25 80 2000
- **show config**
  - Syntax:

    show config
  - Description:

    To display the gvrp configuration.
  - **Argument:**

    None.
  - Possible value:

    None.
  - Example:

    PSES-2126C(gvrp)# show config

    GVRP state: Disable

    ```
    Port  Join Time  Leave Time  LeaveAll Time  Applicant
    Registrar Restricted
    ```

```
---- --------- ---------- ------------ --------------
- --------- ----------
  1     20        60        1000      Normal          Normal
Disable
  2     20        60        1000      Normal          Normal
Disable
  3     20        60        1000      Normal          Normal
Disable
  4     20        60        1000      Normal          Normal
Disable
                                   :
                                   :
                                   :
 23     20        60        1000      Normal          Normal
Disable
 24     20        60        1000      Normal          Normal
Disable
 25     20        60        1000      Normal          Normal
Disable
 26     20        60        1000      Normal          Normal
Disable
```

- **show counter**
  - Syntax:

    show counter <port>
  - Description:

    To show counter of the port.
  - **Argument:**

    <port>: port number, available from 1 to 26
  - Possible value:

    <port>: 1 to 26
  - Example:

    PSES-2126C(gvrp)# show counter 2

    ```
    GVRP Counter port: 2
    ```

DE

```
Counter Name            Received Transmitted
--------------------    -------- -----------
Total GVRP Packets             0           0
Invalid GVRP Packets           0        ----
LeaveAll message               0           0
JoinEmpty message              0           0
JoinIn message                 0           0
LeaveEmpty message             0           0
Empty message                  0           0
```

- **show group**
  - Syntax:

  show group
  - Description:

  To show the gvrp group.
  - **Argument:**

  None.
  - Possible value:

  None.
  - Example:

  PSES-2126C(gvrp)# show group

```
GVRP group information
Current Dynamic Group Number: 0
VID  Member Port
---- ------------------------------------------------
-
```

hostname

- **hostname**
  - Syntax:
  - Description:

  To set up the hostname of the switch.

- Argument:

<name>: hostname, max. 40 characters.

- Possible value:

<name>: hostname, max. 40 characters.

- Example:

PSES-2126C# hostname Company

Company#

igmp-snooping

- **add allowed-group**
  - Syntax:

  add allowed-group <ip-multicast> <vid> <port-range>

  - Description:

  To add the entry of allowed IP multicast group.

  - Argument:

  <ip-multicast>: the range of IP multicast.

  <vid>: VLAN ID. 1-4094 or any.

  <port-range>: syntax 1,5-7, available from 1 to 26

  - Possible value:

  <ip-multicast>: ex: 224.1.1.1-225.2.3.3 or any

  <vid>: 1-4094 or any

  <port-range>: 1 to 26

  - Example:

  PSES-2126C(igmp-snooping)# add allowed-group 224.1.1.1-225.2.3.3 100 1-10

- **del allowed-group**
  - Syntax:

  del allowed-group <index>

  - Description:

  To remove the entry of allowed IP multicast group

  - Argument:

  <index>: the index of the allowed-group.

DE

- Possible value:

<index>: the index of the allowed-group.

- Example:

PSES-2126C(igmp-snooping)# del allowed-group 1

- **set mode**
  - Syntax:
  - Description:

To set up the mode of IGMP Snooping.

- Argument:

<status>: 0:disable, 1:active, 2:passive

- Possible value:

<status>: 0,1or 2

- Example:

PSES-2126C(igmp-snooping)# set mode 2

- **show igmp-snooping**
  - Syntax:
  - Description:

To display IGMP snooping mode and allowed IP multicast entry.

- Argument:

None.

- Possible value:

None.

- Example:

PSES-2126C(igmp-snooping)# show igmp-snooping

Snoop Mode: Active

IP Multicast:

1) IP Address : 224.1.1.1
   VLAN ID : 0
   Member Port : 22

- **show multicast**
  - Syntax:
  - Description:

To display IP multicast table.

- Argument:

None.

- Possible value:

None.

- Example:

PSES-2126C(igmp-snooping)# show multicast

IP Multicast: None

IP

- **disable dhcp**
  - Syntax:

  disable dhcp
  - Description:

  To disable the DHCP function of the system.
  - Argument:

  None.
  - Possible value:

  None.
  - Example:

  PSES-2126C(ip)# disable dhcp

  DHCP is already stopped.
- **enable dhcp**
  - Syntax:

  enable dhcp <manual|auto>
  - Description:

  To enable the system DHCP function and set DNS server via manual or auto mode.
  - Argument:

  <manual|auto> : set DNS by using manual or auto mode.
  - Possible value:

  <manual|auto> : manual or auto
  - Example:

PSES-2126C(ip)# enable dhcp manual

- **set dns**
  - Syntax:

    set dns <ip>
  - Description:

    To set the IP address of DNS server.
  - Argument:

    <ip> : dns ip address
  - Possible value:

    <ip> : 168.95.1.1
  - Example:

    PSES-2126C(ip)# set dns 168.95.1.1
- **set ip**
  - Syntax:

    set ip <ip> <mask> <gateway>
  - Description:

    To set the system IP address, subnet mask and gateway.
  - Argument:

    <ip> : ip address

    <mask> : subnet mask

    <gateway> : default gateway
  - Possible value:

    <ip> : 192.168.1.1 or others

    <mask> : 255.255.255.0 or others

    <gateway> : 192.168.1.253 or others
  - Example:

    PSES-2126C(ip)# set ip 192.168.1.2 255.255.255.0 192.168.1.253
- **show**
  - Syntax:

    show
  - Description:

To display the system's DHCP function state, IP address, subnet mask, default gateway, DNS mode, DNS server IP address and current IP address.

- Argument:

None.

- Possible value:

None.

- Example:

```
PSES-2126C(ip)# show
DHCP               : Disable
IP Address         : 192.168.1.1
Current IP Address : 192.168.1.1
Subnet mask        : 255.255.255.0
Gateway            : 192.168.1.253
DNS Setting        : Manual
DNS Server         : 192.95.1.1
```

log

- **clear**
  - Syntax:

  clear
  - Description:

  To clear the log data.
  - Argument:

  None.
  - Possible value:

  None.
  - Example:

  PSES-2126C(log)# clear
- **disable auto-upload**
  - Syntax:

  disable auto-upload

- Description:

To disable the auto-upload function.

- Argument:

None.

- Possible value:

None.

- Example:

PSES-2126C(log)# disable auto-upload

- **enable auto-upload**
  - Syntax:

enable auto-upload

- Description:

To enable the auto-upload function.

- Argument:

None.

- Possible value:

None.

- Example:

PSES-2126C(log)# enable auto-upload

- **show**
  - Syntax:

show

- Description:

To show a list of trap log events. When any of log events happens, it will be recorded and using show command in log function to query. Up to 120 log records are supported.

- Argument:

None.

- Possible value:

None.

- Example:

```
PSES-2126C(log)# show
```

```
Tftp Server : 0.0.0.0
Auto Upload : Disable

1)  Wed Apr 13 12:13:27 2005  Link Up [Port 1]
2)  Wed Apr 13 12:13:26 2005  Link Down [Port 1]
3)  Wed Apr 13 11:58:31 2005  Login [admin]
4)  Wed Apr 13 11:19:45 2005  Login [admin]
5)  Wed Apr 13 11:19:37 2005  Logout [admin]
```


- **upload**
  - Syntax:

    Upload
  - Description:

    To upload log data through tftp.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

    PSES-2126C(log)# upload

mac-table

<<alias>>

- **del**
  - Syntax:

    del <mac>
  - Description:

    To delete the mac alias entry.
  - Argument:

    <mac> : mac address, format: 00-02-03-04-05-06

- Possible value:

<mac> : mac address

- Example:

PSES-2126C(mac-table-alias)# del 00-44-33-44-55-44

set

- Syntax:

set <mac> <alias>

- Description:

To set up the mac alias entry.

- Argument:

<mac> : mac address, format: 00-02-03-04-05-06

<alias> : mac alias name, max. 15 characters

- Possible value:

<mac> : mac address

<alias> : max. 15 characters

- Example:

PSES-2126C(mac-table-alias)# set 00-44-33-44-55-44 www

show

- Syntax:

show

- Description:

To display the mac alias entry.

- Argument:

None.

- Possible value:

None.

