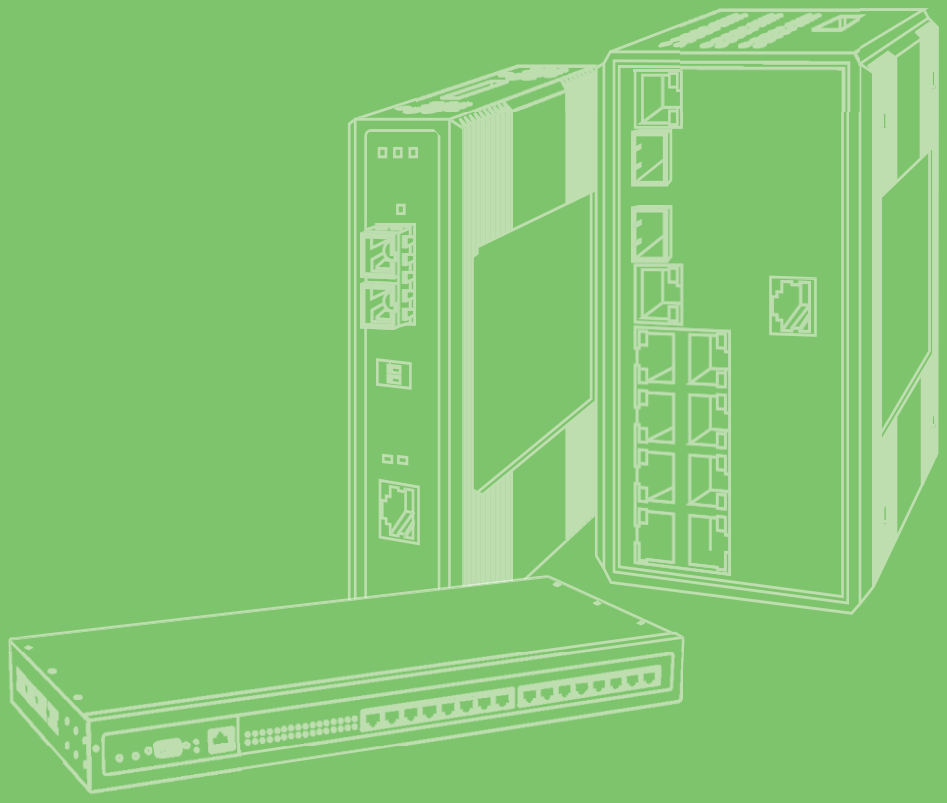
User Manual



EKI-8528 Series

IEC 61850-3 Managed TSN Switch

ADVANTECH

Enabling an Intelligent Planet

Copyright

Acknowledgements

Intel and Pentium are trademarks of Intel Corporation.

Microsoft Windows and MS-DOS are registered trademarks of Microsoft Corp.

All other product names or trademarks are properties of their respective owners.

Product Warranty (5 years)

Advantech warrants to you, the original purchaser, that each of its products will be free from defects in materials and workmanship for five years from the date of purchase.

This warranty does not apply to any products which have been repaired or altered by persons other than repair personnel authorized by Advantech, or which have been subject to misuse, abuse, accident or improper installation. Advantech assumes no liability under the terms of this warranty as a consequence of such events.

Because of Advantech's high quality-control standards and rigorous testing, most of our customers never need to use our repair service. If an Advantech product is defective, it will be repaired or replaced at no charge during the warranty period. For out of-warranty repairs, you will be billed according to the cost of replacement materials, service time and freight. Please consult your dealer for more details.

If you think you have a defective product, follow these steps:

1. Collect all the information about the problem encountered. (For example, CPU speed, Advantech products used, other hardware and software used, etc.) Note anything abnormal and list any on screen messages you get when the problem occurs.
2. Call your dealer and describe the problem. Please have your manual, product, and any helpful information readily available.
3. If your product is diagnosed as defective, obtain an RMA (return merchandize authorization) number from your dealer. This allows us to process your return more quickly.
4. Carefully pack the defective product, a fully-completed Repair and Replacement Order Card and a photocopy proof of purchase date (such as your sales receipt) in a shippable container. A product returned without proof of the purchase date is not eligible for warranty service.
5. Write the RMA number visibly on the outside of the package and ship it prepaid to your dealer.

Edition 2

Printed in Taiwan February 2025

Declaration of Conformity

CE

This product has passed the CE test for environmental specifications. Test conditions for passing included the equipment being operated within an industrial enclosure. In order to protect the product from being damaged by ESD (Electrostatic Discharge) and EMI leakage, we strongly recommend the use of CE-compliant industrial enclosure products.

FCC Class A

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Technical Support and Assistance

1. Visit the Advantech web site at www.advantech.com/support where you can find the latest information about the product.
2. Contact your distributor, sales representative, or Advantech's customer service center for technical support if you need additional assistance. Please have the following information ready before you call:
   - Product name and serial number
   - Description of your peripheral attachments
   - Description of your software (operating system, version, application software, etc.)
   - A complete description of the problem
   - The exact wording of any error messages

Warnings, Cautions and Notes

Warning! *Warnings indicate conditions, which if not observed, can cause personal injury!*

Caution! *Cautions are included to help you avoid damaging hardware or losing data. e.g.*

There is a danger of a new battery exploding if it is incorrectly installed. Do not attempt to recharge, force open, or heat the battery. Replace the battery only with the same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.

Note! *Notes provide optional additional information.*

Document Feedback

To assist us in making improvements to this manual, we would welcome comments and constructive criticism. Please send all such - in writing to: support@advantech.com

Packing List

Before setting up the system, check that the items listed below are included and in good condition. If any item does not accord with the table, please contact your dealer immediately.

- 1 x IEC 61850-3 Managed TSN Switch
- 2 x Wall-mounting Bracket and Screws

Safety Instructions

1. Read these safety instructions carefully.
2. Keep this User Manual for later reference.
3. Disconnect this equipment from any AC outlet before cleaning. Use a damp cloth. Do not use liquid or spray detergents for cleaning.
4. For plug-in equipment, the power outlet socket must be located near the equipment and must be easily accessible.
5. Keep this equipment away from humidity.
6. Put this equipment on a reliable surface during installation. Dropping it or letting it fall may cause damage.
7. The openings on the enclosure are for air convection. Protect the equipment from overheating. DO NOT COVER THE OPENINGS.
8. Make sure the voltage of the power source is correct before connecting the equipment to the power outlet.
9. Position the power cord so that people cannot step on it. Do not place anything over the power cord.
10. All cautions and warnings on the equipment should be noted.
11. If the equipment is not used for a long time, disconnect it from the power source to avoid damage by transient overvoltage.
12. Never pour any liquid into an opening. This may cause fire or electrical shock.
13. Never open the equipment. For safety reasons, the equipment should be opened only by qualified service personnel.
14. If one of the following situations arises, get the equipment checked by service personnel:
15. The power cord or plug is damaged.
16. Liquid has penetrated into the equipment.
17. The equipment has been exposed to moisture.
18. The equipment does not work well, or you cannot get it to work according to the user's manual.
19. The equipment has been dropped and damaged.
20. The equipment has obvious signs of breakage.
21. DO NOT LEAVE THIS EQUIPMENT IN AN ENVIRONMENT WHERE THE STORAGE TEMPERATURE MAY GO -40°C (-40°F) ~ 85°C (185°F). THIS COULD DAMAGE THE EQUIPMENT. THE EQUIPMENT SHOULD BE IN A CONTROLLED ENVIRONMENT.
22. CAUTION: DANGER OF EXPLOSION IF BATTERY IS INCORRECTLY REPLACED. REPLACE ONLY WITH THE SAME OR EQUIVALENT TYPE RECOMMENDED BY THE MANUFACTURER, DISCARD USED BATTERIES ACCORDING TO THE MANUFACTURER'S INSTRUCTIONS.
23. The sound pressure level at the operator's position according to IEC 704-1:1982 is no more than 70 dB (A).

DISCLAIMER: This set of instructions is given according to IEC 704-1. Advantech disclaims all responsibility for the accuracy of any statements contained herein.

Wichtige Sicherheishinweise

1. Bitte lesen sie Sich diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den späteren Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Verwenden Sie Keine Flüssig-oder Aerosolreiniger. Am besten dient ein angefeuchtetes Tuch zur Reinigung.
4. Die NetzanschluBsteckdose soll nahe dem Gerät angebracht und leicht zugänglich sein.
5. Das Gerät ist vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sicheren Stand zu achten. Ein Kippen oder Fallen könnte Verletzungen hervorrufen.
7. Die Belüftungsöffnungen dienen zur Luftzirkulation die das Gerät vor überhitzung schützt. Sorgen Sie dafür, daB diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim. AnschluB an das Stromnetz die AnschluBwerte.
9. Verlegen Sie die NetzanschluBleitung so, daB niemand darüber fallen kann. Es sollte auch nichts auf der Leitung abgestellt werden.
10. Alle Hinweise und Warnungen die sich am Geräten befinden sind zu beachten.
11. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
12. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. elektrischen Schlag auslösen.
13. Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden.
14. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
15. Netzkabel oder Netzstecker sind beschädigt.
16. Flüssigkeit ist in das Gerät eingedrungen.
17. Das Gerät war Feuchtigkeit ausgesetzt.
18. Wenn das Gerät nicht der Bedienungsanleitung entsprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
19. Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
20. Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
21. VOSICHT: Explisionsgefahr bei unsachgemaben Austausch der Batterie.Ersatz nur durch densellben order einem vom Hersteller empfohlene-mahnlichen Typ. Entsorgung gebrauchter Batterien navh Angaben des Herstellers.
22. ACHTUNG: Es besteht die Explosionsgefahr, falls die Batterie auf nicht fachmännische Weise gewechselt wird. Verfangen Sie die Batterie nur gleicher oder entsprechender Type, wie vom Hersteller empfohlen. Entsorgen Sie Batterien nach Anweisung des Herstellers.
23. Der arbeitsplatzbezogene Schalldruckpegel nach DIN 45 635 Teil 1000 beträgt 70dB(A) oder weiger.

Haftungsausschluss: Die Bedienungsanleitungen wurden entsprechend der IEC-704-1 erstellt. Advantech lehnt jegliche Verantwortung für die Richtigkeit der in diesem Zusammenhang getätigten Aussagen ab.

Safety Precaution - Static Electricity

Static electricity can cause bodily harm or damage electronic devices. To avoid damage, keep static-sensitive devices in the static-protective packaging until the installation period. The following guidelines are also recommended:

- Wear a grounded wrist or ankle strap and use gloves to prevent direct contact to the device before servicing the device. Avoid nylon gloves or work clothes, which tend to build up a charge.
- Always disconnect the power from the device before servicing it.
- Before plugging a cable into any port, discharge the voltage stored on the cable by touching the electrical contacts to the ground surface.

Contents

List of Figures

Chapter 1

Product Overview

1.1 Introduction

The EKI-8528 series is a modular, managed Layer 3 and Layer 2 switch designed for standard 19" rackmount installations. It offers up to 24 Gigabit ports and 4x10 Gigabit uplink capabilities, making it ideal for medium to large industrial networking environments. As a distribution-level Layer 3 switch, it supports RIPv1/v2, OSPFv3, and VRRP routing protocols, along with PIM for advanced routing features. The switch also provides a 4.5K routing table size, enabling efficient data exchange across multiple network nodes.

A key feature of the EKI-8528 Series switch is its IEC 61850-3 certification, making it ideal for power substation automation. Additionally, it supports IEEE 1588v2 Precision Time Protocol (PTP), enabling precise time synchronization across devices, ensuring they operate in unison and perform tasks at exactly the required moment.

1.2 Specifications

Specifications	Description	
Interface	I/O Port	■ 3 x 8-port module slots ■ 4 x SFP+ (mini-GBIC) port
	Console Port	RS-232 (RJ45)
	Power Connector	2 x Power supply module slots
Physical	Enclosure	Metal Shell
	Protection Class	IP30
	Installation	Rack mount
	Dimensions (W x H x D)	438 x 44 x 363.5 mm (17.24” x 1.73” x 14.31” in.)
	Weight	5.5 kg (12.1 lbs)
LED Display	System LED	PWR1, PWR2, SYS, Alarm
	Port LED	Speed, Link, Activity
Environment	Operating Temperature	-40 ~ 75°C (-40 ~ 167°F)
	Storage Temperature	-40°C ~ 85°C (-40°F ~ 185°F)
	Ambient Relative Humidity	10 ~ 95% (non-condensing)
Switch Features	L2 MAC Address	32K
	Jumbo Frame	10K
	VLAN Group	256 (VLAN ID 1 ~ 4094)
	Packet Buffer	32Mbits
	VLAN Arrange	■ 801.1ad Q-in-Q VLAN Stacking ■ 802.1Q Tag-based VLAN ■ 802.1v Protocol-based VLAN ■ MAC-based VLAN ■ IP Subnet-based VLAN ■ Private VLAN ■ Voice VLAN

Specifications	Description	
	Port Mirroring	1 to 1, N to 1 Mirroring, Max Mirror Sessions: 5
	Link Aggregation	■ IEEE 802.3ad Dynamic Port Trunking ■ Static Port Trunking ■ Load Balance
	GARP	■ GVRP ■ GMRP
	IP Multicast	■ IGMP Snooping v1/v2/v3 ■ MLD Snooping ■ IGMP Immediate leave
	Storm Control	■ Broadcast ■ Multicast ■ Unknown unicast
	Redundancy	■ IEEE 802.1D-STP ■ IEEE 802.1s-MSTP ■ IEEE 802.1w-RSTP
	Standardized Real-Time Ethernet	■ Time Sensitive Networks (TSN) ■ IEEE 802.1AS, IEEE 802.1Qci ■ IEEE 802.1CB, IEEE 802.1Qbv ■ IEEE 802.1Qbu
	Time Synchronization	■ IEEE 802.1AS gPTP ■ Time Precision: 1 ns ■ IEEE 1588v2 PTP
QoS	Priority Queue Scheduling	■ WRR (Weighted Round Robin) ■ SP (Strict Scheduling Priority) Hybrid Priority
	Class of Service	■ IEEE 802.1p Based CoS ■ IP TOS ■ DSCP based CoS
	Rate Limiting	■ Ingress Rate limit ■ Egress Rate limit
Security	Port Security	■ Static ■ Dynamic IP Source Guard ■ ARP Spoofing Prevention ■ Access Control List ■ DHCP Snooping
	Authentication	■ 802.1x (Port-Based, MD5 Encryption) ■ TACACS+
Management	DHCP	■ DHCP Client / Server ■ DHCP Relay ■ Option 82
	Access	■ SNMP v1/v2c/v3 ■ HTTP ■ HTTPS ■ Telnet ■ Standard ■ MIB
	Configuration Upload / Download	■ HTTP ■ TFTP ■ SFTP

Specifications	Description	
	Security Access	■ SSH2.0 ■ SSL
	Software Upgrade	■ Configuration Backup / Restore ■ Dual Image
	NTP	■ SNTP client ■ NTP Client
Power	Power Consumption	75 Watts(Max)
	Power Input	110/220V AC or 24-48V DC by power module
Certification	Safety	EN 62368-1 compliant
	EMI	EN 55032 Class A, EN 61000-6-4, FCC Part 15 Sub-part B Class A
	EMS	EN 61000-4-2 EN 61000-4-3 EN 61000-4-4 EN 61000-4-5 EN 61000-4-6 EN 61000-4-8
	Shock	IEC 60068-2-27
	Freefall	IEC 60068-2-32
	Vibration	IEC 60068-2-6
	Railway Track Side	EN 50121-4
	Substation	IEC61850-3, IEEE1613