- Example:

PSES-2126C(mac-table-alias)# show

```
MAC Alias List

      MAC Address       Alias
----- ----------------- ----------------
1)    00-02-03-04-05-06 aaa
```

```
2)     00-33-03-04-05-06 ccc
```

<<information>>

- **search**
  - Syntax:

search <port> <mac> <vid>

  - Description:

To look for the relative mac information in mac table.

  - Argument:

<port> : set up the range of the ports to search for,
syntax 1,5-7, available form 1 to 26

<mac> : mac address, format: 01-02-03-04-05-06, '?' can be used

<vid> : VLAN id, from 1 to 4094; '?' as don't care, 0 as untagged

  - Possible value:

<port> : 1 to 26

<vid> : 0, 1 ~4094

  - Example:

```
PSES-2126C(mac-table-information)# search 1-26 ??-??-
??-??-??-?? ?

MAC Table List

Alias            MAC Address       Port VID  State

---------------- ----------------- ---- ---- ---------
--------

                 00-40-c7-88-00-06    1   0  Dynamic

PSES-2126C(mac-table-information)#
```

- **show**
  - Syntax:

show

  - Description:

To display all mac table information.

  - Argument:

None.

  - Possible value:

None.

- Example:

PSES-2126C(mac-table-information)# show

MAC Table List

Alias	MAC Address	Port	VID	State
ABC	00-40-c7-d6-00-01	1	2	Static Forwarding
ABC123	00-40-c7-d6-00-02	1	3	Static Filtering

<<maintain>>

- **set aging**
  - Syntax:

set aging <time>

  - Description:

To set up the age out time of dynamic learning mac.

  - Argument:

<time> : Mac table ageout time between 10 and 1000000 seconds. The value "0"
means to disable age out time

  - Possible value:

<time> : 10-1000000 seconds or 0

  - Example:

PSES-2126C(mac-table-maintain)# set aging 300

- **set learning**
  - Syntax:

set learning <port> <num>

  - Description:

To set up the maximum amount of MAC that each port can learn.

  - Argument:

<port> : port range, syntax 1,5-7, available form 1 to 24

<num>: MAC address numbers which can be dynamically learned

num range: between 0 to 8191; 0 for learning disabled

  - Possible value:

<port> : 1 to 24

<num>: 0 to 8191

- Example:

PSES-2126C(mac-table-maintain)# set learning 5 100

- **show**
  - Syntax:

show

  - Description:

To display the settings of MAC table ageout time and the learning limit of each port.

  - Argument:

None.

  - Possible value:

None.

  - Example:

```
PSES-2126C(mac-table-maintain)# show

Mac table ageout time: 300 seconds

 Port   Dynamically learn limit

------ -------------------------

   1    8191

   2    8191

   3    8191

   4    8191

   5    8191

        :

        :

        :

  21    8191

  22    8191

  23    8191

  24    8191
```

DE

```
  25      8192
  26      8192
```

<<static-mac>>

- **add**
  - Syntax:

    add <mac> <vid> <queue> <rule> <port>
  - Description:

    To add the static mac entry.
  - Argument:

    <mac>: mac address, format: 01-02-03-04-05-06

    <vid>: VLAN id, from 1 to 4094

    <queue>: which queue you want to set, from 0 to 3

    <rule> : forwarding rule, from 0 to 2

    0:static

    1:drop destination address matches

    2:drop source address matches

    <port> : forwarded destination port, form 1 to 26
  - Possible value:

    <vid>: 1 to 4094

    <queue>: 0 to 3

    <rule>: 0 to 2

    <port>: 1 to 26
  - Example:

    PSES-2126C (mac-table-static-mac)# add 00-22-44-55-66-77 1 0 0 6
- **del**
  - Syntax:

    del <mac>
  - Description:

    To remove the static mac entry.
  - Argument:

    <mac> : mac address, format: 00-02-03-04-05-06

- Possible value:

<mac> : mac address

- Example:

PSES-2126C(mac-table-static-mac)# del 00-02-03-04-05-06

- **show**
  - Syntax:

show

  - Description:

To display static mac entry.

  - Argument:

None.

  - Possible value:

None.

  - Example:

PSES-2126C(mac-table-static-mac)# show

	MAC	VID	Queue	Forwarding Rule	Port
1)	00-40-C7-D6-00-01	200	2	Static with Destination Drop	2

management

- **add**
  - Syntax:

Usage: set [<name> <value>] [<vid> <value>] [<ip> <value>] [<port> <value>]

[<type> <value>] <action> <value>

Synopsis: set name Mary vid 20 ip 192.168.1.1-192.168.1.90 port 2-5,8

type h,s action a

Synopsis: set name Mary vid 20 ip 192.168.1.1-192.168.1.90

  - Description:

To save the adding management policy records.

When you don't know how to set the management policy records, you can use this command as follows:

DE

PSES-2126C(management-add)# set

This command will show exhaustive operating explanation for setting the management policy records.

□ Argument:

[<name> <value>]	ACL entry name.
[<vid> <value>]	VLAN ID.
[<ip> <value>]	IP range.
[<port> <value>]	Incoming port.
[<type> <value>]	Access type.
<action> <value>	a(ccept) or d(eny).

□ Possible value:

[<name> <value>]	No default and it must be set.
[<vid> <value>]	The range is 1-4095 and can be set to any.
[<ip> <value>]	For example, 192.168.1.90-192.168.1.90 or any.
[<port> <value>]	For example, 1 or 1-8 or 1,3-5 or any
[<type> <value>]	For example, h(ttp),s(nmp),t(elnet) or any.
<action> <value>	No default and it must be set.

□ Example:

```
PSES-2126C(management-add)# set name Mary vid 20 ip
192.168.1.1-192.168.1.90 port 2-5,8 type h,s action a

PSES-2126C(management-add)# show

 #: 1

Name : Mary                VlanID : 20          IP :
192.168.1.1-192.168.1.90

Type : Http,SNMP           Action : Accept      Port :
2,3,4,5,8
```

■ **delete**

□ Syntax:

delete #

□ Description:

To delete a specific record or range.

□ Argument:

[#]: a specific or range management security entry(s)

- Possible value:

None.

- Example:

```
PSES-2126C(management)# show

 #: 1
Name : Tom                    VlanID : 2           IP :
192.168.1.30-192.168.1.80
Type : SNMP              Action : Deny      Port : 1,2

PSES-2126C(management)# delete 1

PSES-2126C(management)# show

Security rule list is empty now
```

- **edit**

the specific management policy entry.

- Available range:

1 to 65536.

- Syntax:

Usage: set [<name> <value>] [<vid> <value>] [<ip> <value>] [<port> <value>]

[<type> <value>] <action> <value>

Synopsis: set name Mary vid 20 ip 192.168.1.1-192.168.1.90 port 2-5,8

type h,s action a

Synopsis: set name Mary vid 20 ip 192.168.1.1-192.168.1.90

- Description:

To edit management policy record.

- Argument:

[<name> <value>] ACL entry name.

DE

[<vid> <value>]	VLAN ID.
[<ip> <value>]	IP Range.
[<port> <value>]	Incoming port.
[<type> <value>]	Access type.
<action> <value>	a(ccept) or d(eny).

- Possible value:

[<name> <value>]	No default and it must be set.
[<vid> <value>]	The range is 1-4095 and can be set to any.
[<ip> <value>]	For example, 192.168.1.90-192.168.1.90 or any
[<port> <value>]	For example, 1 or 1-8 or 1,3-5 or any
[<type> <value>]	For example, h(ttp),s(nmp),t(elnet) or any
<action> <value>	No default and it must be set.