1.3 Hardware Views

1.3.1 Front View

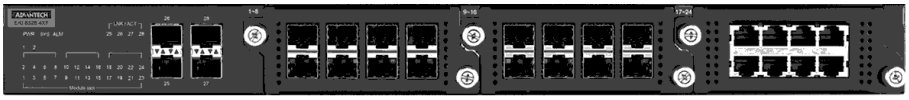


Figure 1.1 Front View

No.	Item	Description
1.	System LED panel	See “System LED Panel” on page 6 for further details.
2.	ETH port	4 x 10G SFP+ ports
3.	Ethernet Modular Slot	Optional 8-port copper or fiber modular

1.3.1.1 System LED Panel

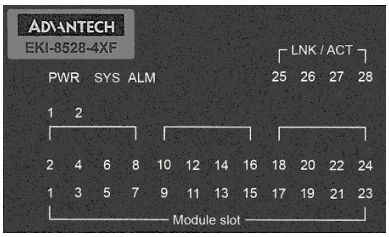


Figure 1.2 System LED Panel

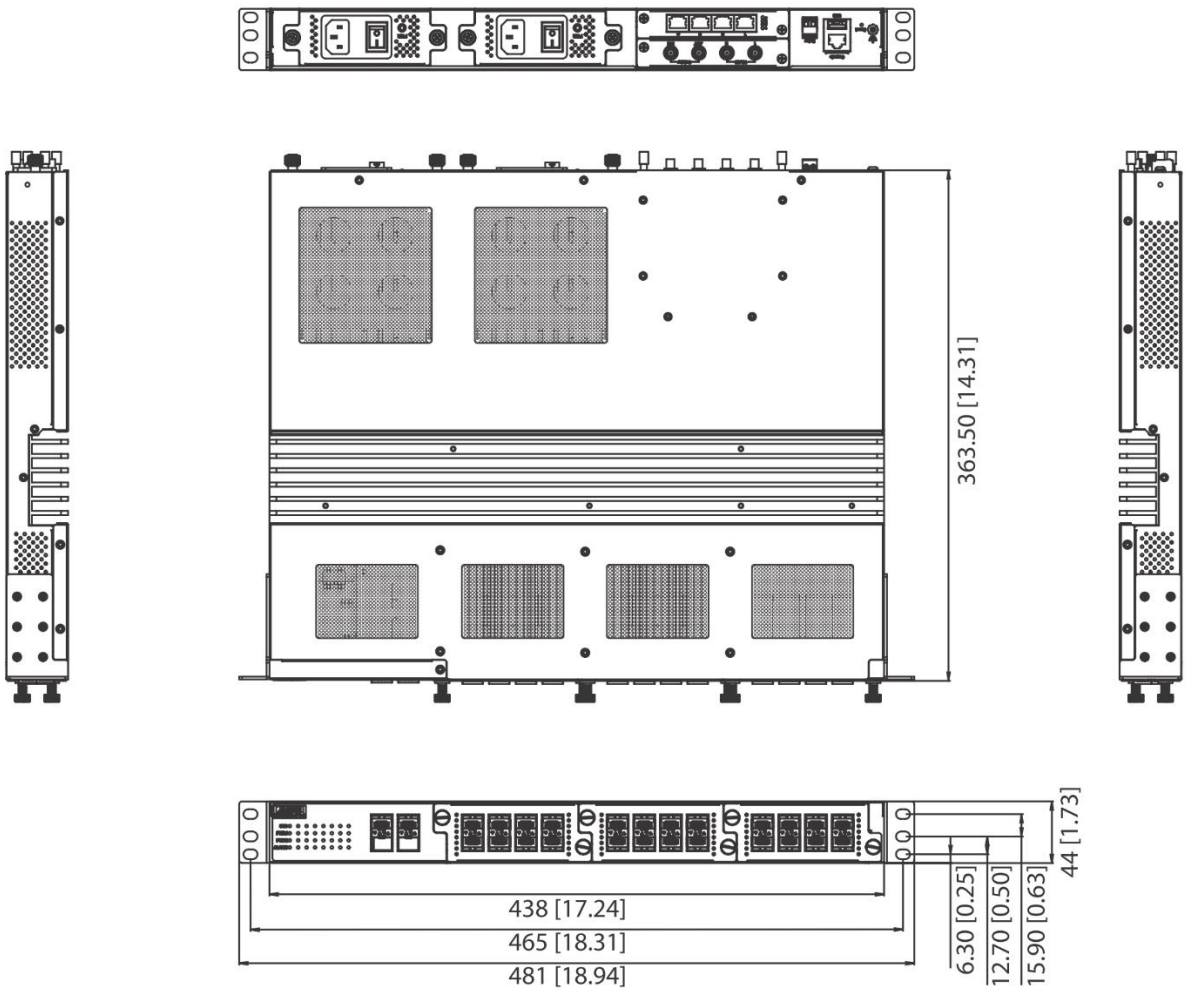
No.	LED Name	LED Color	Description
1.	PWR1	Solid green	Powered up
		Off	Powered down or not installed
2.	PWR2	Solid green	Powered up
		Off	Power down or not installed
3.	SYS	Solid green	System is operating normally
		Off	System is powered down / system crash / operation initiating
4.	Alarm	Red	Active when power failure is detected

1.3.2 Rear View

Figure 1.3 Rear View

No.	Item	Description
1.	Reset button	Button allows for system soft reset or factory default reset.
2.	Console serial port	Console cable port to COM port (DB9 male) on computer to RS232 managed switch (RJ45 female).
3.	USB	Allows configuration backup and restore
4.	IIoT Modular Slot	Optional for HSR/PRP modular
5.	Power Modular Slot	Optional AC or DC power modular

1.3.3 Dimension



Chapter 2

Switch Installation

2.1 Installation Guidelines

The following guidelines are provided to optimize the device performance. Review the guidelines before installing the device.

- Make sure cabling is away from sources of electrical noise. Radios, power lines, and fluorescent lighting fixtures can interference with the device performance.
- Make sure the cabling is positioned away from equipment that can damage the cables.
- Operating environment is within the ranges listed range, see “Specifications” on page 2.
- Relative humidity around the switch does not exceed 95 percent (noncondensing).
- Altitude at the installation site is not higher than 10,000 feet.
- In 10/100 and 10/100/1000 fixed port devices, the cable length from the switch to connected devices can not exceed 100 meters (328 feet).
- Make sure airflow around the switch and respective vents is unrestricted. Without proper airflow the switch can overheat. To prevent performance degredation and damage to the switch, make sure there is clerance at the top and bottom and around the exhaust vents.

2.1.1 Connecting Hardware

In this instruction, it will explain how to find a proper location for your Modbus Gateways, and how to connect to the network, hock up the power cable, and connect to the EKI-8500 Series.

2.2 Verifying Switch Operation

Before installing the device in a rack or on a wall, power on the switch to verify that the switch passes the power-on self-test (POST). To connect the cabling to the power source see “Power Supply Installation” on page 19.

At startup (POST), the System LED blinks green, while the remaining LEDs are a solidy green. Once the switch passes POST self-test, the System LED turns green. The other LEDs turn off and return to their operating status. If the switch fails POST, the System LED switches to an amber state.

After a successful self-test, power down the switch and disconnect the power cabling.

The switch is now ready for installation on its final location.

2.3 Installing the Switch

2.3.1 Rack-Mounting

1. Align the rack mount brackets with the holes on the switch.
2. Secure the rack mount brackets with the provided screws.

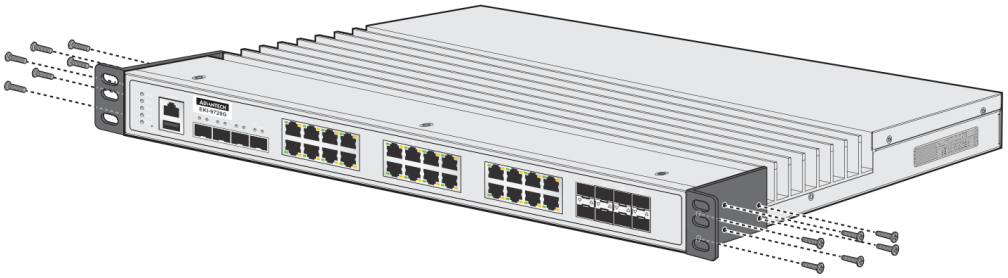


Figure 2.1 Installing the Rack Mount Brackets

3. Align the switch with the posts on the rack cabinet.
4. Secure the switch with the provided screws.

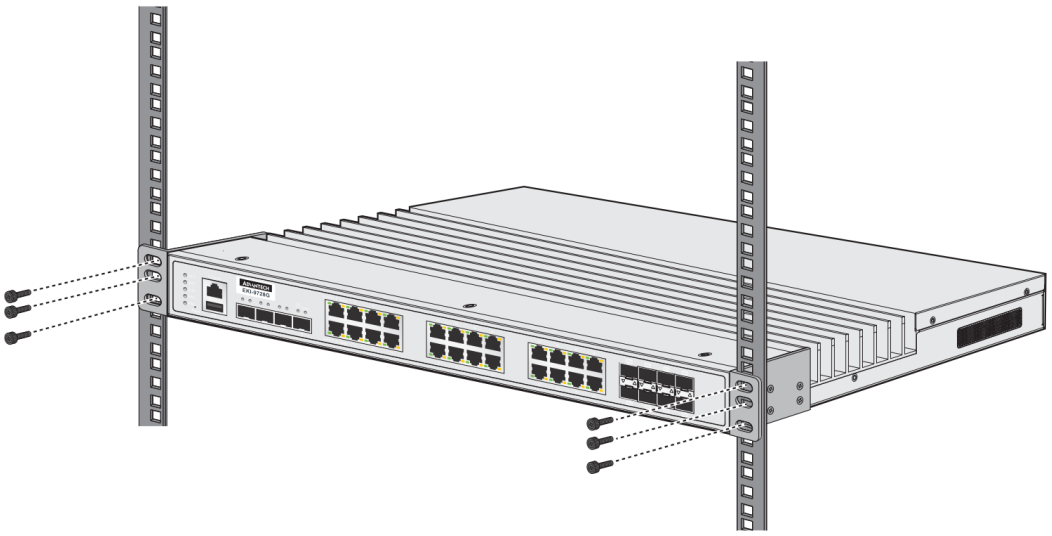


Figure 2.2 Installing the Switch

2.4 Installing and Removing SFP Modules

Up to two fiber optic ports are available (dependent on model) for use in the switch. Refer to the technical specifications for details.

The Gigabit Ethernet ports on the switch are 100/1000Base SFP Fiber ports, which require using the 100M or 1G mini-GBIC fiber transceivers to work properly. Advantech provides completed transceiver models for different distance requirement.

The concept behind the LC port and cable is quite straight forward. Suppose that you are connecting devices I and II; contrary to electrical signals, optical signals do not require a circuit in order to transmit data. Consequently, one of the optical lines is used to transmit data from device I to device II, and the other optical line is used transmit data from device II to device I, for full-duplex transmission.

Remember to connect the Tx (transmit) port of device I to the Rx (receive) port of device II, and the Rx (receive) port of device I to the Tx (transmit) port of device II. If you make your own cable, we suggest labeling the two sides of the same line with the same letter (A-to-A and B-to-B, as shown below, or A1-to-A2 and B1-to-B2).

Note! *This is a Class 1 Laser/LED product. To avoid causing serious damage to your eyes, do not stare directly into the Laser Beam.*

2.4.1 Installing SFP Modules

To connect the fiber transceiver and LC cable, use the following guidelines:

1. Remove the dust plug from the fiber optic slot chosen for the SFP transceiver.

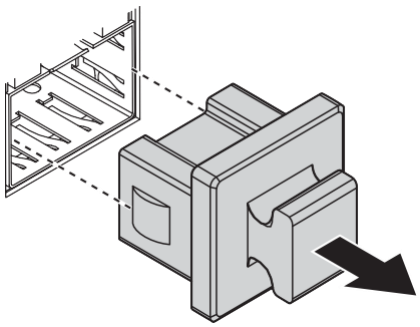


Figure 2.3 Removing the Dust Plug from an SFP Slot

Note! *Do not remove the dust plug from the SFP slot if you are not installing the transceiver at this time. The dust plug protects hardware from dust contamination.*

2. Position the SFP transceiver with the handle on top, see the following figure.
3. Locate the triangular marking in the slot and align it with the bottom of the transceiver.
4. Insert the SFP transceiver into the slot until it clicks into place.

5. Make sure the module is seated correctly before sliding the module into the slot. A click sounds when it is locked in place.

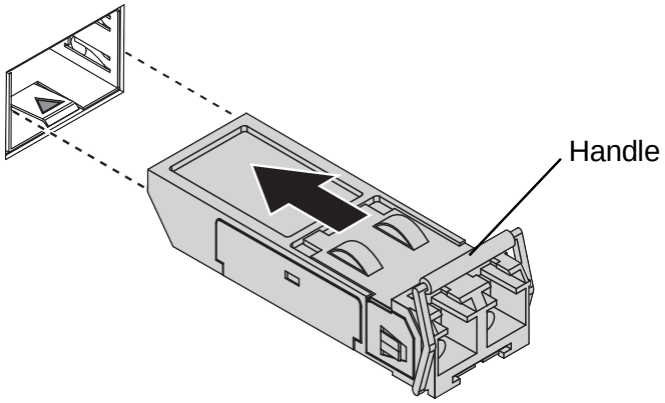


Figure 2.4 Installing an SFP Transceiver

Note! *If you are attaching fiber optic cables to the transceiver, continue with the following step. Otherwise, repeat the previous steps to install the remaining SFP transceivers in the device.*

6. Remove the protective plug from the SFP transceiver.

Note! *Do not remove the dust plug from the transceiver if you are not installing the fiber optic cable at this time. The dust plug protects hardware from dust contamination.*

7. Insert the fiber cable into the transceiver. The connector snaps into place and locks.

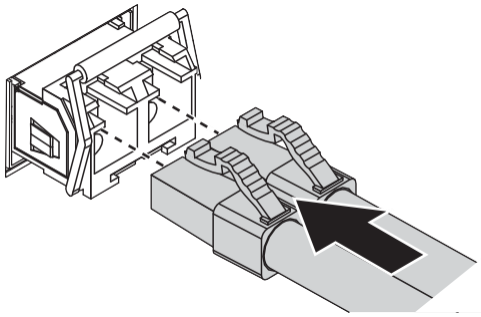


Figure 2.9 Attaching a Fiber Optic Cable to a Transceiver

8. Repeat the previous procedures to install any additional SFP transceivers in the switch.

The fiber port is now setup.

2.4.2 Removing SFP Modules

To disconnect an LC connector, use the following guidelines:

1. Press down and hold the locking clips on the upper side of the optic cable.

2. Pull the optic cable out to release it from the transceiver.

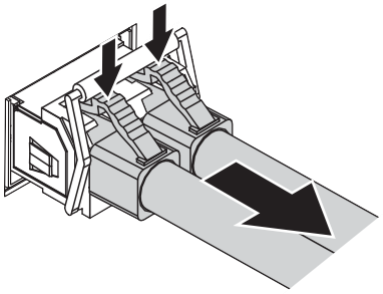


Figure 2.5 Removing a Fiber Optic Cable to a Transceiver

3. Hold the handle on the transceiver and pull the transceiver out of the slot.

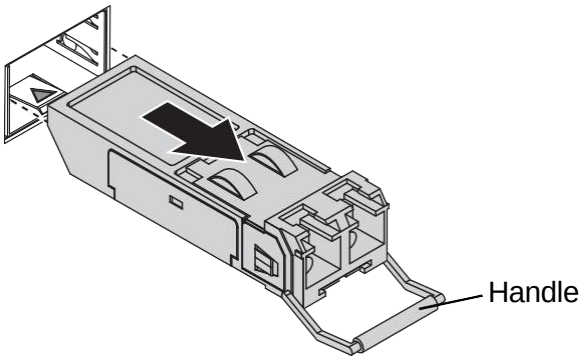


Figure 2.6 Removing an SFP Transceiver

Note! *Replace the dust plug on the slot if you are not installing a transceiver. The dust plug protects hardware from dust contamination.*

2.5 Connecting the Switch to Ethernet Ports

2.5.1 RJ45 Ethernet Cable Wiring

For RJ45 connectors, data-quality, twisted pair cabling (rated CAT5 or better) is recommended. The connector bodies on the RJ45 Ethernet ports are metallic and connected to the GND terminal. For best performance, use shielded cabling. Shielded cabling may be used to provide further protection.

Straight-thru Cable Wiring		Cross-over Cable Wiring	
Pin 1	Pin 1	Pin 1	Pin 3
Pin 2	Pin 2	Pin 2	Pin 6
Pin 3	Pin 3	Pin 3	Pin 1
Pin 6	Pin 6	Pin 6	Pin 2

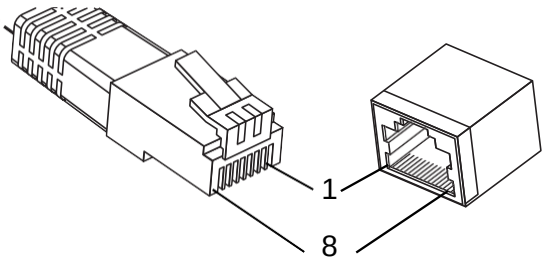


Figure 2.7 Ethernet Plug & Connector Pin Position

Maximum cable length: 100 meters (328 ft.) for 10/100/1000BaseT.

2.6 Connecting the Switch to Console Port

The industrial switch supports a secondary means of management. By connecting the RJ45 to RS232 serial cable between a COM port on your PC (9-pin D-sub female) and the switch's RJ45 (RJ45) port, a wired connection for management can be established.

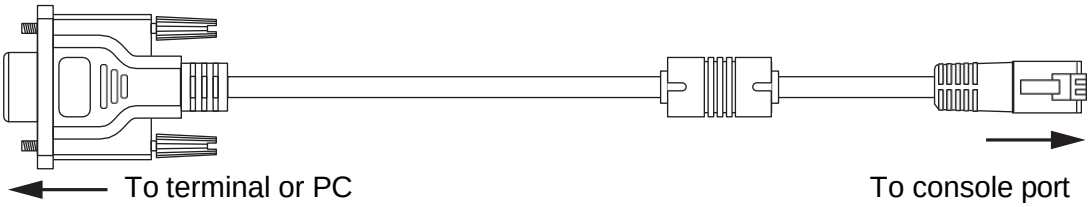


Figure 2.8 Serial Console Cable

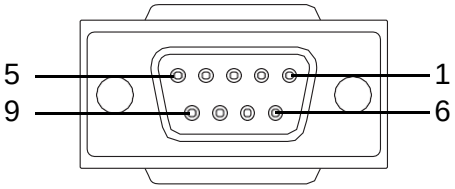


Figure 2.9 DB 9 Pin Position

DB9 Connector	RJ45 Connector
NC	1 Orange/White
NC	2 Orange
2	3 Green/White
NC	4 Blue
5	5 Blue/White
3	6 Green
NC	7 Brown/White
NC	8 Brown

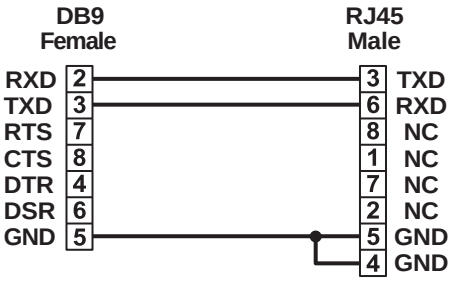


Figure 2.10 Pin Assignment

2.7 Power Supply Installation

2.7.1 Overview

Warning! *Power down and disconnect the power cord before servicing or wiring the switch.*

Caution! *Do not disconnect modules or cabling unless the power is first switched off.*

The device only supports the voltage outlined in the type plate. Do not use any other power components except those specifically designated for the switch device.

Caution! *Disconnect the power cord before installation or cable wiring.*

The switches can be powered using the same DC source used to power other devices. A DC voltage range of 24 to 48 VDC must be applied between the V1+ terminal and the V1- terminal (PW1), see the following illustrations. The chassis ground screw terminal should be tied to the panel or chassis ground. A redundant power configuration is supported through a secondary power supply unit to reduce network down time as a result of hardware failure. Dual power inputs are supported and allow you to connect a backup power source.

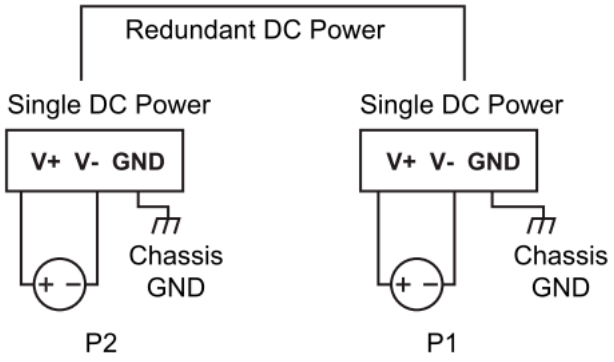


Figure 2.11 Power Wiring for EKI-8528 Series

2.7.2 Considerations

Take into consideration the following guidelines before wiring the device:

- The Terminal Block (CN1) is suitable for 12-24 AWG (3.31 - 0.205 mm^2). Torque value 7 lb-in.
- The cross sectional area of the earthing conductors shall be at least 3.31 mm^2.
- Calculate the maximum possible current for each power and common wire. Make sure the power draw is within limits of local electrical code regulations.
- For best practices, route wiring for power and devices on separate paths.
- Do not bundle together wiring with similar electrical characteristics.
- Make sure to separate input and output wiring.
- Label all wiring and cabling to the various devices for more effective management and servicing.

Note! *Routing communications and power wiring through the same conduit may cause signal interference. To avoid interference and signal degradation, route power and communications wires through separate conduits.*

2.7.3 Grounding the Device

Caution! *Do not disconnect modules or cabling unless the power is first switched off.*

The device only supports the voltage outlined in the type plate. Do not use any other power components except those specifically designated for the switch device.

Caution! *Before connecting the device properly ground the device. Lack of a proper grounding setup may result in a safety risk and could be hazardous.*

Caution! *Do not service equipment or cables during periods of lightning activity.*

Caution! *Do not service any components unless qualified and authorized to do so.*

Caution! *Do not block air ventilation holes.*

Electromagnetic Interference (EMI) affects the transmission performance of a device. By properly grounding the device to earth ground through a drain wire, you can setup the best possible noise immunity and emissions.

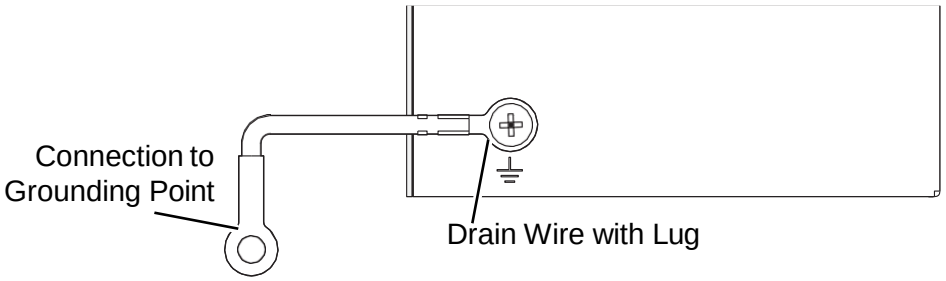


Figure 2.12 Grounding Connection

By connecting the ground terminal by drain wire to earth ground the switch and chassis can be ground.

Note! *Before applying power to the grounded switch, it is advisable to use a volt meter to ensure there is no voltage difference between the power supply's negative output terminal and the grounding point on the switch.*

2.7.4 Wiring a Relay Contact

The following section details the wiring of the relay output. The terminal block on the EKI-8528 Series is wired and then installed onto the terminal receptor located on the EKI-8528 Series.

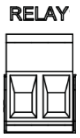


Figure 2.13 Terminal Receptor: Relay Contact

2.7.5 Wiring the Power Inputs

Caution! *Do not disconnect modules or cabling unless the power is first switched off.*

The device only supports the voltage outlined in the type plate. Do not use any other power components except those specifically designated for the switch device.

Warning! *Power down and disconnect the power cord before servicing or wiring the switch.*

For DC power modular

There are two power modular slots for single and redundant power configurations. See the following for terminal block connector views.

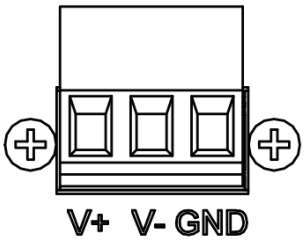


Figure 2.14 Terminal Receptor: Power Input Contacts

To wire the power inputs:

Make sure the power is not connected to the switch or the power converter before proceeding.

1. Insert a small flat-bladed screwdriver in the V+ / V- wire-clamp screws and loosen the screws.
2. Insert the positive and negative DC wires into the V+ and V-terminals of PW1. If setting up power redundancy, connect PW2 in the same manner.

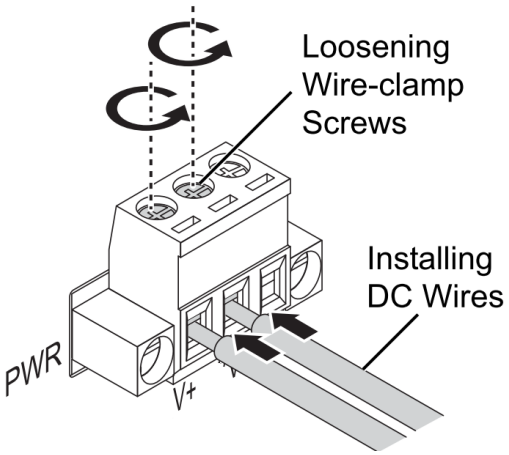


Figure 2.15 Removing a Terminal Block

3. Tighten the wire-clamp screws to secure the DC wires in place.

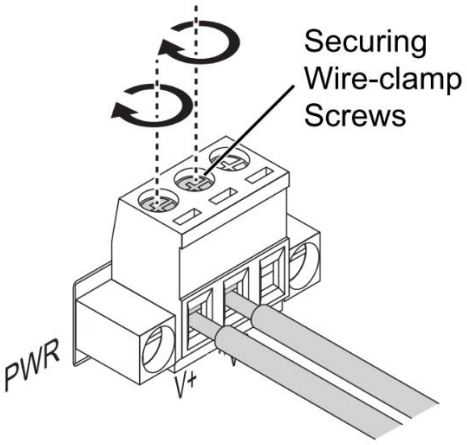


Figure 2.16 Securing DC Wires in a Terminal Block

2.8 Reset Button

Reset configuration to factory default:

Press and hold Reset button for 5 seconds.

System reboot:

Press and hold Reset button for 2 seconds.

Note! *Do NOT power off the Ethernet switch when loading default settings.*

Chapter 3

Configuration Utility

3.1 First Time Setup

3.1.1 Overview

The Industrial Ethernet Managed Switch is a configurable device that facilitates the interconnection of Ethernet devices on an Ethernet network. This includes computers, operator interfaces, I/O, controllers, RTUs, PLCs, other switches/hubs or any device that supports the standard IEEE 802.3 protocol.

This switch has all the capabilities of a store and forward Ethernet switch plus advanced management features such as SNMP, RSTP and port mirroring. This manual details how to configure the various management parameters in this easy to use switch.

3.1.2 Introduction

To take full advantage of all the features and resources available from the switch, it must be configured for your network.

The switch implements Rapid Spanning Tree Protocol (RSTP) and Simple Network Management Protocol (SNMP) to provide most of the services offered by the switch. Rapid Spanning Tree Protocol allows managed switches to communicate with each other to ensure that there exists only one active route between each pair of network nodes and provides automatic failover to the next available redundant route. A brief explanation of how RSTP works is given in the Spanning Tree section.

The switch is capable of communicating with other SNMP capable devices on the network to exchange management information. This statistical/derived information from the network is saved in the Management Information Base (MIB) of the switch. The MIB is divided into several different information storage groups. These groups will be elaborated in detail in the Management and SNMP information section of this document. The switch implements Internet Group Management Protocol (IGMP) to optimize the flow of multicast traffic on your network.

The switch supports both port-based and tag-based Virtual LANs for flexible integration with VLAN-aware networks with support for VLAN-unaware devices.

3.1.3 Administrative Interface Access

There are several administrative interfaces to the switch:

1. A graphical web interface accessible via the switch's built-in web server. Both HTTP and secure HTTPS with SSL are supported.

   Note! *This is the recommended method for managing the switch.*

2. A terminal interface via the RS232/USB port or over the network using telnet or Secure Shell (SSH).
3. An SNMP interface can be used to read/write many settings.
4. Command Line Interface (CLI) can be used to read/write most settings. Initial setup must be done using an Ethernet connection (recommended) or the serial port.

3.1.4 Using the Graphical (Web) Interface

The graphical interface is provided via a web server in the switch and can be accessed via a web browser such as Chrome, Firefox, or Internet Explorer.

Note! *JavaScript must be supported and enabled in your browser for the graphical interface to work correctly.*

HTTP and HTTPS (secure HTTP) are supported for access to the web server. By default, only HTTP is enabled. Either or both may be enabled or disabled to secure the switch. (See the Remote Access Security topic in this section.)

To access the graphical interface, enter a URL like HTTP://192.168.1.1 in your browser's address bar. Replace “http” with “https” to use secure http and replace “192.168.1.1” with your switch's IP address if you've changed it from the factory default.

The web server in the switch uses a signed security certificate. When you access the server via https, you may see a warning dialog indicating that the certificate was signed by an unknown authority. This is expected and to avoid this message in the future you can choose to install the certificate on your computer.

Note! *This manual describes and depicts the web user interface in detail. The terminal interface is not specifically shown but is basically the same.*

3.1.5 Configuring the Switch for Network Access

To control and monitor the switch via the network, it must be configured with basic network settings, including an IP address and subnet mask.

To configure the switch for network access, select [Add Menu Address Here] to reach the System Settings menu. The settings in this menu control the switch's general network configuration.

- DHCP Enabled/Disabled: The switch can automatically obtain an IP address from a server using the Dynamic Host Configuration Protocol (DHCP). This can speed up initial set up, as the network administrator does not have to find an open IP address.
- IP Address and subnet mask configuration: The IP address for the switch can be changed to a user-defined address along with a customized subnet mask to separate subnets.