- Example:

```
PSES-2126C(management)# edit 1

PSES-2126C(management-edit-1)# set name Tom vid 2 ip
192.168.1.30-192.168.1.80 port 1-2 type s action d

PSES-2126C(management-edit-1)# show

 #: 1

Name : Tom                  VlanID : 2          IP :
192.168.1.30-192.168.1.80

Type : SNMP             Action : Deny      Port : 1,2
```

- **show**
  - Syntax:

    show
  - Description:

    To show the specific management policy record.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
PSES-2126C(management)# show
#: 1
Name : Tom                    VlanID : 2          IP :
192.168.1.30-192.168.1.80
Type : SNMP              Action : Deny      Port : 1,2
```


poe

- **set priority**
  - Syntax:

    set priority <port-range> <priority>
  - Description:

    To set the PoE priority on ports.
  - Argument:

    <port-range>¡G

    <priority>: set priority as 0:Low, 1:Normal, 2:High
  - Possible value:

    <port range>: 1 to 24

    <priority>: 0, 1 or 2
  - Example:

    `PSES-2126C(poe)# set priority 1-12 2`
- **set state**
  - Syntax:

    set state <port-range> <state>
  - Description:

    To set the PoE state on ports.
  - Argument:

    <port-range>¡G

    <state>: enable or disable PoE function. 0:Disable 1:Enable
  - Possible value:

    <port-range>¡G

    <state>: 0 or 1
  - Example:

DE

```
PSES-2126C(poe)# set state 11 0
```

- **show**
  - Syntax:

    show
  - Description:

    To display the PoE status.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
PSES-2126C(poe)# show
Vmain         : 48.3 V
Imain         : 0.0 A
Pconsume      : 0.0 W
Power Limit   : 185 W
Temperature   : 37 'C / 98 'F

Port No                 | 1  2  3  4  5  6  7  8  9  10  11  12
------------------------ | -  -  -  -  -  -  -  -  -  -  --  --
Port On                  | X  X  X  X  X  X  X  X  X  X   X   X
AC Disconnect Port Off   | X  X  X  X  X  X  X  X  X  X   X   X
DC Disconnect Port Off   | X  X  X  X  X  X  X  X  X  X   X   X
Overload Port Off        | X  X  X  X  X  X  X  X  X  X   X   X
Short Circuit Port Off   | X  X  X  X  X  X  X  X  X  X   X   X
Over Temp. Protection    | X  X  X  X  X  X  X  X  X  X   X   X
```

```
Power Management Port Off | X  X  X  X  X  X  X  X  X
X   X   X
```

```
Port No                   | 13 14 15 16 17 18 19 20 21
22  23  24
------------------------- | -- -- -- -- -- -- -- -- --
--  --  --
Port On                | X  X  X  X  X  X  X  X  X  X  X
AC Disconnect Port Off    | X  X  X  X  X  X  X  X  X
X   X   X
DC Disconnect Port Off    | X  X  X  X  X  X  X  X  X
X   X   X
Overload Port Off         | X  X  X  X  X  X  X  X  X
X   X   X
Short Circuit Port Off    | X  X  X  X  X  X  X  X  X
X   X   X
Over Temp. Protection     | X  X  X  X  X  X  X  X  X
X   X   X
Power Management Port Off | X  X  X  X  X  X  X  X  X
X   X   X
```

Port	Status	State	Priority	Power(W)	Current(mA)	Class
1	Normal	Enable	Normal	0.0	0	0
2	Normal	Enable	Normal	0.0	0	0
3	Normal	Enable	Normal	0.0	0	0
4	Normal	Enable	Normal	0.0	0	0
5	Normal	Enable	Normal	0.0	0	0
6	Normal	Enable	Normal	0.0	0	0
7	Normal	Enable	Normal	0.0	0	0
8	Normal	Enable	Normal	0.0	0	0

DE

```
 9  Normal Enable   Normal     0.0        0          0
10  Normal Enable   Normal     0.0        0          0
11  Normal Enable   Normal     0.0        0          0
12  Normal Enable   Normal     0.0        0          0
13  Normal Enable   Normal     0.0        0          0
14  Normal Enable   Normal     0.0        0          0
15  Normal Enable   Normal     0.0        0          0
16  Normal Enable   Normal     0.0        0          0
17  Normal Enable   Normal     0.0        0          0
18  Normal Enable   Normal     0.0        0          0
19  Normal Enable   Normal     0.0        0          0
20  Normal Enable   Normal     0.0        0          0
21  Normal Enable   Normal     0.0        0          0
22  Normal Enable   Normal     0.0        0          0
23  Normal Enable   Normal     0.0        0          0
24  Normal Enable   Normal     0.0        0          0
```

port

- **clear counter**
  - Syntax:

    clear counter
  - Description:

    To clear all ports' counter (include simple and detail port counter) information.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

    PSES-2126C(port)# clear counter
- **disable state**
  - Syntax:

disable state <range>

- Description:

To disable the communication capability of the port.

- Argument:

<range>: port range, syntax 1,5-7, available from 1 to 26

- Possible value:

<range>: 1 ~ 26

- Example:

PSES-2126C(port)# disable state 12

- **enable state**
  - Syntax:

enable state

- Description:

To enable the communication capability of the port.

- Argument:

<range>: port range, syntax 1,5-7, available from 1 to 26

- Possible value:

<range>: 1 ~ 26

- Example:

PSES-2126C(port)# enable state 3-10

- **set flow-control**
  - Syntax:

set flow-control <range> <symmetric|asymmetric>

- Description:

To set up the flow control function of all ports.

- Argument:

<range>:port range, syntax 1,5-7, available from 1 to 26

<symmetric>: set its flow control as symmetric

<asymmetric>: set its flow control as asymmetric

- Possible value:

<range>: 1 to 26

- Example:

PSES-2126C(port)# set flow-control 3-6 symmetric

- **set speed-duplex**
  - Syntax:

    set speed-duplex <range> <auto>|[<10|100|1000> <half|full>]
  - Description:

    To set up the speed and duplex of all ports.
  - Argument:

    <range>:port range, syntax 1,5-7, available from 1 to 26

    <port-speed>:

    auto : set auto-negotiation mode

    10 : set speed to 10M

    100 : set speed to 100M

    1000 : set speed to 1000M

    <port-duplex> :

    half : set to half duplex

    full : set to full duplex
  - Possible value:

    <range>: 1 to 26

    <port-speed> : auto, 10, 100, 1000

    <port-duplex> : full, half
  - Example:

    PSES-2126C(port)# set speed-duplex 8 100 full
- **show conf**
  - Syntax:

    show conf
  - Description:

    To display the each port's configuration about state, speed-duplex and flow control.
  - Argument:

    None.
  - Possible value:

    None.

- Example:

PSES-2126C(port)# show conf

- **show detail-counter**
  - Syntax:

show detail-counter <#>

  - Description:

To display the detailed counting number of each port's traffic.

  - Argument:

<#> : port, available from 1 to 26

  - Possible value:

<#>:1 ~ 26

  - Example:

PSES-2126C(port)# show detail-counter 6

- **show media**
  - Syntax:

show media <port>

  - Description:

To display the module 25 or 26 information.

  - Argument:

<port>: available 25, 26

  - Possible value:

<port>: 25, 26

  - Example:

PSES-2126C(port)# show media 25

```
Port 25 Fiber Media Information
-------------------------------------------------------
---------------
Connector Type        : SFP - LC
Fiber Type            : Multi-mode (MM)
Tx Central Wavelength : 850
Baud Rate             : 1G
Vendor OUI            : 00:40:c7
```

```
Vendor Name             : APAC Opto
Vendor PN               : KM28-C3S-TC-N
Vendor Rev              : 0000
Vendor SN               : 5425011140
Date Code               : 050530
Temperature             : none
Vcc                     : none
Mon1 (Bias) mA          : none
Mon2 (TX PWR)           : none
Mon3 (RX PWR)           : none
```

- **show simple-counter**
  - Syntax:

    show simple-counter
  - Description:

    To display the summary counting of each port's traffic.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

    PSES-2126C(port)# show simple-counter
- **show status**
  - Syntax:

    show status
  - Description:

    To display the port's current status.
  - Argument:

    None.
  - Possible value:

    None.

DE

□ Example:

```
PSES-2126C(port)# show status

Port Media Link  State  Auto Nego. Speed/Duplex Rx Pause
Tx Pause
---- ----- ---- ------- ---------- ------------ ------
-- --------
  1   TP   Down  Enable   Enable   ----/----     ----
----
  2   TP   Down  Enable   Enable   ----/----     ----
----
  3   TP   Down  Enable   Enable   ----/----     ----
----
  4   TP   Down  Enable   Enable   ----/----     ----
----
  5   TP   Up   Enable   Enable   100M/Full      ON     ON
  6   TP   Down  Enable   Enable   ----/----     ----
----
  7   TP   Down  Enable   Enable   ----/----     ----
----
                              :
                           :
                           :
 24   TP   Down  Enable   Enable   ----/----     ----
----
 25   TP   Down  Enable   Enable   ----/----     ----
----
 26   TP   Down  Enable   Enable   ----/----     ----
----
```

qos

■ **disable 1p**

□ Syntax:

disable 1p

DE

- Description:

  To disable 802.1p qos.

- Argument:

  None.

- Possible value:

  None.

- Example:

  PSES-2126C(qos)# disable 1p

disable dscp

- Syntax:

  disable dscp

- Description:

  To disable IP DSCP qos.

- Argument:

  None.