Note! *Advanced users can set the IP address to 0.0.0.0 to disable the use of an IP address for additional security. However, any features requiring an IP address (i.e., web interface, etc.) will no longer be available.*

- Default Gateway Selection: A Gateway Address is chosen to be the address of a router that connects two different networks. This can be an IP address or a Fully Qualified Domain Name (FQDN) such as “domainname.org”.
- NTP Server: The IP address or domain name of an NTP (Network Time Protocol) server from which the switch may retrieve the current time at startup. Please note that using a domain name requires that at least one domain name server be configured.

3.1.6 Configuring the Ethernet Ports

The switch comes with default port settings that should allow you to connect to the Ethernet Ports with out any necessary configuration. Should there be a need to change the name of the ports, negotiation settings or flow control settings, you can do this in the Port Configuration menu. Access this menu by selecting Setup from the Main menu, and then selecting Main Settings.

- Port Name: Each port in the managed switch can be identified with a custom name. Specify a name for each port here.
- Admin: Ports can be enabled or disabled in the managed switch. For ports that are disabled, they are virtually non-existent (not visible in terms of switch operation or spanning tree algorithm). Choose to enable or disable a port by selecting Enabled or Disabled, respectively.
- Negotiation: All copper ports and gigabit fiber ports in the managed switch are capable of autonegotiation such that the fastest bandwidth is selected. Choose to enable auto-negotiation or use fixed settings. 100Mbps Fiber ports are Fixed speed only.
- Speed/Duplex/Flow Control: The managed switch accepts three local area network Ethernet Standards. The first standard, 10BASE-T, runs 10Mbps with twisted pair Ethernet cable between network interfaces. The second local area network standard is 100BASE-T, which runs at 100Mbps over the same twisted pair Ethernet cable. Lastly, there is 100BASE-F, which enables fast Ethernet (100Mbps) over fiber.

These options are available:

- 10h–10 Mbps, Half Duplex
- 10f –10 Mbps, Full Duplex
- 100h–100 Mbps, Half Duplex
- 100f –100 Mbps, Full Duplex
- 1000f–1000 Mbps, Full Duplex

On managed switches with gigabit combination ports, those ports with have two rows, a standard row of check boxes and a row labeled “SFP” with radio buttons. The SFP setting independently sets the speed at which a transceiver will operate if one is plugged in. Otherwise, the switch will use the fixed Ethernet port and the corresponding settings for it.

Note! *When 100f is selected for the SFP of a gigabit combination port, the corresponding fixed Ethernet jack will be disabled unless it is changed back to 1000F.*

3.2 Command Line Interface Configuration

3.2.1 Introduction to Command-Line Interface (CLI)

The command-line interface (CLI) is constructed with an eye toward automation of CLI-based configuration. The interaction is modeled on that used in many Internet protocols such as Telnet, FTP, and SMTP. After each command is entered and processed, the switch will issue a reply that consists of a numeric status code and a human-readable explanation of the status.

The general format of commands is:

section parameter [value]

where:

– section is used to group parameters.

– parameter will specify the parameter within the section. For example, the network section will have parameters for DHCP, IP address, subnet mask, and default gateway.
– value is the new value of the parameter. If value is omitted, the current value is displayed.

Please note that new values will not take effect until explicitly committed.

Sections and parameter names are case sensitive (e.g., “Network” is not the same as “network”).

Note! *Any commands in the CLI Commands section of this chapter, with the exception of the global commands, must be prefaced with the name of the section they are in. For example, to change the IP address of the switch, you would type:*

network address <newIP>

3.2.2 Accessing the CLI

The command-line interface (CLI) is the primary user interface used to configure, monitor and maintain the devices. It allows you to directly execute CLI commands.

After initially configuring and connecting the device to the network, you can configure the device by using the remote access method. The following console settings with default:

- Baud rate speed 115200
- Databits 8 bits
- Parity - none
- Stop bits 1 bits

Connect the EKI-8528 to a terminal or to a “COM” port of PC by using terminal emulation. Press any key or call up the Command Line Interface via Telnet. Press any key to continue and enter the user name and password as below with default, the screen will displays.

- User name: admin
- Password: admin

3.3 Web Browser Configuration

The switch has an HTML based user interface embedded in the flash memory. The interface offers an easy to use means to manage basic and advanced switch functions. The interface allows for local or remote switch configuration anywhere on the network.

The interface is designed for use with [Internet Explorer (10.0), Chrome, Firefox].

3.3.1 Preparing for Web Configuration

The interface requires the installation and connection of the switch to the existing network. A PC also connected to the network is required to connect to the switch and access the interface through a web browser. The required networking information is provided as follows:

- IP address: 192.168.1.1
- Subnet mask: 255.255.255.0
- Default gateway: 192.168.1.254
- User name: admin
- Password: admin

3.3.2 System Login

Once the switch is installed and connected, power on the switch. The following information guides you through the logging in process.

1. Launch your web browser on the PC.
2. In the browser's address bar, type the switch's default IP address (192.168.1.1).

The login screen displays.

3. Enter the user default name and password (admin / admin).
4. Click **OK** on the login screen to log in.

The main interface displays.

Chapter 4

Managing Switch

4.1 Log In

To access the login window, connect the device to the network, see “Connecting the Switch to Ethernet Ports” on page 17. Once the switch is installed and connected, power on the switch see the following procedures to log into your switch.

When the switch is first installed, the default network configuration is set to DHCP enabled. You will need to make sure your network environment supports the switch setup before connecting it to the network.

1. Launch your web browser on a computer.
2. In the browser’s address bar type in the switch’s default IP address (192.168.1.1). The login screen displays.
3. Enter the default user name and password (admin/admin) to log into the management interface. You can change the default password after you have successfully logged in.
4. Click **Login** to enter the management interface.

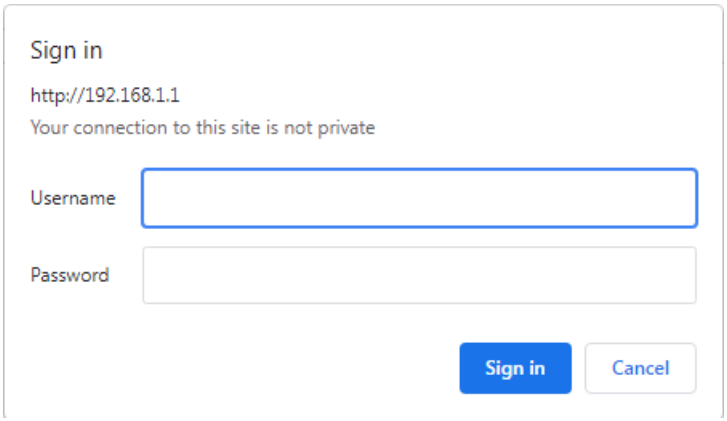


Figure 4.1 Login Screen

4.2 Recommended Practices

One of the easiest things to do to help increase the security posture of the network infrastructure is to implement a policy and standard for secure management. This practice is an easy way to maintain a healthy and secure network.

After you have performed the basic configurations on your switches, the following is a recommendation which is considered best practice policy.

4.2.1 Changing Default Password

In keeping with good management and security practices, it is recommended that you change the default password as soon as the device is functioning and setup correctly. The following details the necessary steps to change the default password.

To change the password:

1. Navigate to **Configuration** > **Security** > **Users**.
2. From the User Configuration table, click the Admin (default) account to select it.
3. The Edit User screen displays, click the Change Password drop-down menu and select **Yes**.
4. In the **Password** field (maximum length: 32 characters), type in the new password. Re-type the same password in the **Password (again)** field.

5. Click **Save** to change the current account settings. Alternatively, click **Reset** or **Cancel**.

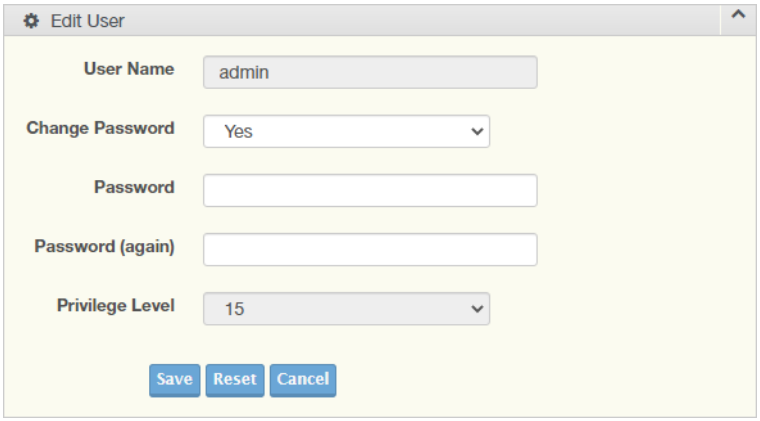


Figure 4.2 Changing a Default Password

After saving all the desired settings, perform a system save (**Maintenance** > **Configuration > Save startup-config**) by clicking **Save Configuration**. The changes are saved.

4.3 Configuration

4.3.1 System

4.3.1.1 Information Configuration

To access this page:

1. Navigate to **Configuration** > **System** and click **Information**.
   The System Information Configuration page displays.

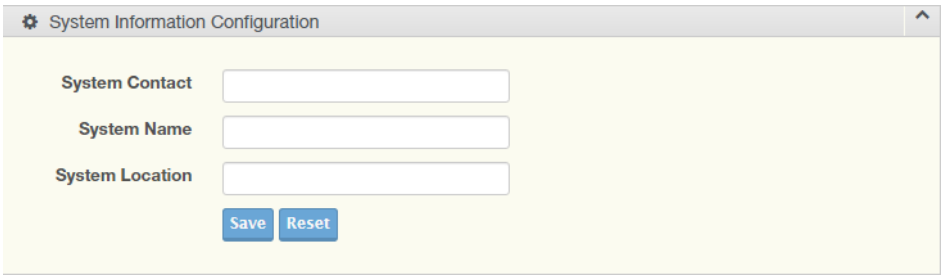


Figure 4.3 Creating System Information Settings

The following table describes the items in the previous figure.

Item	Description
System Contact	Enter identification information to describe the contact option for management events. String length is 0 to 255. Only ASCII characters from 32 to 126 are supported.
System Name	Enter the name to the assigned contact information using alpha numeric characters (A-Za-z), digits (0-9), and minus symbol (-). String length is 0 to 255. No space characters are supported. The first character must be an alphanumeric character. The first or last character must not be a minus sign.
System Location	Enter a description to identify the physical location of this node. The allowed string length is 0 to 255. Only ASCII characters from 32 to 126 are supported.
Save	Click **Save** to store the settings.
Reset	Click **Reset** to clear the settings.

4.3.1.2 IP Configuration

To access this page:

1. Navigate to **Configuration** > **System** and click **IP**.
   The IP Configuration page displays.

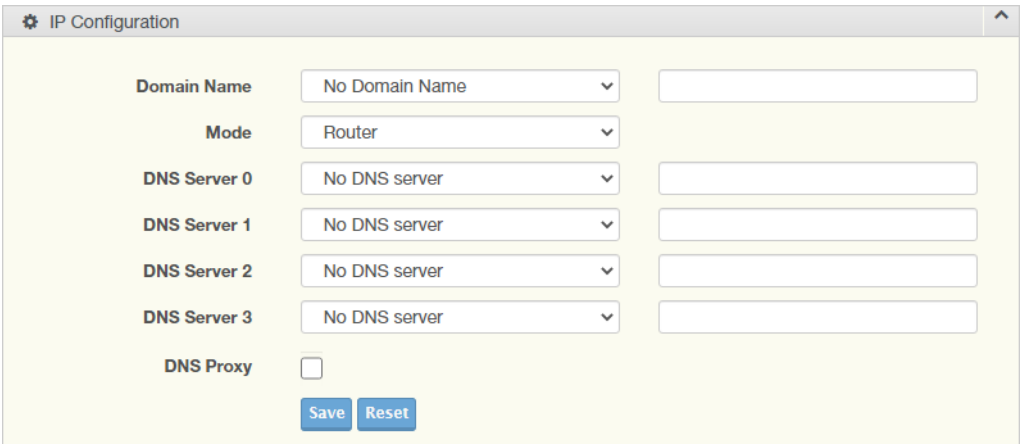


Figure 4.4 Configuring IP Settings

The following table describes the items in the previous figure.

Item	Description
Domain Name	Enter the string to define the domain name using alpha numeric characters (A-Z, a-z), digits (0-9), and minus symbol (-). String length is 0 to 255. No space characters are supported. The first character must be an alphanumeric character. The first or last character must not be a minus sign.
Mode	Click the drop-down menu to set the mode as a Host or a Router. In Host mode, IP traffic between interfaces is not routed, while in Router mode traffic is routed between all interfaces.
DNS Server (0 ~ 3)	Click the drop-down menu to set the DNS name resolution for the device. The following modes are supported: ■ No DNS server (default): No DNS server is used. ■ Configured IPv4 or IPv6: Enter the specified IPv4/IPv6 address of the DNS Server. ■ From any DHCPv4/DHCPv6 interfaces: First DNS server instance from a DHCP lease to a DHCP-enabled interface is used. ■ From this DHCPv4/DHCPv6 interface: Specify a DHCP-enabled interface to provide DNS server function.
DNS Proxy	Click to enable DNS proxy. The system relay DNS requests to the currently configured DNS server, and replies as a DNS resolver to the network client devices.
Save	Click **Save** to store the settings.
Reset	Click **Reset** to clear the settings.

To configure the IP interfaces:

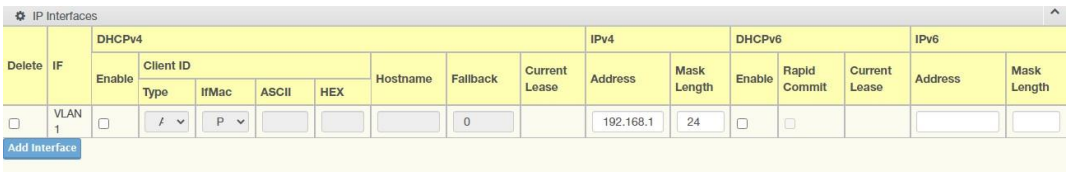


Figure 4.5 Configuring IP Interfaces

To add an IP interface:

Item	Description
Delete	Click to select the deletion of existing IP interface(s).
VLAN	Enter a value to identify the VLAN associated with the IP interface. Only ports within the identified VLAN can access the IP interface. Only available when creating a new interface.
DHCPv4	
Enabled	Click to enable the interface. If enabled, configure the client ID type (IfMac,ASCII, or HEX) IPv4 address and mask length of the interface for the DHCP protocol.
Type	Click the drop-down menu to specify the client identifier. Options: ■ IfMac ■ ASCII ■ HEX
IfMac	Click the drop-down menu to specify the DHCP client identifier by using the MAC address in the DHCP option 61 field.
ASCII	Enter a string to specify the DHCP client identifier by using the ASCII type string in the DHCP option 61 field.
HEX	Enter a string to specify the DHCP client identifier by using the HEX type string in the DHCP option 61 field.
Hostname	Enter a string to identify the DHCP client hostname.
Fallback	Enter a value to define the time out threshold in seconds (0 to 4294967295 seconds) when trying to obtain a DHCP lease. Once threshold is reached, the configured IPv4 address is used as the IPv4 interface address. A value of zero disables the function.
Current Lease	An active lease is identified by the DHCP interface's current interface address, as provided by the DHCP server.
IPv4 Address	If DHCP is not enabled, enter the IPv4 address to designate the interface.
IPv4 Mask	If DHCP is not enabled, enter the IPv4 network mask in bits (0 & 30 bits for an IPv4 address). If enabled, the fallback address network mask is used.
DHCPv6	
Enable	Click to enable the interface. If enabled, configure the client ID type (IfMac,ASCII, or HEX) IPv6 address and mask length of the interface.
Rapid Commit	Click to enable or disable (default) the rapid-commit option. If this option is enabled, the DHCPv6 client terminates the waiting process as soon as a Reply message with a Rapid Commit option is received.
Current Lease	Displays the current lease of the interface address.
IPv6	
Address	Enter a string to identify IPv6 address of the interface. The field may be left blank if IPv6 operation on the interface is not desired.
Mask Length	Enter a string to identify the length of a network address must match for qualification in the route (values: 0 to 32 bits respectively 128 for IPv6 routes).
Add Interface	Click to add a new IP interface entry.