- Possible value:

  None.

- Example:

  PSES-2126C(qos)# disable dscp

disable qos

- Syntax:

  disable qos

- Description:

  To disable qos function.

- Argument:

  None.

- Possible value:

  None.

- Example:

  PSES-2126C(qos)# disable qos

disable tos

- Syntax:

disable tos

- Description:

To disable IP TOS qos.

- Argument:

None.

- Possible value:

None.

- Example:

PSES-2126C(qos)# disable tos

- **enable 1p**
  - Syntax:

enable 1p

- Description:

To enable 802.1p qos.

- Argument:

None.

- Possible value:

None.

- Example:

PSES-2126C(qos)# enable 1p

- **enable dscp**
  - Syntax:

enable dscp

- Description:

To enable IP DSCP qos.

- Argument:

None.

- Possible value:

None.

- Example:

PSES-2126C(qos)# enable dscp

DE

- **enable qos**
  - Syntax:

    enable qos
  - Description:

    To enable qos function.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

    PSES-2126C(qos)# enable qos
- **enable tos**
  - Syntax:

    enable tos
  - Description:

    To enable IP TOS qos.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

    PSES-2126C(qos)# enable tos
- **set dscp**
  - Syntax:

    set dscp [<q0><priority>] [<q1><priority>] [<q2><priority>] [<q3><priority>]
  - Description:

    To set IP DSCP qos weighting for 4 queues.
  - Argument:

    <q>: queue level, q0: queue 0; q1: queue 1; q2: queue 2; q3: queue 3.

    <priority>: priority level. One queue has been assigned 2 different priorities.

You don't need to use all of queue, but must assign queue in order.

Syntax: 1,2 or 2,5-7, available from 0 to 63.

- Possible value:

<priority>: 0 to 63

- Example:

PSES-2126C(qos)# set dscp q0 2 q1 2 q2 2 q3 3

- **set pri-tag**
  - Syntax:

set pri-tag [<q0><priority>] [<q1><priority>] [<q2><priority>] [<q3><priority>]

  - Description:

To set 802.1p qos weighting for 4 queues.

  - Argument:

<q>: queue level, q0: queue 0; q1: queue 1; q2: queue 2; q3: queue 3.

<priority>: priority level. One queue has been assigned 2 different priorities.

You don't need to use all of queues, but must assign queues in order.

  - Syntax: 1,2 or 2,5-7, available from 0 to 7.
  - Possible value:

<priority>: 0 to 7.

  - Example:

PSES-2126C(qos)# set pri-tag q0 0 q1 2 q3 4

- **set sche**
  - Syntax:

set sche <wrr|strict> <wrr_0> <wrr_1> <wrr_2> <wrr_3>

  - Description:

To set qos schedule and weight for 4 queues.

  - Argument:

<wrr> : scheduling weighted round robin method

<strict> : scheduling strict method.

<wrr_0 to 3>: weighted for every queue. Weighted range : 1-55.

  - Possible value:

<wrr|strict>: wrr or strict

<wrr_0 to 3>: 1-55.

- Example:

PSES-2126C(qos)# set sche wrr 1 2 8 16

- **set tos**
  - Syntax:

set tos <type_value> [<q0><priority>] [<q1><priority>] [<q2><priority>]

[<q3><priority>]

  - Description:

To set IP tos qos weighting for 4 queues.

  - Argument:

<type_value>: Delay Priority: 0;

Throughput Priority: 1;

Reliability Priority: 2;

Monetary Cost Priority: 3.

<q>: queue level, q0: queue 0; q1: queue 1; q2: queue 2; q3: queue 3.

<priority>: priority level. One queue has been assigned 2 different priorities.

You don't need to use all of queues, but must assign queues in order (from low queue to high queue).

  - Syntax: 1,2 or 2,5-7, available from 0 to 7.
  - Possible value:

<type_value>: 0~3

<priority>: 0 to 7.

  - Example:

PSES-2126C(qos)# set tos 0 q0 1 q1 2 q2 4 q3 6

- **set vip**
  - Syntax:

set vip <port_range> <mode>

  - Description:

To set vip port for strict priority.

- Argument:

<port_range>: syntax 1,5-7, available from 1 to 26

<mode>: enable/disable vip port for each port. 1: enable. 0: disable.

- Possible value:

<port_range>: 1 to 26

<mode>: 1 or 0

- Example:

PSES-2126C(qos)# set vip 1-6 1

- **show dscp**
  - Syntax:

show dscp

- Description:

To show IP DSCP Qos configuration.

- Argument:

None.

- Possible value:

None.

- Example:

```
PSES-2126C(qos)# show dscp
ip diffserv classification
====================
Global QoS mode: Enable QoS
                 Disable 802.1p Priority
                 Disable ip tos classification
                 Enable ip diffserv classification
Scheduling:      weighted round robin method.
weight:          wrr 0 = 1; wrr 1 = 1; wrr 2 = 8; wrr 3
= 16.
                 weighted range: 1~55.
P0~63:           Priority 0~63.
Default mode:    Queue0: P0~15; Queue1: P16~31; Queue2:
P32~47; Queue3: P48~63.
```

DE

```
 DiffServ   Queue   DiffServ   Queue   DiffServ   Queue
DiffServ   Queue
---------- ------- ---------- ------- ---------- -----
-- ---------- ------
     0          0         1          0         2          0
3          0
     4          0         5          0         6          0
7          0
     8          0         9          0        10          0
11         0
    12          0        13          0        14          0
15         0
    16          1        17          1        18          1
19         1
    20          1        21          1        22          1
23         1
    24          1        25          1        26          1
27         1
    28          1        29          1        30          1
31         1
    32          2        33          2        34          2
35         2
    36          2        37          2        38          2
39         2
    40          2        41          2        42          2
43         2
    44          2        45          2        46          2
47         2
    48          3        49          3        50          3
51         3
    52          3        53          3        54          3
55         3
```

```
    56          3       57          3       58          3
59          3
    60          3       61          3       62          3
63          3
```

- **show port**
  - Syntax:

    show port
  - Description:

    To show VIP port configuration.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
PSES-2126C(qos)# show port
Port Based Priority
====================
Global QoS mode: Enable QoS
                 Enable 802.1p Priority
                 Disable ip tos classification
                 Disable ip diffserv classification
 Port No  Mode    Port No   Mode
-------- -------  --------- -------
    1     Enable       2     Enable
    3     Enable       4     Enable
    5     Enable       6     Enable
            :
            :
   23    Disable      24    Disable
   25    Disable      26    Disable
```

DE

show priority-tag

- Syntax:

show priority-tag

- Description:

To show 802.1p Qos configuration.

- Argument:

None.

- Possible value:

None.

- Example:

```
PSES-2126C(qos)# show priority-tag
802.1p priority
====================
Global QoS mode: Enable QoS
                 Enable 802.1p Priority
                 Disable ip tos classification
                 Disable ip diffserv classification
Scheduling:      weighted round robin method.
weight:          wrr 0 = 1; wrr 1 = 1; wrr 2 = 8; wrr 3
= 16.
                 weighted range: 1~55.
P0~7:            Priority 0~7.
Default mode:    Queue0: P0,P1; Queue1: P2,P3; Queue2:
P4,P5; Queue3: P6,P7.

        P0   P1   P2   P3   P4   P5   P6   P7
      ---- ---- ---- ---- ---- ---- ---- ----
Queue  0    0    1    1    2    2    3    3
```

DE

show tos

- Syntax:

show tos

- Description:

To show IP tos Qos configuration.

- Argument:

None.

- Possible value:

None.

- Example:

```
PSES-2126C(qos)# show tos
ip tos classification
====================
Global QoS mode: Enable QoS
                 Disable 802.1p Priority
                 Enable ip tos classification
                 Disable ip diffserv classification
Scheduling:      weighted round robin method.
weight:          wrr 0 = 1; wrr 1 = 1; wrr 2 = 8; wrr 3
= 16.
                 weighted range: 1~55.
P0~7:            Priority 0~7.
Default mode:    Queue0: P0,P1; Queue1: P2,P3; Queue2:
P4,P5; Queue3: P6,P7.

       P0   P1   P2   P3   P4   P5   P6   P7
      ---- ---- ---- ---- ---- ---- ---- ----
Queue  0    0    1    1    2    2    3    3
TOS type: Delay Priority
```

DE

```
        P0   P1   P2   P3   P4   P5   P6   P7
       ---- ---- ---- ---- ---- ---- ---- ----
Queue  0    0    1    1    2    2    3    3
TOS type: Throughput Priority

        P0   P1   P2   P3   P4   P5   P6   P7
       ---- ---- ---- ---- ---- ---- ---- ----
Queue  0    0    1    1    2    2    3    3
TOS type: Reliability Priority

        P0   P1   P2   P3   P4   P5   P6   P7
       ---- ---- ---- ---- ---- ---- ---- ----
Queue  0    0    1    1    2    2    3    3
TOS type: Monetary Cost Priority
```

reboot

- **reboot**
  - Syntax:

    reboot
  - Description:

    To reboot the system.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

    PSES-2126C# reboot

security

<<isolated-group>>

- **set**
  - Syntax:

    set <port>
  - Description:

    To set up the function of the isolated group.
  - Argument:
  - <port> : isolated port; range syntax: 1,5-7, available from 0 to 26

    set 0 as disabled
  - Possible value:

    <port>:0 to 26
  - Example:

    PSES-2126C(security-isolated-group)# set 2,3,4
- **show**
  - Syntax:

    show
  - Description:

    To display the current setting status of isolated group.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

    PSES-2126C(security-isolated-group)# show

    Isolated group:

    2 3 4

    <<mirror>>
- **disable**
  - Syntax:

    disable
  - Description:

    To disable the function of mirror.
  - Argument:

None.

- Possible value:

None.

- Example:

PSES-2126C(security-mirror)# disable

- **enable**
  - Syntax:

enable

- Description:

To enable the function of mirror.

- Argument:

None.

- Possible value:

None.

- Example:

PSES-2126C(security-mirror)# enable

- **set**
  - Syntax:

set <spy> <ingress> <egress>

- Description:

To set up the monitoring port and monitored ports of the mirror function. User can monitor the ports that receive or transmit the packets.

- Argument:

<spy>: monitoring port

- <ingress>: monitored ingress port; range syntax: 1,5-7, available from 0 to 26
- <egress>: monitored egress port; range syntax: 1,5-7, available from 0 to 26

  set ingress/egress to 0 as ingress/egress disabled

- Possible value:

<ingress>: 0 to 26

<egress>: 0 to 26

- Example:

PSES-2126C(security-mirror)# set 1 4 2-3

- **show**
  - Syntax:

  show
  - Description:

  To display the current setting status of mirror.
  - Argument:

  None.
  - Possible value:

  None.
  - Example:

  PSES-2126C(security-mirror)# show

  Mirror:

  Monitoring Port :1

  Monitored Ingress :4

  Monitored Egress :2 3

snmp

- **disable**
  - Syntax:

  disable set-community

  disable snmp
  - Description:

  The Disable here is used for the de-activation of snmp or set-community.
  - Argument:

  None.
  - Possible value:

  None.
  - Example:

  ```
  PSES-2126C(snmp)# disable set-community
  PSES-2126C(snmp)# disable snmp
  ```

DE

- **enable**
  - Syntax:

    enable set-community

    enable snmp
  - Description:

    The Enable here is used for the activation snmp or set-community.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

    ```
    PSES-2126C(snmp)# enable set-community
    PSES-2126C(snmp)# enable snmp
    ```
- **set**
  - Syntax:

    set get-community <community>

    set set-community <community>

    set trap <#> <ip> [port] [community]
  - Description:

    The Set here is used for the setup of get-community, set-community, trap host ip, host port and trap- community.
  - Argument:

    <#>: trap number, range: 1 to 6

    <ip>: ip address or domain name

    <port>: trap port

    <community>: community name
  - Possible value:

    <trap number> : 1 to 6

    <port> :1~65535
  - Example:

    ```
    PSES-2126C(snmp)# set get-community public
    PSES-2126C(snmp)# set set-community private
    ```

```
PSES-2126C(snmp)# set trap 1 192.168.1.1 162 public
```

- **show**
  - **Syntax**:

    show
  - Description:

    The Show here is to display the configuration of SNMP.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
PSES-2126C(snmp)# show
SNMP          : Enable
Get Community: public
Set Community: private [Enable]
Trap Host 1 IP Address: 192.168.1.1 Port: 162 Community:
public
Trap Host 2 IP Address: 0.0.0.0 Port: 162 Community:
public
Trap Host 3 IP Address: 0.0.0.0 Port: 162 Community:
public
Trap Host 4 IP Address: 0.0.0.0 Port: 162 Community:
public
Trap Host 5 IP Address: 0.0.0.0 Port: 162 Community:
public
Trap Host 6 IP Address: 0.0.0.0 Port: 162 Community:
public
```

stp

- **MCheck**
  - Syntax:

    MCheck <range>
  - Description:

To force the port to transmit RST BPDUs.

- Argument:

<range>: syntax 1,5-7, available from 1 to 26

- Possible value:

<range>: 1 to 26

- Example:

PSES-2126C(stp)# Mcheck 1-8

- **disable**
  - Syntax:

disable

  - Description:

To disable the function of STP.

  - Argument:

None.

  - Possible value:

None.

  - Example:

PSES-2126C(stp)# disable

- **enable**
  - Syntax:

enable

  - Description:

To enable the function of STP.

  - Argument:

None.

  - Possible value:

None.

  - Example:

PSES-2126C(stp)# enable

- **set config**
  - Syntax:

set config <Bridge Priority> <Hello Time> <Max. Age> <Forward Delay>

- Description:

To set up the parameters of STP.

- Argument:

<Bridge Priority>: priority must be a multiple of 4096,available from 0 to 61440.

<Hello Time>: available from 1 to 10.

<Max. Age>: available from 6 to 40.

<Forward Delay>: available from 4 to 30.

Note: 2*(Forward Delay -1) >= Max Age

Max Age >= 2*(Hello Time +1)

- Possible value:

<Bridge Priority>: 0 to 61440.

<Hello Time>: 1 to 10.

<Max. Age>: 6 to 40.

<Forward Delay>: 4 to 30.

- Example:

PSES-2126C(stp)# set config 61440 2 20 15

set port

- Syntax:

set port <range> <path cost> <priority> <edge_port> <admin p2p>

- Description:

To set up the port information of STP.

- Argument:

<range>: syntax 1,5-7, available from 1 to 26

<path cost>: 0, 1-200000000. The value zero means auto status

<priority>: priority must be a multiple of 16, available from 0 to 240

<edge_port>: Admin Edge Port, <yes|no>

<admin p2p>: Admin point to point, <auto|true|false>

- Possible value:

<range> :1 to 26 <path cost>: 0, 1-200000000.

<priority> : 0 to 240 <edge_port> : yes / no

<admin p2p>: auto / true / false

- Example:

PSES-2126C(stp)# set port 1-16 0 128 yes auto

- **set version**
  - Syntax:

set version <stp|rstp>

  - Description:

To set up the version of STP.

  - Argument:

<stp|rstp>:stp / rstp

  - Possible value:

<stp|rstp>:stp / rstp

  - Example:

PSES-2126C(stp)# set version rstp

- **show config**
  - Syntax:

show config

  - Description:

To display the STP configuration data.

  - Argument:

None.

  - Possible value:

None.

  - Example:

```
PSES-2126C(stp)# show config
STP State Configuration :
Spanning Tree Protocol    : Enabled
Bridge Priority (0-61440) : 61440
Hello Time (1-10 sec)     : 2
Max. Age (6-40 sec)       : 20
Forward Delay (4-30 sec)  : 15
Force Version             : RSTP
```

show port

- Syntax:

show port

- Description:

To display the port information of STP.

- Argument:

None.

- Possible value:

None.