To add an IP route:

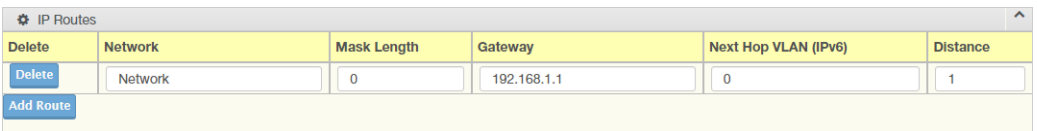


Figure 4.6 Configuring IP Routes

Item	Description
Delete	Click **Delete t**o remove the specified route entry.
Network	Enter the destination IP network or host address of the route. The following values denotes a default route: 0.0.0.0 or IPv6 ::.
Mask Length	Enter a value to define the IP network or host mask in number of bits (prefix length). Valid values are between 0 and 32 bits (128 for IPv6 routes). Only a default route has a mask length of 0.
Gateway	Enter the IP address of the IP gateway. The gateway and Network must be of the same type.
Next Hop VLAN (IPv6)	Enter the IPv6 to specify the interface associated with the gateway. Range: 1 to 4094. The range is valid only when the corresponding IPv6 interface is valid. Link-local addresses, must specify the next hop VLAN. If the IPv6 gateway address is not link-local, the system ignores the next hop VLAN for the gateway.
Distance	Enter a value to specify the next hop distance for the route.
Add Route	Click **Add Route** to add a route entry.

4.3.1.3 NTP Configuration

To configure NTP, access the page as follows:

1. Navigate to **Configuration** > **System** and click **NTP**.
   The NTP Configuration page displays.

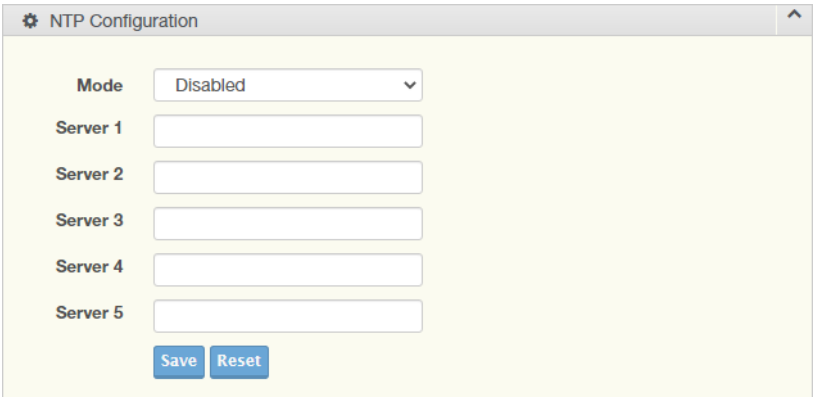


Figure 4.7 Configuring IP Settings

The following table describes the items in the previous figure.

Item	Description
Mode	Click the drop-down menu to select the operation mode: ■ Enabled: Enable NTP client mode operation. ■ Disabled: Disable NTP client mode operation.
Server 1 / 5	Enter the IPv4 or IPv6 address of an NTP server. For IPv6 addresses, enter a 128-bit record represented as eight fields of up to four hexadecimal digits with a colon (:) separating each field.
Save	Click **Save** to store the settings.
Reset	Click **Reset** to clear the settings.

4.3.1.4 Time Zone Configuration

To configure Time Zone Configuration, access the page as follows:

1. Navigate to **Configuration** > **System** and click **Time**.

The Time Zone Configuration page displays.

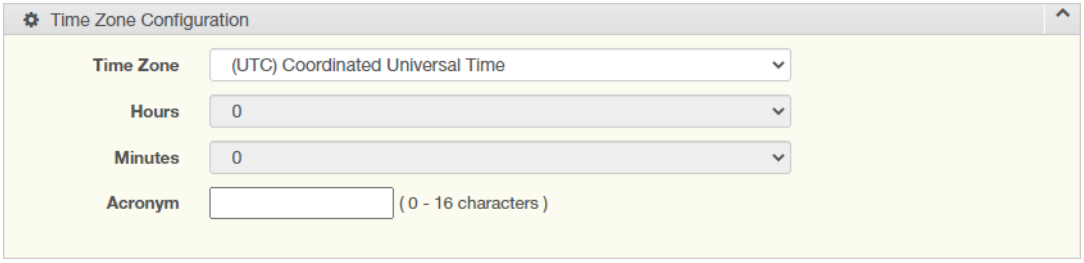


Figure 4.8 Time Zone Configuration

The following table describes the items in the previous figure.

Item	Description
Time Zone	Click the drop-down menu to select manual to enter a custom time zone setting or an available world wide time zone.
Hours	For manual entries, enter the number of hours offset from UTC.
Minutes	For manual entries, enter the number of minutes offset from UTC.
Acronym	Enter an acronym to easily identify the setting (Range: Up to 16 characters).

The Daylight Saving Time Configuration page is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. To configure the daylight saving time:

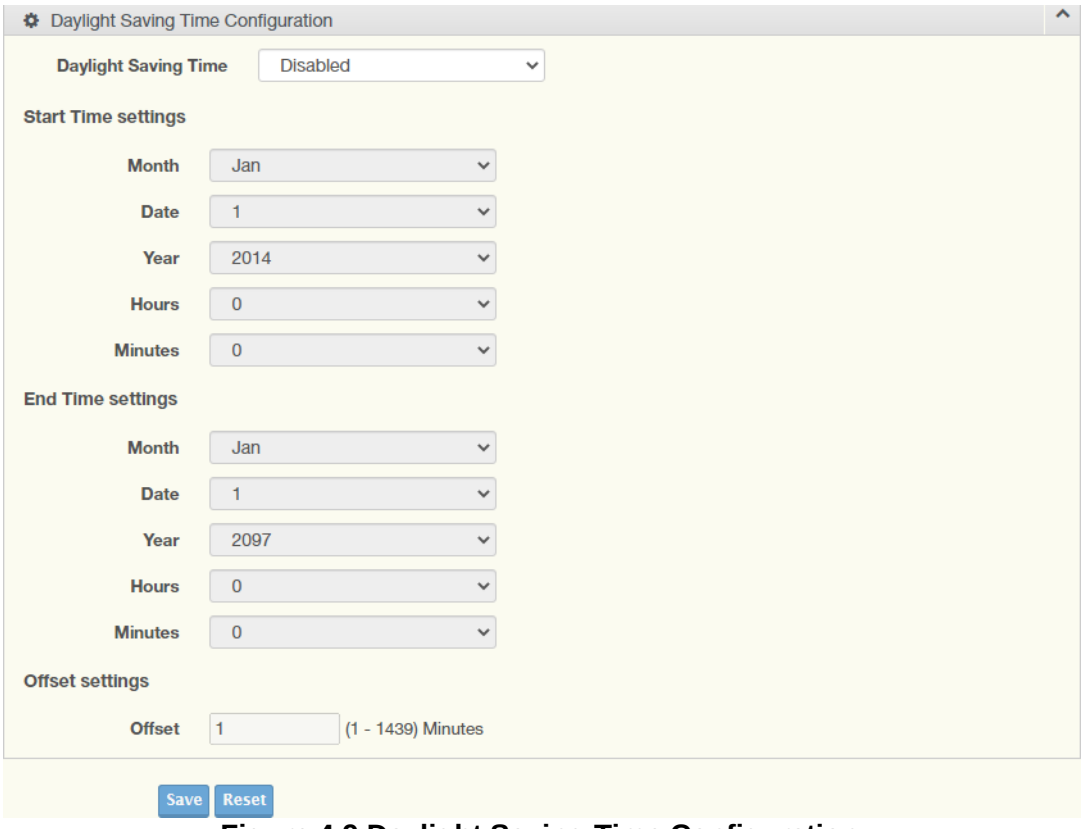


Figure 4.9 Daylight Saving Time Configuration

The following table describes the items in the previous figure.

Item	Description
Daylight Saving Time	Click the drop-down menu to select disable (default), recurring, non-recurring. ■ Disabled ■ Recurring: the configuration repeats every year ■ Non-Recurring: A single time configuration
Start Time Settings	Enter the Month, Date, Year, Hours, and Minutes to setup start time.
End Time Settings	Enter the Month, Date, Year, Hours, and Minutes to setup end time.
Offset Settings	Enter the number of minutes to add during Daylight Saving Time (Range: 1 to 1439).
Save	Click **Save** to store the settings.
Reset	Click **Reset** to clear the settings.

4.3.1.5 Log Configuration

The System Log provides server mode operations. When the mode is enabled, a syslog message is sent to the syslog server. The syslog protocol is based on UDP communication and received on UDP port 514. The syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet are sent out even if the syslog server does not exist.

To configure System Log, access the page as follows:

1. Navigate to **Configuration** > **System** and click **Log**.
   The System Log Configuration page displays.

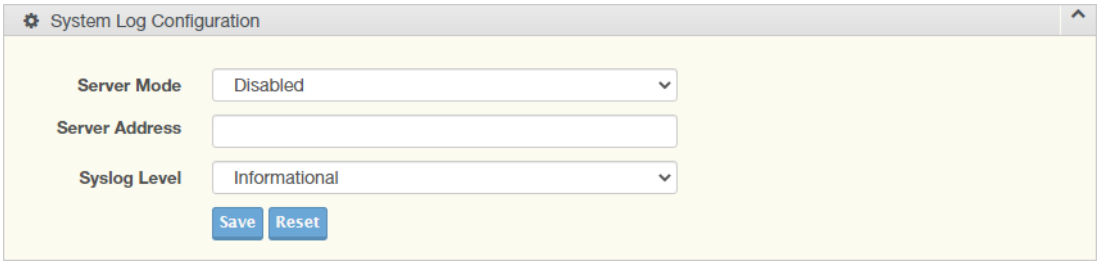


Figure 4.10 System Log Configuration

The following table describes the items in the previous figure.

Item	Description
Server Mode	Click the drop-down menu to enable or disable (default) the server mode function.
Server Address	Enter the IPv4 host address of the syslog server. If DNS is featured, a domain name can be indicated.
Syslog Level	Click the drop-down menu to indicate the type of message: ■ Error: Send a specific message(s) if the severity code is less or equal than Error (3). ■ Warning: Send a specific message(s) if the severity code is less or equal than Warning (4). ■ Notice: Send a specific message(s) if the severity code is less or equal than Notice (5). ■ Informational: Send a specific message(s) if the severity code is less or equal than Informational (6).
Save	Click **Save** to store the settings.
Reset	Click **Reset** to clear the settings.

4.3.2 Ports Configuration

The System Log provides server mode operations. When the mode is enabled, a syslog message is sent to the syslog server. The syslog protocol is based on UDP communication and received on UDP port 514. The syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet are sent out even if the syslog server does not exist.

To configure System Log, access the page as follows:

1. Navigate to **Configuration** and click **Ports**.
   The Port Configuration page displays.

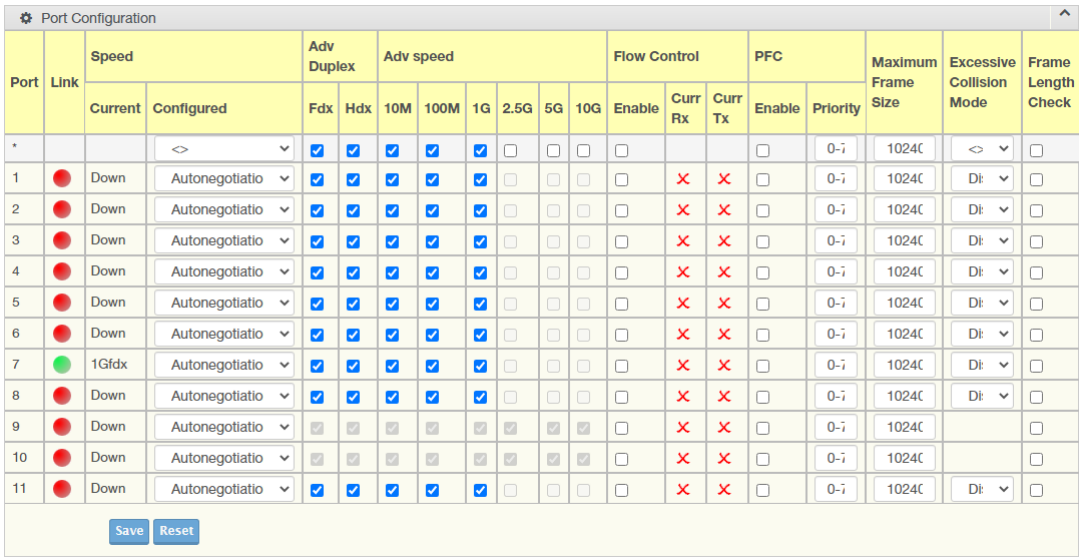


Figure 4.11 Port Configuration

The following table describes the items in the previous figure.

Item	Description
Port	Displays the logical port number of the entry.
Link	Displays the current link state. Green indicates the link is up and red that it is down.
Current Link Speed	Displays the current link speed of the port.
Configured Link Speed	Click the drop-down menu to select an available link speed for the given switch port. Only speeds supported by the specific port are shown. ■ Disabled - Disables the switch port operation. ■ Auto negotiation - Port auto negotiating speed and duplex with the link partner and selects the highest speed that is compatible with the link partner. ■ 10Mbps HDX - Forces the port in 10Mbps half duplex mode. ■ 10Mbps FDX - Forces the port in 10Mbps full duplex mode. ■ 100Mbps HDX - Forces the port in 100Mbps half duplex mode. ■ 100Mbps FDX - Forces the port in 100Mbps full duplex mode. ■ 1Gbps FDX - Forces the port in 1Gbps full duplex
Advertise Duplex	If duplex is set as auto negotiation, the port only advertises the specified duplex as either Fdx or Hdx to the link partner. By default port will advertise all the supported duplexes if the Duplex is Auto.
Advertise Speed	If speed is set as auto negotiation, the port only advertises the specified speeds (10M 100M 1G 2.5G 5G 10G) to the link partner. By default port will advertise all the supported speeds if speed is set as Auto.