- Example:

```
PSES-2126C(stp)# show port

Port  Port  Status      Path Cost  Priority  Admin  Edge  Port
Admin Point To Point

====  ============  =========  ========  ===============
====================

   1   DISCARDING      2000000      128             Yes
Auto

   2   DISCARDING      2000000      128             Yes
Auto

   3   DISCARDING      2000000      128             Yes
Auto

   4   DISCARDING      2000000      128             Yes
Auto

   5   DISCARDING      2000000      128             Yes
Auto

                  :

                  :

                  :

  23   DISCARDING       200000      128              No
Auto

  24   DISCARDING       200000      128              No
Auto
```

```
  25    DISCARDING          20000       128              No
Auto
  26    DISCARDING          20000       128              No
Auto
```

- **show status**
  - Syntax:

    show status
  - Description:

    To display of the status of STP.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
PSES-2126C(stp)# show status
STP Status :
STP State                              : Enabled
Bridge ID                             : 00:40:C7:D8:09:1D
Bridge Priority                        : 61440
Designated Root                       : 00:40:C7:D8:09:1D
Designated Priority                    : 61440
Root Port                              : 0
Root Path Cost                         : 0
Current Max. Age(sec)                  : 20
Current Forward Delay(sec)             : 15
Hello Time(sec)                        : 2
STP Topology Change Count              : 0
Time Since Last Topology Change(sec)  : 848
```

system

- **set contact**
  - Syntax:

set contact <contact>

- Description:

To set the contact description of the switch.

- Argument:

<contact>:string length up to 40 characters.

- Possible value:

<contact>: A, b, c, d, ... ,z and 1, 2, 3, …. etc.

- Example:

PSES-2126C(system)# set contact Taipei

- **set device-name**
  - Syntax:

set device-name <device-name>

- Description:

To set the device name description of the switch.

- Argument:

<device-name>: string length up to 40 characters.

- Possible value:

<device-name>: A, b, c, d, ... ,z and 1, 2, 3, …. etc.

- Example:

PSES-2126C(system)# set device-name CR-2600

- **set location**
  - Syntax:

set location <location>

- Description:

To set the location description of the switch.

- Argument:

<location>: string length up to 40 characters

- Possible value:

<location>: A, b, c, d, ... ,z and 1, 2, 3, …. etc.

- Example:

PSES-2126C(system)# set location Taipei

DE

- **show**
  - Syntax:

    show
  - Description:

    To display the basic information of the switch.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
PSES-2126C(system)# show
Model Name                      : PSES-2126C
System Description               : 24-Port 10/100BaseT/TX
Managed PoE Switch
Location                        :
Contact                         :
Device Name                     : PSES-2126C
System Up Time              : 0 Days 0 Hours 4 Mins 50 Secs
Current Time                   : Wed Feb 08 16:55:29 2006
BIOS Version                    : v1.05
Firmware Version                : v2.07
Hardware-Mechanical Version   : v1.01-v1.01
Serial Number                   : 031203000004
Host IP Address                 : 192.168.1.1
Host MAC Address                : 00-00-8c-00-d8-00
Device Port                  : UART * 1  TP *24  Fiber * 2
RAM Size                        : 16 M
Flash Size                      : 2 M
```

tac-plus

- **show access**
  - Syntax:

show access

- Description:

Shows the access configuration.

- Example:

```
ES-2126+(tac-plus)# show access
Access retry : 3
Access    Login     Login
          Primary   Secondary
-------   -------   ---------
Console   Local     None
Telnet    TACACS    Local
Web       TACACS    Local
```

- **show tac-plus**
  - Syntax:

show tac-access

- Description:

Shows the TACACS+ configuration.

- Example:

```
ES-2126+(tac-plus)# show tac-plus
Authorization                   : Enable
Fallback to Local Authorization: Enable
Accounting                      : Enable
Secret Key: secret
#     Server IP
- ---------------
1   10.1.1.1
2   0.0.0.0
```

- **enable**
  - Syntax:

enable <argument>

- Description:

Enables the TACACS+ functions for accounting, authorization and fallback to local authorization.

- Arguments:

Accounting: enables the TACACS+ accounting.

Authorization: enables the TACACS+ authorization.

Fallback-author: enables the fallback to local authorization.

- **disable**
  - Syntax:

disable <argument>

  - Description:

Disables the TACACS+ functions for accounting, authorization and fallback to local authorization.

  - Arguments:

Accounting: disables the TACACS+ accounting.

Authorization: disables the TACACS+ authorization.

Fallback-author: disables the fallback to local authorization.

- **set console-access**
  - Syntax:

set console-access <method1> <method2>

  - Description:

Sets the primary and secondary access mode for the login via console (outband).

  - Arguments:

Method from 0 to 2:

0: Authentication via local user accounts of the device.

1: Authentication via TACACS+-Server.

2: No authentication required (for method 2 only).

  - Example:

ES-2126+(tac-plus)# set console-access 1 0

Sets the primary access mode for the login via console to TACACS+ and the secondary access mode to local user accounts.

- **set host**
  - Syntax:

    set host <#> <ip>
  - Description:

    Sets the IP addresses for the first and secondary TACACS+ server.
  - Arguments:

    #: Number from 1 (first TACACS+ server) to 2 (secondary TACACS+ server).

    ip: IP address of the TACACS+ server
  - Example:

    ES-2126+(tac-plus)# set host 1 10.1.1.1

    Sets the IP address of the primary TACACS+ server to "10.1.1.1".
- **set key**
  - Syntax:

    set key <secret-key>
  - Description:

    Sets the encryption key for the communication with the TACACS+ server. This key must correspond with the encryption key which is configured in the TACACS+ server.
  - Arguments:

    secret-key: maximum 31 characters.
  - Example:

    ES-2126+(tac-plus)# set key secret

    Sets the encryption key to "secret".
- **set retry**
  - Syntax:

    set retry <retry>
  - Description:

    Sets the access retry value. When the login failed for the number of retries, the secondary login method will be used.

    If TACACS+ is defined as primary access mode, the secondary TACACS+ server is used after the number of login failures has reached the access retry value. After the number of login failures has reached the access retry

value even on the secondary TACACS+ server, the secondary login method will be used.

- Arguments:

retry: 1 to 3.

- Example:

ES-2126+(tac-plus)# set retry 2

Sets the access retry value to "2".

- **set telnet-access**
  - Syntax:

set telnet-access <method1> <method2>

  - Description:

Sets the primary and secondary access mode for the login via telnet.

  - Arguments:

Method from 0 to 2:

0: Authentication via local user accounts of the device.

1: Authentication via TACACS+-Server.

2: No authentication required (for method 2 only).

  - Example:

ES-2126+(tac-plus)# set telnet-access 1 0

Sets the primary access mode for the login via telnet to TACACS+ and the secondary access mode to local user accounts.

- **set web-access**
  - Syntax:

set web-access <method1> <method2>

  - Description:

Sets the primary and secondary access mode for the login via web browser.

  - Arguments:

Method from 0 to 2:

0: Authentication via local user accounts of the device.

1: Authentication via TACACS+-Server.

2: No authentication required (for method 2 only).

- Example:

ES-2126+(tac-plus)# set web-access 1 0

Sets the primary access mode for the login via web browser to TACACS+ and the secondary access mode to local user accounts.

tftp

- **set server**
  - Syntax:

set server <ip>

  - Description:

To set up the IP address of tftp server.

  - Argument:

<ip>: the IP address of tftp server

  - Possible value:

<ip>: tftp server IP

  - Example:

PSES-2126C(tftp)# set server 192.168.3.111

- **show**
  - Syntax:

show

  - Description:

To display the information of tftp server.

  - Argument:

None.

  - Possible value:

None.

  - Example:

PSES-2126C(tftp)# show

Tftp Server : 192.168.3.111

time

- **set daylightsaving**
  - Syntax:

set daylightsaving <hr> <MM/DD/HH> <mm/dd/hh>

- Description:

To set up the daylight saving.

- Argument:

```
<hr>   : daylight saving hour, range: -5 to +5
<MM>   : daylight saving start Month (01-12)
<DD>   : daylight saving start Day (01-31)
<HH>   : daylight saving start Hour (00-23)
<mm>   : daylight saving end Month (01-12)
<dd>   : daylight saving end Day (01-31)
<hh>   : daylight saving end Hour (00-23)
```

- Possible value:

```
<hr>   : -5 to +5
<MM>   : (01-12)
<DD>   : (01-31)
<HH>   : (00-23)
<mm>   : (01-12)
<dd>   : (01-31)
<hh>   : (00-23)
```

- Example:

PSES-2126C(time)# set daylightsaving 3 10/12/01 11/12/01

set manual

- Syntax:

set manual <YYYY/MM/DD> <hh:mm:ss>

- Description:

To set up the current time manually.

- Argument:

```
<YYYY> : Year   (2000-2036)    <MM>  : Month  (01-12)
<DD>   : Day    (01-31)        <hh>  : Hour   (00-23)
<mm>   : Minute (00-59)        <ss>  : Second (00-59)
```

- Possible value:

<YYYY>: (2000-2036) <MM> : (01-12)

<DD> : (01-31) <hh> : (00-23)

<mm> : (00-59) <ss> : (00-59)

- Example:

PSES-2126C(time)# set manual 2005/04/21 16:18:50

- **set ntp**
  - Syntax:

set ntp <ip> <timezone>

  - Description:

To set up the current time via NTP server.