Item	Description
Flow Control	If auto speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner, otherwise fixed-speed is used if selected. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto Negotiation setting. Check a setting to use flow control. This setting is related to the setting for Configured Link Speed. Note: The 100FX standard doesn't support Auto Negotiation. In 100FX mode the flow control capabilities are shown as disabled.
PFC	When PFC (802.1Qbb Priority Flow Control) is enabled on a port flow control on a priority level is enabled. Through the Priority field, range (one or more) of priorities can be configured, e.g. '0-3,7' which equals '0,1,2,3,7'. PFC is not supported through auto negotiation. PFC and Flowcontrol cannot both be enabled on the same port.
Maximum Frame Size	Enter the maximum frame size allowed for the switch port, including FCS. The range is 1518-10240 bytes.
Excessive Collision Mode	Configure the port transmit collision behavior. ■ Discard: Discard frame after 16 collisions (default). ■ Restart: Restart backoff algorithm after 16 collisions.
Frame Length Check	Check an option to configure if frames with incorrect frame length in the EtherType/Length field are to be dropped. An Ethernet frame contains a field EtherType which can be used to indicate the frame payload size (in bytes) for values of 1535 and below. If the EtherType/ Length field is above 1535, it indicates that the field is used as an EtherType (indicating which protocol is encapsulated in the payload of the frame). If frame length check is enabled and EtherType/Length field doesn't match the actually payload length, frames with payload size less than 1536 bytes are dropped. If frame length check is disabled, frames are not dropped due to frame length mismatch. Note: No drop counters count frames dropped due to frame length mismatch
Save	Click **Save** to store the settings.
Reset	Click **Reset** to clear the settings.

4.3.3 VLANs

4.3.3.1 Global VLAN Configuration

The function allows you to configure VLAN control settings.

1. Navigate to **Configuration** > **VLANs** and click **Configuration**.

The Global VLAN Configuration page displays.

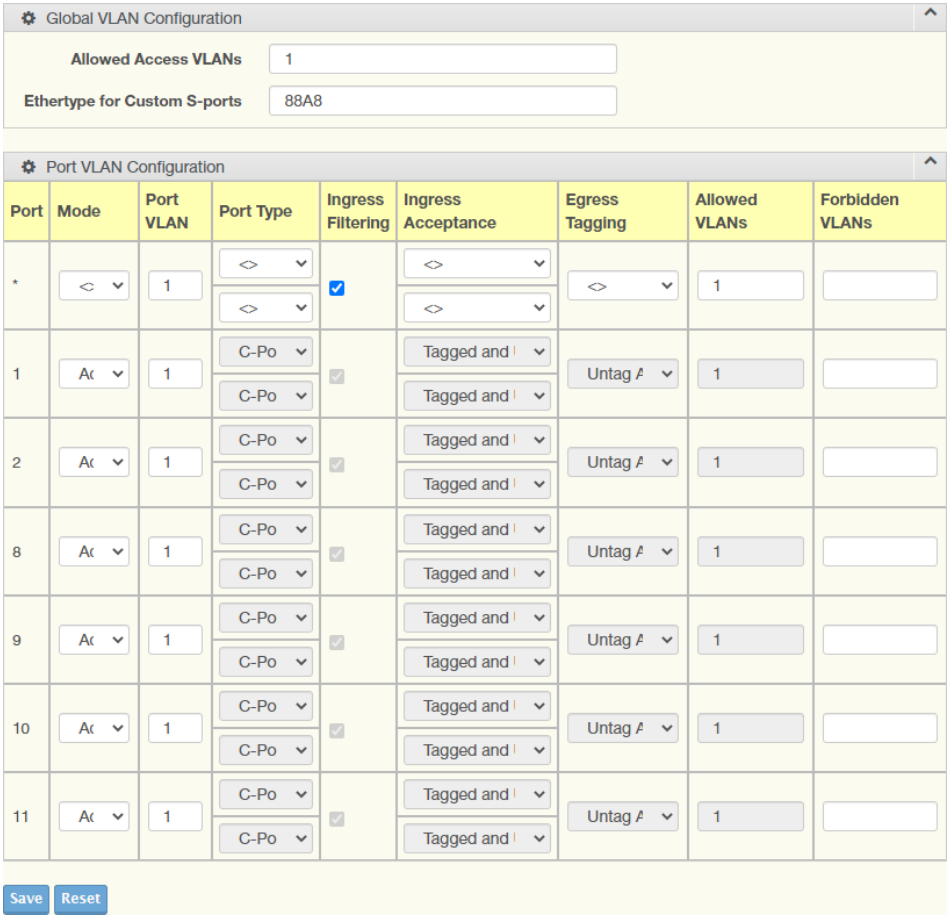


Figure 4.12 Global VLAN Configuration

The following table describes the items in the previous figure.

Item	Description
Global VLAN Configuration	
Allowed Access VLANs	Enter the string to indicate the allowed access VLANs. VLAN 1 is enabled by default. List range entry is supported.
Ethertype for Custom S-ports	Enter the string to indicate the ethertype/TPID used for custom s-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.
Port VLAN Configuration	
Port	Displays the logical port number for the entry.

Item	Description
Mode	Click the drop-down menu to indicate the behavior of the port. Options: ■ Access: Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics: Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1 Accepts untagged and C-tagged frames Discards all frames not classified to the Access VLAN On egress all frames are transmitted untagged ■ Trunk: Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics: By default, a trunk port is member of all VLANs (1 to 4095) The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs Frames classified to a VLAN that the port is not a member of are discarded By default, all frames but frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress ■ Hybrid: Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities: Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware Ingress filtering can be controlled Ingress acceptance of frames and configuration of egress tagging can be configured independently
Port VLAN	Enter the string to indicate the port's VLAD ID (range: 1 to 4095, default 1).

Item	Description
Port Type	Click the drop-down menu to indicate the port type. Options: ■ Unaware: On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress. ■ C-Port: On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag. ■ S-Port: On egress, if frames must be tagged, they will be tagged with an S-tag. On ingress, frames with a VLAN tag with TPID = 0x88A8 get classified to the VLAN ID embedded in the tag. Priority-tagged frames are classified to the Port VLAN. If the port is configured to accept Tagged Only frames (see Ingress Acceptance below), frames without this TPID are dropped. ■ S-Custom-Port: On egress, if frames must be tagged, they will be tagged with the custom S-tag. On ingress, frames with a VLAN tag with a TPID equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. Priority-tagged frames are classified to the Port VLAN. If the port is configured to accept Tagged Only frames (see Ingress Acceptance below), frames without this TPID are dropped.
Ingress Filtering	Click to enable (default) or disable ingress filtering. ■ Enabled: frames classified to a VLAN that the port is not a member of get discarded. ■ Disabled: frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.
Ingress Acceptance	Click the drop-down menu to indicate the ingress acceptance type. Options: ■ Tagged and Untagged: Both tagged and untagged frames are accepted. See Port Type for a description of when a frame is considered tagged. ■ Tagged Only: Only frames tagged with the corresponding Port Type tag are accepted on ingress. ■ Untagged Only: Only untagged frames are accepted on ingress. See Port Type for a description of when a frame is considered untagged.
Egress Tagging	Click the drop-down menu to indicate the frame egress tagging control. Options: ■ Untag Port VLAN: Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag. ■ Tag All: All frames, whether classified to the Port VLAN or not, are transmitted with a tag. ■ Untag All: All frames, whether classified to the Port VLAN or not, are transmitted without a tag. This option is only available for ports in Hybrid mode.
Allowed VLANs	Enter the string to indicate the bound VLAN membership. By default, a Trunk or Hybrid port becomes member of all VLANs, and is therefore set to 1 to 4095.

Item	Description
Forbidden VLANs	Enter the string to indicate the exclusion of membership to a VLAN membership. Note: Dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs, which is achieved through this function. By default, the field is left blank indicating that the port can be a member of all possible VLANs.
Save	Click **Save** to create a new user account.
Reset	Click **Reset** to clear the settings.

4.3.3.2 SVL Configuration

The function allows you to configure VLAN control settings.

In SVL, one or more VLANs map to a Filter ID (FID). By default, there is a one-to-one mapping from VLAN to FID, in which case the switch acts as an IVL bridge, but with SVL multiple VLANs may share the same MAC address table entries.

1. Navigate to **Configuration** > **VLANs** and click **SVL**.
   The Shared VLAN Learning Configuration page displays.

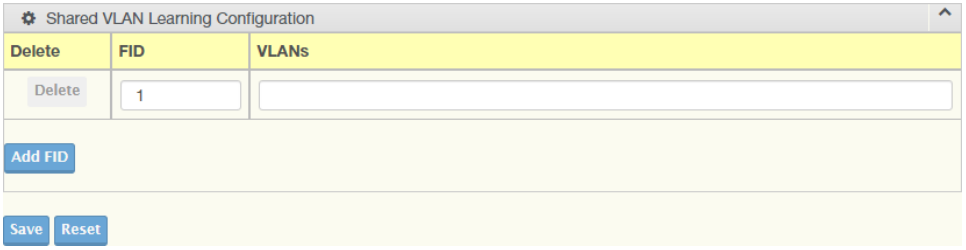


Figure 4.13 Shared VLAN Learning Configuration

The following table describes the items in the previous figure.

Item	Description
Delete	Click Delete to remove an allocated FID.
FID	Enter the string to indicate the ID to bind with the VLAN learning function as shown in the MAC table. SVL must be enabled. Range: 1 to 4095.
VLANs	Enter the string to indicate the VLANs to be mapped into FID. Both individual and range entries are supported.
Add FID	Click **Add FID** to add a new entry in the SVL table.
Save	Click **Save** to create a new user account.
Reset	Click **Reset** to clear the settings.

4.3.4 QoS

4.3.4.1 Port Classification

This function allows you to configure the basic QoS Classification settings for all switch ports.

1. Navigate to **Configuration** > **QoS** and click **Port Classification**.

The QoS Port Classification page displays.

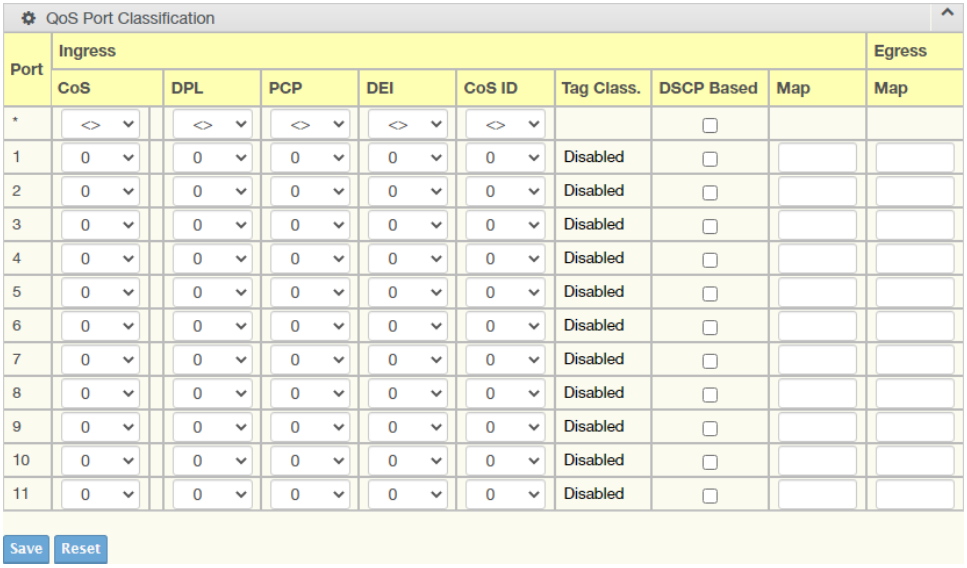


Figure 4.14 QoS Port Classification

The following table describes the items in the previous figure.

Item	Description
Port	Displays the port number for the configuration entry.
CoS	Click the drop-down menu to select the default CoS value. All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority. Note: If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.
DPL	Click the drop-down menu to select the default DPL value. All frames are classified to a Drop Precedence Level. If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DPL. The classified DPL can be overruled by a QCL entry.
PCP	Click the drop-down menu to select the default PCP value. All frames are classified to a PCP value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.
DEI	Click the drop-down menu to select the default DEI value. All frames are classified to a DEI value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.
CoS ID	Click the drop-down menu to select the default CoS ID value. Every incoming frame is classified to a CoS ID, which later can be used as basis for rewriting of different parts of the frame.
Tag Class.	Displays the classification mode for the tagged frames on the port. ■ Disabled: Use default CoS and DPL for tagged frames. ■ Enabled: Use mapped versions of PCP and DEI for tagged frames. Note: This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL.
DSCP Based	Click to enable or disable (default) the DSCP Based QoS Ingress Port classification.

Item	Description
Ingress Map	Enter the string to indicate the ID for the Ingress Map (range: 0 to 255). An empty field indicates no map selection.
Egress Map	Enter the string to indicate the ID for the Egress Map (range: 0 to 511). An empty field indicates no map selection.
Save	Click **Save** to create a new user account.
Reset	Click **Reset** to clear the settings.

4.3.4.2 Port Policing

This function allows you to configure the Policer settings for all switch ports.

1. Navigate to **Configuration** > **QoS** and click **Port Policing**.
   The QoS Ingress Port Policer page displays.

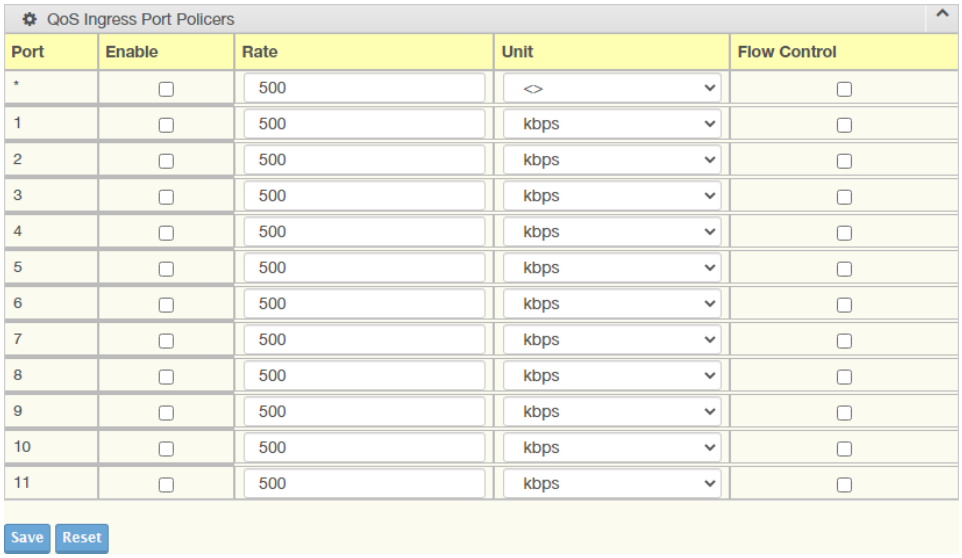


Figure 4.15 QoS Ingress Port Policer

The following table describes the items in the previous figure.

Item	Description
Port	Displays the port number for the entry.
Enable	Click to enable or disable (default) the port policer for the port.
Rate	Enter the string to indicate the control rate of the port policer (values: 10 to 13128147 for kbps, 1 to 13128 Mbps/fps/kfps).
Unit	Click the drop-down menu to select the measurement unit. Options: ■ kbps ■ Mbps ■ fps ■ kfps
Flow Control	Click to enable or disable (default) flow control mode. If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.
Save	Click **Save** to create a new user account.
Reset	Click **Reset** to clear the settings.

4.3.4.3 Queue Policing

This function allows you to configure the Queue Policer settings for all switch ports.

1. Navigate to **Configuration** > **QoS** and click **Quene Policing**.

The QoS Ingress Queue Policer Configuration page displays.

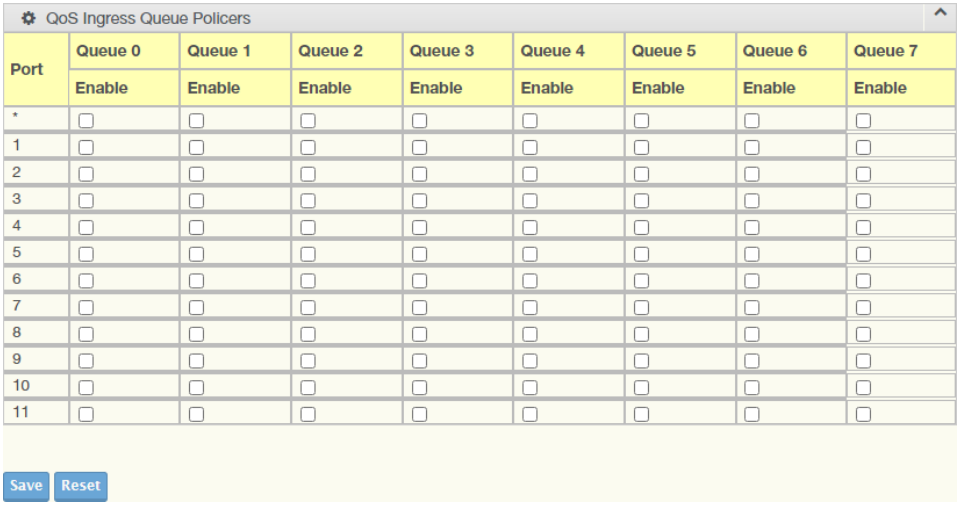


Figure 4.16 QoS Ingress Queue Policer Configuration

The following table describes the items in the previous figure.

Item	Description
Port	The port number for which the configuration below applies.
Enable (E)	Enable or disable the port policer for this switch port. If enabled, rate and unit options display.
Rate	Enter the string to indicate the rate for the queue policer (values: 10 to 13128147 for kbps, 1 to 13128 Mbps/fps/kfps). The field displays if one of the queue policers is enabled.
Unit	Click the drop-down menu to indicate the rate unit of measurement (options: kbps or Mbps). The field displays if one of the queue policers is enabled.
Save	Click **Save** to create a new user account.
Reset	Click **Reset** to clear the settings.

4.3.4.4 Port Scheduler

This function provides an overview of QoS Egress Port Schedulers for all switch ports.

1. Navigate to **Configuration** > **QoS** and click **Port Scheduler**.
   The QoS Egress Port Schedulers page displays.

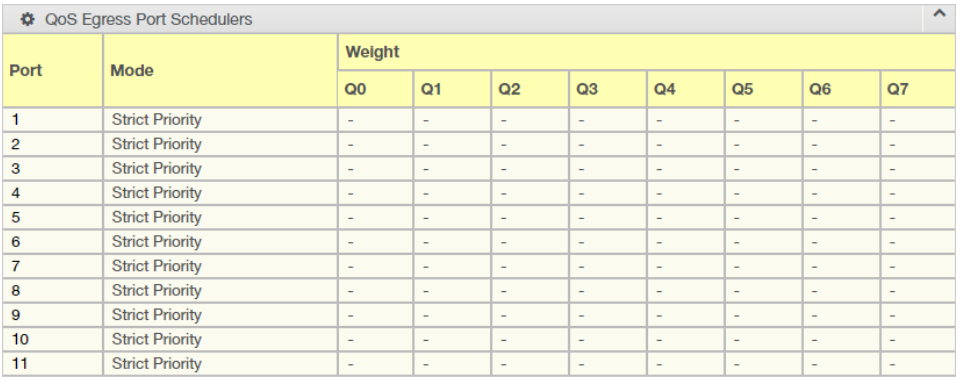


Figure 4.17 QoS Egress Port Schedulers

The following table describes the items in the previous figure.

Item	Description
Port	Displays the logical port settings. Click on a port number to view the Port Scheduler and Shapers page.
Mode	Shows the scheduling mode for this port.
Qn	Shows the weight for this queue and port.

4.3.4.4.1 Port Scheduler and Shapers Configuration

This function provides an overview of QoS Egress Port Schedulers for all switch ports.

1. Navigate to **Configuration** > **QoS** > **Port Scheduler** and click **Port #**..
   The QoS Egress Port Scheduler and Shapers page displays.

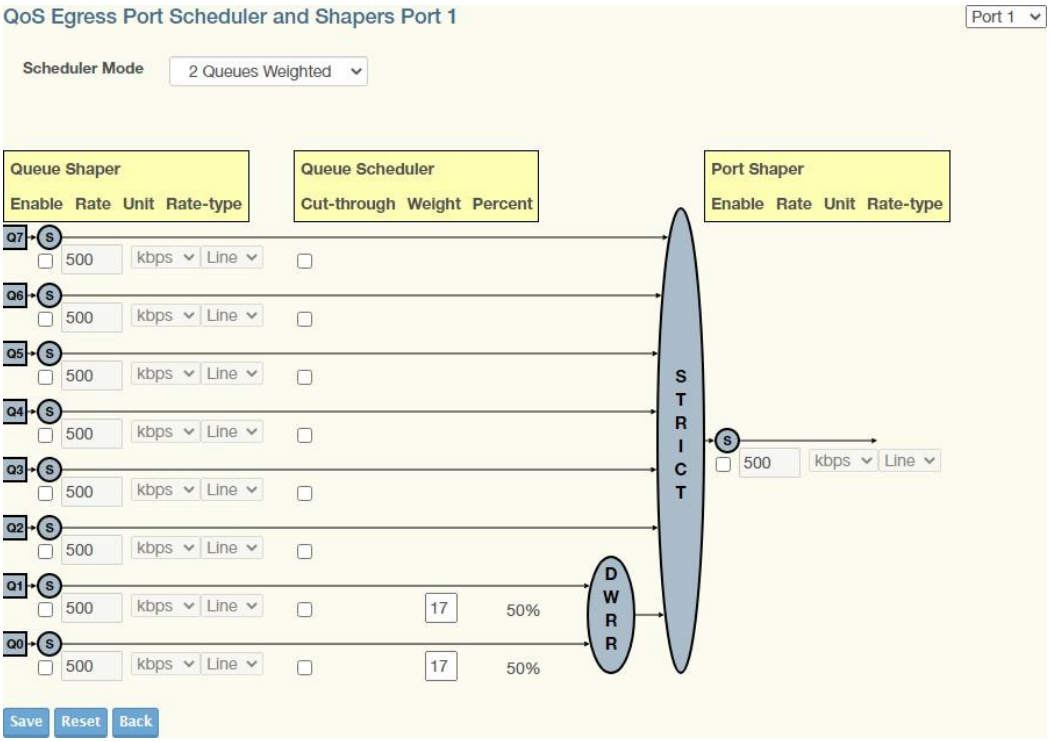


Figure 4.18 QoS Egress Port Scheduler and Shapers

The following table describes the items in the previous figure.

Item	Description
Scheduler Mode	Click the drop-down menu to indicate the number of queues to be scheduled as strict and how many are scheduled as weighted on the switch port.
Queue Shaper Enable	Click to enable or disable (default) the function.
Queue Shaper Rate	Enter the string to indicate the rate for the queue policer (values: 10 to 13128147 for kbps, 1 to 13128 Mbps/fps/kfps). The field displays if one of the queue policers is enabled.
Queue Shaper Unit	Click the drop-down menu to indicate the rate unit of measurement (options: kbps or Mbps). The field displays if one of the queue policers is enabled.
Queue Shaper Rate-type	Click the drop-down menu to indicate the rate type of the queue shaper. Options: ■ Line: Specify that this shaper operates on line rate. ■ Data: Specify that this shaper operates on data rate.

Item	Description
Queue Scheduler Cut-through	Click to enable or disable (default) cut-through.
Queue Scheduler Preemption	Click to enable or disable (default) frame preemption.
Queue Scheduler Weight	Enter the string to indicate the queue weight (values: 1 to 100). This parameter is only available if Scheduler Mode is set to Weighted.
Queue Scheduler Percent	Displays the queue weight as a percentage.
Port Shaper Enable	Click to enable or disable (default) port shaper.
Port Shaper Rate	Enter the string to indicate the rate for the port shaper (values: 100 to 13107100/kbps (1 to 13107 Mbps)).
Port Shaper Unit	Click the drop-down menu to select the unit measurement (values: kbps/Mbps).
Port Shaper Rate-type	Click the drop-down menu to select the rate type. Options: ■ Line: Specify that this shaper operates on line rate. ■ Data: Specify that this shaper operates on data rate.
Save	Click **Save** to create a new user account.
Reset	Click **Reset** to clear the settings.
Back	Click **Back** to return to the previous menu without saving settings.

4.3.4.5 Port Shaping

This function provides an overview of QoS Egress Port Shapers for all switch ports.

1. Navigate to **Configuration** > **QoS** and click **Port Shaping**.
   The QoS Egress Port Shapers page displays.

QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-	-	-
9	-	-	-	-	-	-	-	-	-
10	-	-	-	-	-	-	-	-	-
11	-	-	-	-	-	-	-	-	-

Figure 4.19 QoS Egress Port Shapers

The following table describes the items in the previous figure.

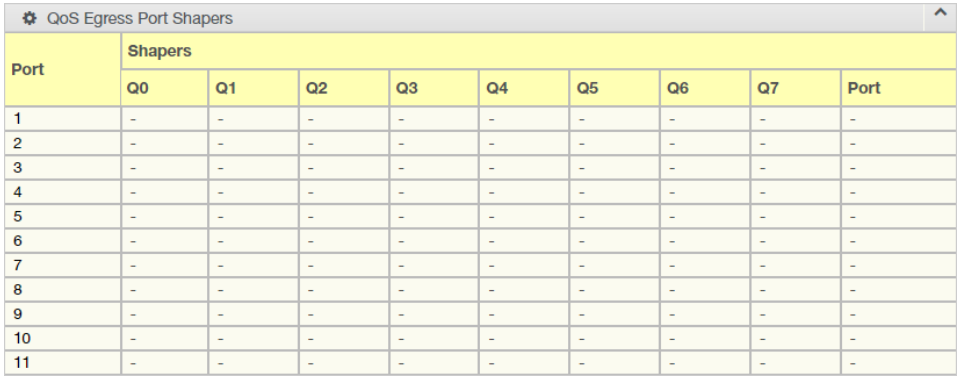
Item	Description
Port	Displays the logical port for the entry. Click on the port number in order to configure the shapers. See “Port Scheduler and Shapers Configuration” on page 47.
Qn	Displays the shaper rate status: disabled or actual queue shaper rate.
Port	Displays the shaper rate status: disabled or actual port shaper rate.

4.3.4.6 Port Tag Remarking

This function provides an overview of QoS Egress Port Tag Remarking for all switch ports.

1. Navigate to **Configuration** > **QoS** and click **Port Tag Remarking**.

The QoS Egress Port Tag Remarking page displays.



Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-	-	-
9	-	-	-	-	-	-	-	-	-
10	-	-	-	-	-	-	-	-	-
11	-	-	-	-	-	-	-	-	-

Figure 4.20 QoS Egress Port Tag Remarking

The following table describes the items in the previous figure.

Item	Description
Port	Displays the logical port for the entry. Click on the port number to to configure tag remarking.
Mode	Shows the tag remarking mode for this port. **Classified:** Use classified PCP/DEI values. **Default:** Use default PCP/DEI values. **Mapped:** Use mapped versions of CoS and DPL.

4.3.4.6.1 Egress Port Tag Remarking Configuration

This function provides an overview of QoS Egress Port Tag Remarking for all switch ports.

1. Navigate to **Configuration** > **QoS** and click **Port Tag Remarking**.
   The QoS Egress Port Tag Remarking page displays.

Figure 4.21 QoS Egress Port Tag Remarking PortN

The following table describes the items in the previous figure.

Item	Description
Tag Remarking Mode	Click the drop-down menu select the mode. Options: ■ Classified: Use classified PCP/DEI values ■ Default: Use default PCP/DEI values ■ Mapped: Use mapped versions of CoS and DPL
Port	Click the drop-down menu to select the port to configure.
Save	Click **Save** to create a new user account.
Reset	Click **Reset** to clear the settings.
Cancel	Click **Cancel** to return to the previous menu without saving settings.

4.3.4.7 Port DSCP

This function allows you to configure the basic QoS Port DSCP Configuration settings for all switch ports.

1. Navigate to **Configuration** > **QoS** and click **Port DSCP**.

The Port DSCP Configuration page displays.

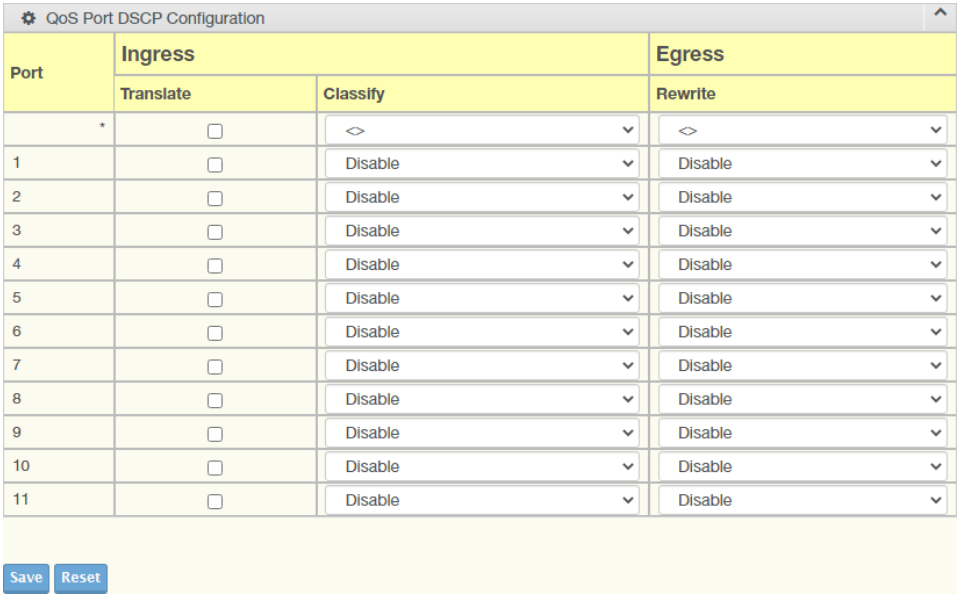


Figure 4.22 Port DSCP Configuration

The following table describes the items in the previous figure.