  - Argument:

<ip>: ntp server ip address or domain name

<timezone>: time zone (GMT), range: -12 to +13

  - Possible value:

<timezone>: -12,-11…,0,1…,13

  - Example:

PSES-2126C(time)# set ntp clock.via.net 8

Synchronizing...(1)

Synchronization success

- **show**
  - Syntax:

show

  - Description:

To show the time configuration, including “Current Time”, “NTP Server”,” Timezone”,
” Daylight Saving”,” Daylight Saving Start” and “Daylight Saving End”

  - Argument:

None.

  - Possible value:

None.

  - Example:

PSES-2126C(time)# show

```
   Current Time          : Wed Apr 21 06:16:22 2005
NTP Server            : 209.81.9.7
   Timezone              : 8
   Day light Saving      : 4 Hours
   Day light Saving Start: Mth: 2 Day: 20 Hour: 10
   Day light Saving End  : Mth: 3 Day: 20 Hour: 10
```

trunk

- **del trunk**
  - Syntax:

    del trunk <port-range>
  - Description:

    To remove the trunk port.
  - Argument:

    <port-range> : syntax 1,5-7, available from 1 to 26
  - Possible value:

    <port-range> : 1 to 26
  - Example:

    PSES-2126C(trunk)# del trunk 1
- **set hash**
  - Syntax:

    set hash <method>
  - Description:

    To set up trunk hash method.
  - Argument:

    <method>: lacp hash method

    0: DA and SA

    1: SA

    2: DA

    Note : This hash method applies to both LACP and static trunk.
  - Possible value:

    <method>: 0~2

- Example:

PSES-2126C(trunk)# set hash 2

- **set priority**
  - Syntax:

set priority <range>

  - Description:

To set up the LACP system priority.

  - Argument:

<range>:available from 1 to 65535.

  - Possible value:

<range>:1 to 65535.

  - Example:

PSES-2126C(trunk)# set priority 33333

- **set trunk**
  - Syntax:

set trunk <port-range> <method> <group> <active LACP>

  - Description:

To set up the status of trunk, including the group number and mode of the trunk as well as LACP mode.

  - Argument:

<port-range> : syntax 1,5-7, available from 1 to 26

<method>: <static|lacp>

static : adopt the static link aggregation

lacp : adopt the dynamic link aggregation- link aggregation control protocol

<group>: 1-3.

<active LACP>: <passive|active>

active : set the LACP to active mode

passive : set the LACP to passive mode

  - Possible value:

<port-range> : 1 to 26

<method>: static or lacp

<group>: 1-3.

<active LACP>: active or passive

- Example:

PSES-2126C(trunk)# set trunk 2-5 lacp 1 active

- **show aggtr-view**
  - Syntax:

show aggtr-view

  - Description:

To display the aggregator list.

  - Argument:

None.

  - Possible value:

None.

  - Example:

PSES-2126C(trunk)# show aggtr-view

```
Aggregator  1) Method: None
               Member Ports: 1
               Ready Ports:1

Aggregator  2) Method: LACP
               Member Ports: 2
               Ready Ports:
                  :
                  :
                  :
```

- **show lacp-config**
  - Syntax:

show lacp-config

  - Description:

To display the value of LACP Priority.

DE

- Argument:

None.

- Possible value:

None.

- Example:

PSES-2126C(trunk)# show lacp-config

LACP System Priority : 33333

Hash Method : DA

- **show lacp-detail**
  - Syntax:

show lacp-detail <aggtr>

- Description:

To display the detailed information of the LACP trunk group.

- Argument:

<aggtr> : aggregator, available from 1 to 26

- Possible value:

<aggtr> : 1 to 26

- Example:

PSES-2126C(trunk)# show lacp-detail 2

```
Aggregator 2 Information:
              Actor                                Partner
---------------------------------  --------------------
-------------
System Priority    MAC Address    System Priority    MAC
Address
---------------  -----------------  ---------------  ----
-------------
     32768       00-40-c7-e8-00-02       32768       00-
00-00-00-00-00

 Port    Key      Trunk Status        Port            Key
```

DE

```
------ -------- ---------------- --------------- ----
-------------
   2     257          ---              2               0
```

show status

- Syntax:

show status

- Description: Description:

To display the aggregator status and the settings of each port.

- Argument:

None.

- Possible value:

None.

- Example:

```
PSES-2126C(trunk)# show status
         Trunk Port Setting           Trunk Port Status
------------------------------------ ----------------
------
 port    Method    Group    Active LACP    Aggtregator
Status
======  ========  =======  =============  =============
========
   1     None      0       Active           1        Ready
   2     LACP      1        Active           2         ---
   3     LACP      1        Active           3         ---
   4     LACP      1        Active           4         ---
   5     LACP      1        Active           5         ---
   6     None      0        Active           6         ---
   7     None      0        Active           7         ---
   8     None      0        Active           8         ---
   9     None      0        Active           9         ---
  10     None      0        Active          10         ---
  11     None      0        Active          11         ---
```

12	None	0	Active	12	---
13	None	0	Active	13	---
14	None	0	Active	14	---
15	None	0	Active	15	---
16	None	0	Active	16	---
17	None	0	Active	17	---
18	None	0	Active	18	---
19	None	0	Active	19	---
20	None	0	Active	20	---
21	None	0	Active	21	---
22	None	0	Active	22	---
23	None	0	Active	23	---
24	None	0	Active	24	---
25	None	0	Active	25	---
26	None	0	Active	26	---

VLAN

- **del port-group**
  - Syntax:

    del port-group <name>
  - Description:

    To delete the port-based VLAN group.
  - Argument:

    <name>: port-VLAN name
  - Possible value:

    <name>: port-VLAN name
  - Example:

    PSES-2126C(VLAN)# del port-group VLAN-2
- **del tag-group**
  - Syntax:

    del tag-group <vid>
  - Description:

To delete the tag-based VLAN group.

- Argument:

<vid>: VLAN ID, available from 1 to 4094

- Possible value:

<vid>: 1 to 4094

- Example:

PSES-2126C(VLAN)# del tag-group 2

- **disable double-tag**
  - Syntax:

disable double-tag

  - Description:

To disable double-tag.

  - Argument:

None.

  - Possible value:

None.

  - Example:

PSES-2126C(VLAN)# disable double-tag

- **disable drop-untag**
  - Syntax:

disable drop-untag <port_range>

  - Description:

To disable drop-untag.

  - Argument:
  - <port_range>: which port(s) you want not to drop untagged frames. Syntax: 1,5-7, available from 1 to 26
  - Possible value:

<port_range>: 1 to 26

  - Example:

PSES-2126C(VLAN)# disable drop-untag 2,4,5-7

- **disable svl**
  - Syntax:

disable svl

- Description:

To enable Independent VLAN Learning.

- Argument:

None.

- Possible value:

None.

- Example:

PSES-2126C(VLAN)# disable svl

- **disable symmetric**
  - Syntax:

disable symmetric

  - Description:

To Not drop frames from the non-member port.

  - Argument:

None.

  - Possible value:

None.

  - Example:

PSES-2126C(VLAN)# disable symmetric

- **enable double-tag**
  - Syntax:

enable double-tag

  - Description:

To enable double-tag.

  - Argument:

None.

  - Possible value:

None.

  - Example:

PSES-2126C(VLAN)# enable double-tag

DE

- **enable drop-untag**
  - Syntax:

    enable drop-untag <port_range>
  - Description:

    To enable drop-untag.
  - Argument:
  - <port_range>: which port(s) you want to drop untagged frames. Syntax: 1,5-7, available from 1 to 26
  - Possible value:

    <port_range>: 1 to 26
  - Example:

    PSES-2126C(VLAN)# enable drop-untag 2,4,5-7
- **enable svl**
  - Syntax:

    enable svl
  - Description:

    To enable Shared VLAN Learning.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

    PSES-2126C(VLAN)# enable svl
- **enable symmetric**
  - Syntax:

    enable symmetric
  - Description:

    To drop frames from the non-member port.
  - Argument:

    None.
  - Possible value:

    None.

- Example:

PSES-2126C(VLAN)# enable symmetric

- **set mode**
  - Syntax:

set mode <port|tag>

  - Description:

To switch VLAN mode between port-based and tag-based modes.

  - Argument:

<port|tag>: port or tag

tag: set tag-based VLAN

port: set port-based VLAN

  - Possible value:

<port|tag>: port or tag

  - Example:

PSES-2126C(VLAN)# set mode tag

- **set port-group**
  - Syntax:

set port-group <name> <range>

  - Description:

To add or edit a port-based VLAN group.

  - Argument:

<name>: port-VLAN name

  - <range>: VLAN group members, syntax: 1,5-7, available from 1 to 26
  - Possible value:

<range>: 1 to 26

  - Example:

PSES-2126C(VLAN)# set port-group VLAN-1 2-5,6-10

- **set pvid**
  - Syntax:

set pvid <port_range> <pvid> <default_priority>

  - Description:

To set VLAN PVID and port pripority.

DE

- Argument:

<port_range>: which port(s) you want to set PVID(s). Syntax 1,5-7, available from 1 to 26

<pvid>: which PVID you want to set, available from 1 to 4094

<default_priority>: which priority you want to set, available from 0 to 7

- Possible value:

<port_range>: 1 to 26

<pvid>: 1 to 4094

<default_priority>: 0 to 7

- Example:

PSES-2126C(VLAN)# set pvid 3,5,6-8 5 6

set tag-group

- Syntax:

set tag-group <vid> <name> <member_range> <untag_range>

- Description:

To add or edit the tag-based VLAN group.

- Argument:

<vid>: VLAN id, from 1 to 4094

<name>: tag-VLAN group name

- <member_range>: member port; syntax: 1,5-7, available from 1 to 26
- <untag_range>: untagged out port; syntax: 1,5-7, available from 0 to 26

  set untag_range to 0 as none of the ports are force untagged

- Possible value:

<vid>: 1 to 4094

<member_range>: 1 to 26

<untag_range>: 0 to 26

- Example:

PSES-2126C(VLAN)# set tag-group 2 VLAN-2 2-5,6,15-13 0

show config

- Syntax:

show config

- Description:

To display the current VLAN mode, Symmetric VLAN, SVL and Double tag states.

- Argument:

None.

- Possible value:

None.

- Example:

PSES-2126C(VLAN)# show config

```
Current VLAN mode:Tag-based VLAN
Global setting:
Symmetric VLAN  : Disable (Asymmetric)
SVL             : Disable (IVL)
Double tag      : Disable
```

- **show group**
  - Syntax:

show group

- Description:

To display VLAN mode and VLAN group.

- Argument:

None.

- Possible value:

None.

- Example:

PSES-2126C(VLAN)# show group

```
Vlan mode is tag-based.

1)  Name  :default
```

```
    VID   :1
    Member:1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
19 20 21 22 23 24
          25 26
    Untag :1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
19 20 21 22 23 24
          25 26
2)  Name  :VLAN-2
    VID   :2
    Member:2 3 4 5 6 13 14 15
    Untag :
```

- **show pvid**
  - Syntax:

    show pvid
  - Description:

    To display pvid, priority and drop untag result.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
PSES-2126C(VLAN)# show pvid
 Port   PVID   Priority   Drop Untag
------ ------ ---------- ------------
   1       1        0      Disable
   2       1        0      Disable
   3       5        6      Disable
   4       1        0      Disable
   5       5        6      Disable
   6       5        6      Disable
   7       5        6      Disable
   8       5        6      Disable
```

```
  9        1          0       Disable
 10        1          0       Disable
 11        1          0       Disable
 12        1          0       Disable
 13        1          0       Disable
 14        1          0       Disable
 15        1          0       Disable
 16        1          0       Disable
 17        1          0       Disable
 18        1          0       Disable
 19        1          0       Disable
 20        1          0       Disable
 21        1          0       Disable
 22        1          0       Disable
 23        1          0       Disable
 24        1          0       Disable
 25        1          0       Disable
 26        1          0       Disable
```

vs

- **disable**
  - Syntax:

    disable
  - Description:

    To disable the virtual stack.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

    ```
    PSES-2126C(vs)# disable
    ```

DE

- **enable**
  - Syntax:

    enable
  - Description:

    To enable the virtual stack.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

    ```
    PSES-2126C(vs)# enable
    ```
- **set gid**
  - Syntax:

    set gid <gid>
  - Description:

    To set the group id.
  - Argument:

    <gid>: group ID
  - Possible value:

    <gid>: a-z,A-Z,0-9
  - Example:

    PSES-2126C(vs)# set gid group1
- **set role**
  - Syntax:

    set role <master|slave>
  - Description:

    To set role.
  - Argument:

    <master|slave>: master: act as master, slave : act as slave
  - Possible value:

    <master|slave>: master or slave
  - Example:

PSES-2126C(vs)# set role master

- **show**
  - Syntax:

  show
  - Description:

  To display the configuration of the virtual stack.
  - Argument:

  None.
  - Possible value:

  None.
  - Example:

  PSES-2126C(vs)# show

```
Virtual Stack Config:
State     : Enable
Role      : Master
Group ID  : group1
```

6 Anhang

6.1 Leistungs- und Kenndaten

		LANCOM ES-2126+	LANCOM ES-2126P
Performance	Switching Technologie	Store and forward mit Latenzzeiten kleiner 5 µs	
	Anzahl MAC-Adressen	Unterstützung von maximal 8K MAC-Adressen	
	Durchsatz	maximal 8,8 Gbit/s auf der Backplane	
	Virtual Stacking Management (VSM)	Unterstützt Stacking von bis zu 16 Geräten, mehrere Switche können über eine IP-Adresse verwaltet werden	
	VLAN	Port-basiertes und IEEE 802.1q tag-basiertes VLAN mit bis zu 4096 VLAN und bis zu 256 aktiven VLANs; Unterstützung von Ingress und Egress Paket-Filtern im Port-basierten VLAN	
LAN-Protokolle	Link Aggregation Control Protocol (LACP)	2 Fast- und 1 Gigabit-Ethernet Gruppe, maximal 4 Mitglieder pro Gruppe, Unterstützt DA, SA und DA+SA MAC basiertes Trunking mit automatischem Fail-over	
	Multicasting	Unterstützt IGMP snooping inklusive aktivem und passivem Modus	
	GVRP/GARP	802.1q mit GVRP/GARP	
	Spanning Tree Protokoll (STP) / Rapid STP	802.1d/1w	
802.3af Features	Ports		24x 802.3af PoE Ports
	Leistung		Maximal 185 Watt Leistung mit dynamischer Leistungsverteilung auf allen Ports (z. B. bis 15,4 Watt für 12 Ports oder 7,7 Watt für 24 Ports)
	Priorisierung		Unterstützt Port-basierte Priorisierung und Setzten des PoE Status
	Statusanzeigen		Überwachung per LED, Anzeige der momentanen Leistung pro Port im Webinterface
Anschlüsse	Ethernet Ports	24 Ports 10/100 Mbit/s Fast Ethernet, 2 Combo-Ports TP/SFP 10/100/1000 Mbit/s	
	Serielle Schnittstelle	Serielle Konfigurationsschnittstelle	
Stromversorgung		Internes Netzteil (110–230 V, 50-60 Hz)	
Gehäuse		Robustes Metallgehäuse, 19" 1 HE (440 x 44,2 x 209 mm) mit abschraubbaren Montagewinkeln, Netzwerkanschlüsse auf der Frontseite	

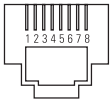
		LANCOM ES-2126+ LANCOM ES-2126P
Normen		CE-konform nach EN 55022, EN 55024, EN 60950
Umgebung/ Temperatur		Temperaturbereich 0–40°C; Luftfeuchtigkeit 5–90%; nicht kondensierend
Zubehör		■ 1000Base-SX SFP-Modul, LANCOM SFP-SX-LC1, Art.-Nr.: 61556 ■ 1000Base-LX SFP-Modul, LANCOM SFP-LX-LC1, Art.-Nr.: 61557
Service		5 Jahre Garantie auf alle Komponenten
Support		Über Hotline und Internet

DE

6.2 Anschlussbelegung

6.2.1 Ethernet-Schnittstelle 10/100Base-TX

8-polige RJ45-Buchsen, entsprechend ISO 8877, EN 60603-7

Steckverbindung	Pin	Leitung
	1	T+
	2	T-
	3	R+
	4	PoE/G
	5	PoE/G
	6	R-
	7	PoE/-48 V
	8	PoE/-48 V

6.3 CE-Konformitätserklärungen

CE Hiermit erklärt LANCOM Systems, dass sich die in dieser Dokumentation beschriebenen Geräte in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befinden.

Die CE-Konformitätserklärungen für Ihr Gerät finden Sie im jeweiligen Produktbereich der LANCOM-Website (www.lancom.de).