Item	Description
Port	Displays the port number of the entry.
Ingress Translate	Click to enable or disable (default) the Ingress Translation settings.
Ingress Classify	Click the drop-down menu to select the port classification. Options: ■ **Disable:** No Ingress DSCP Classification ■ **DSCP=0:** Classify if incoming (or translated if enabled) DSCP is 0 ■ **Selected:** Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP ■ **All:** Classify all DSCP
Egress	■ Click the drop-down menu to set the egress rewriting setting. Options: ■ **Disable:** No Egress rewrite. ■ **Enable:** Rewrite enabled without remapping. ■ **Remap:** DSCP from analyzer is remapped and frame is remarked with remapped DSCP value.
Save	Click **Save** to save changes.
Reset	Click **Reset** to undo any changes made locally and revert to previously saved values.

4.3.4.8 DSCP-Based QoS

This function allows you to configure the basic QoS DSCP based QoS Ingress Classification settings for all switches.

1. Navigate to **Configuration** > **QoS** and click **DSCP-Based QoS**.

The DSCP based QoS Ingress Classification page displays.

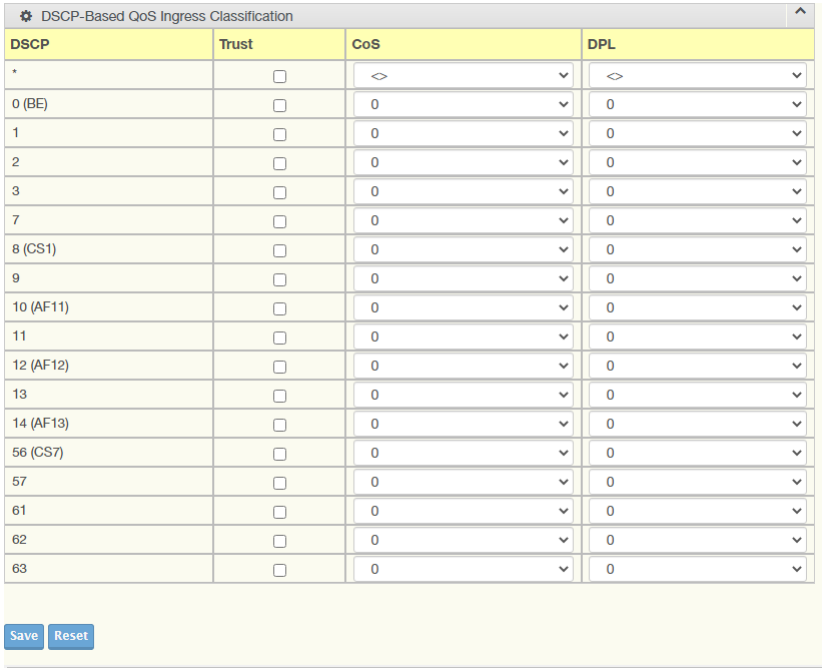


Figure 4.23 DSCP based QoS Ingress Classification

The following table describes the items in the previous figure.

Item	Description
DSCP	Displays the maximum number of supported DSCP (64).
Trust	Click to enable or disable (default) trust classification. Only frames with trusted DSCP values are mapped to a specific CoS and DPL. Frames with untrusted DSCP values are treated as a non-IP frame.
CoS	Click the drop-down menu to set the CoS value (values: 0 to 7).
DPL	Click the drop-down menu to set the Drop Precedence Level (values: 0 to 3).
Save	Click **Save** to save changes.
Reset	Click **Reset** to undo any changes made locally and revert to previously saved values.

4.3.4.9 DSCP Translation

This function allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress.

1. Navigate to **Configuration** > **QoS** and click **DSCP Translation**.

The DSCP Translation page displays.

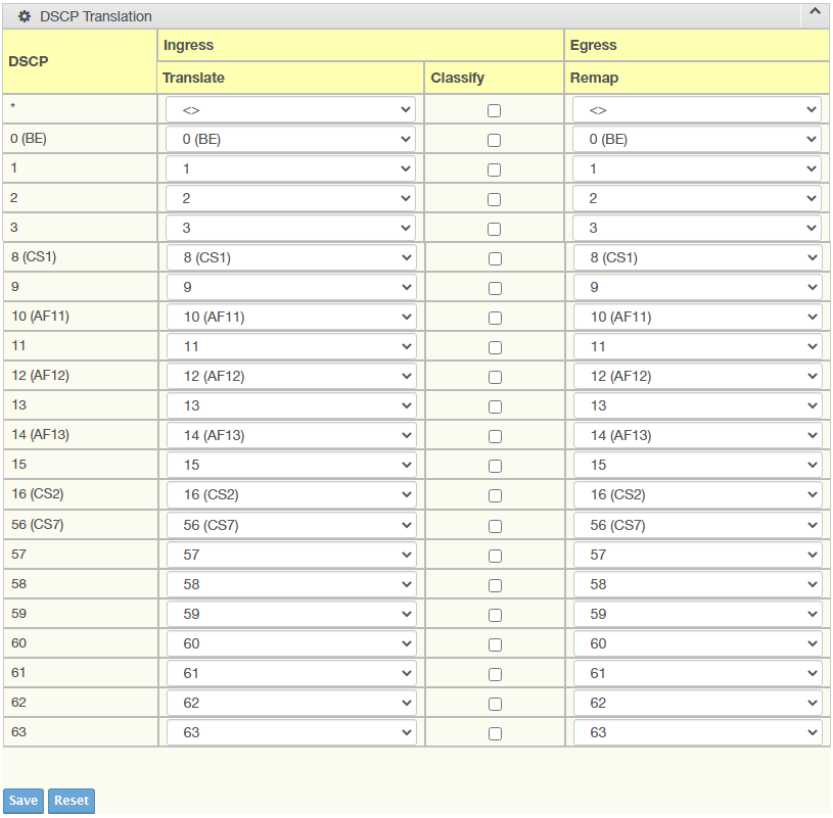


Figure 4.24 DSCP Translation

The following table describes the items in the previous figure.

Item	Description
DSCP	Displays the maximum number of supported DSCP values (range: 0 to 63).
Trust	Click to enable or disable (default) trust for the DSCP entry.
CoS	Click the drop-down menu to select the precedence level (values: 0 to 3).
DPL	Click the drop-down menu to select the CoS value (values: 0 to 7).
Save	Click **Save** to save changes.
Reset	Click **Reset** to undo any changes made locally and revert to previously saved values.

4.3.4.10 DSCP Classification

This function allows you to configure the mapping of CoS and DPL to DSCP value.

1. Navigate to **Configuration** > **QoS** and click **DSCP Classification**.

The DSCP Classification page displays.

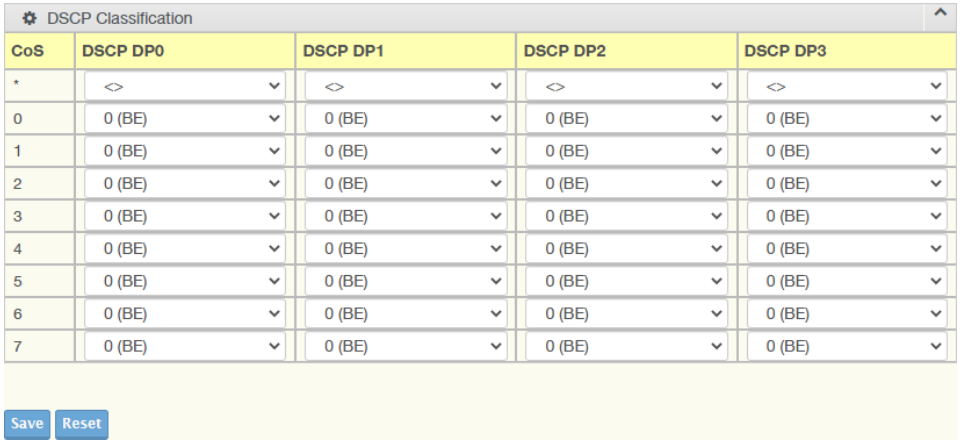


Figure 4.25 DSCP Classification

The following table describes the items in the previous figure.

Item	Description
CoS	Displays the identifier for the class of service entry.
DSCP DP0	Click the drop-down menu to select the classified DSCP value (values: 0 to 63) for Drop Precedence Level 0.
DSCP DP1	Click the drop-down menu to select the classified DSCP value (values: 0 to 63) for Drop Precedence Level 1.
DSCP DP2	Click the drop-down menu to select the classified DSCP value (values: 0 to 63) for Drop Precedence Level 2.
DSCP DP3	Click the drop-down menu to select the classified DSCP value (values: 0 to 63) for Drop Precedence Level 3.
Save	Click **Save** to save changes.
Reset	Click **Reset** to undo any changes made locally and revert to previously saved values.

4.3.4.11 Ingress Map

This function shows a table of QoS Ingress Maps which is made up of individual map entries. Each entry has a key and an action. The key indicates which fields of the frame will be mapped to the fields specified by and according to the action. Each Map can hold a number of map rules, or mappings between possible keys and actions. Which of those rules will be applied depends on the selection of (Key-Type, Action-Type). Each row describes a user-defined map.

Maps contain multiple rules. The page allows you to view and configure the key and action filters that will be used when searching through the rules.

1. Navigate to **Configuration** > **QoS** and click **Ingress Map**.

   The QoS Ingress Map Configuration page displays.

Figure 4.26 QoS Ingress Map Configuration

The following table describes the items in the previous figure.

Item	Description
Map ID	Displays the map ID for the entry. Click the ID to edit the Ingress map.

Item	Description
Key-Type	Displays the key type for the entry. Options: ■ **PCP:** Use PCP as key for tagged frames and none for the rest. Table width: 1 ■ **PCP - DEI:** Use PCP/DEI as key for tagged frames and none for the rest. Table width: 2 ■ **DSCP:** Use DSCP as key for IP frames and none for the rest. Table width: 8 ■ **DSCP - PCP - DEI:** Use DSCP as key for IP frames, PCP/DEI for tagged frames and none for the rest. Table width:10
Action-Type	Indicates the Action Type for filtering the map rules when applying the map. Options: ■ **CoS:** Class of Service ■ **DPL:** Drop Precedence Level ■ **PCP:** Priority Code Point ■ **DEI:** Drop Eligible Indicator ■ **DSCP:** Differentiated Services Code Point ■ **CoS ID:** CoS ID
QoS Ingress Map Modification Buttons	Click to modify the selected entry. Options: ■ **Edit**: Edits the map ■ **Delete**: Deletes the map ■ **Add**: Adds a new map in the table
Refresh	Click **Refresh** to refresh the page.
Remove All	Click **Remove All** to remove all Ingress Maps (and their corresponding rules).

4.3.4.12 Egress Map

This function displays QoS Egress Maps made up of individual map entries. Each entry has a key and an action indicating the field of the frame corresponding to the specified field action. Each Map can hold a number of map rules, or mappings between possible keys and actions. Which of those rules will be applied depends on the selection of (Key-Type, Action-Type).

NOTE: This is just an overview of the configured maps. The user can add new ones or edit existing maps using the Add/Edit buttons. Click on the lowest plus sign (empty map entry) to add a new Ingress Map to the table.

QoS Map Rules Configuration

Maps have multiple rules inside them and this page allows to view and configure the key and action filters that will be used when searching through the rules. To see and configure the set of rules for each map click on the Map ID (link) for each map. (Note: not the edit button).

1. Navigate to **Configuration** > **QoS** and click **Egress Map**.
   The QoS Egress Map Configuration page displays.

Figure 4.27 QoS Egress Map Configuration

The following table describes the items in the previous figure.

Item	Description
Map ID	Indicates the Map (unique) ID. Range is 0 to 511.

Item	Description
Key-Type	Indicates the Key Type that will be used to filter the map rules when applying the map. As mentioned above, map rules can have various keys and this is to make a select set of them. Possible Key types are: **CoS ID:** Use classified COS ID as key. Table width: 1 **CoS ID - DPL:** Use classified COS ID and DPL as key. Table width: 4 **DSCP:** Use classified DSCP as key. Table width: 8 **DSCP - DPL:** Use classified DSCP and DPL as key. Table width: 32
QoS Egress Map Modification Buttons	It is possible to modify each map (or add new maps) in the table using the following buttons: ■ **Edit**: Edits the map. ■ **Delete**: Deletes the map. ■ **Add**: Adds a new map in the table.
Refresh	Click **Refresh** to refresh the page.
Remove All	Click **Remove All** to remove all Ingress Maps (and their corresponding rules).

4.3.4.13 QoS Control List

This function shows the QoS Control List (QCL) consisting of the QCEs. Each row describes a defined QCE. The maximum number of QCEs is 256 on each switch.

Click on the lowest plus sign to add a new QCE to the list.

1. Navigate to **Configuration** > **QoS** and click **QoS Control List**.
   The QoS Control List Configuration page displays.

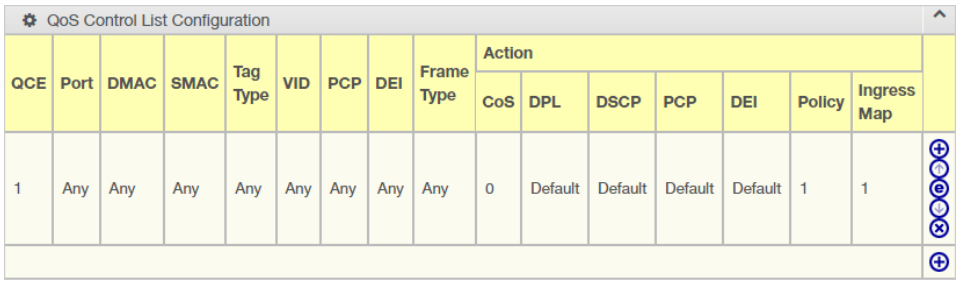


Figure 4.28 QoS Control List Configuration

The following table describes the items in the previous figure.

Item	Description
QCE	Indicates the QCE ID.
Port	Indicates the list of ports configured with the **QCE** or **Any**.
DMAC	Indicates the destination MAC address. Possible values are: ■ **Any (default):** Match any DMAC ■ **Unicast:** Match unicast DMAC ■ **Multicast:** Match multicast DMAC ■ **Broadcast:** Match broadcast DMAC ■ **<MAC>:** Match specific DMAC
SMAC	Match specific source MAC address or **Any**.
Tag Type	Indicates tag type. Possible values are: ■ **Any (default):** Match tagged and untagged frames. ■ **Untagged:** Match untagged frames. ■ **Tagged:** Match tagged frames. ■ **C-Tagged:** Match C-tagged frames. ■ **S-Tagged:** Match S-tagged frames.

Item	Description
VID	Indicates (VLAN ID), either a specific VID or range of VIDs (range 1 to 4095 or Any).
PCP	Indicates the Priority Code Point. Single values, a range, or Any are displayed.
DEI	Indicates a Drop Eligible Indicator. Values: 0, 1 or **Any**.
Frame Type	Indicates the type of frame. Possible values are: ■ **Any:** Match any frame type. ■ **Ethernet:** Match EtherType frames. ■ **LLC:** Match (LLC) frames. ■ **SNAP:** Match (SNAP) frames. ■ **IPv4:** Match IPv4 frames. ■ **IPv6:** Match IPv6 frames.
Action	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are: ■ **CoS:** Classify Class of Service. ■ **DPL:** Classify Drop Precedence Level. ■ **DSCP:** Classify DSCP value. ■ **PCP:** Classify PCP value. ■ **DEI:** Classify DEI value. ■ **Policy:** Classify ACL Policy number. ■ **Ingress Map:** Classify Ingress Map ID.
Modification Buttons	Click an option to modify the selected QCE (QoS Control Entry) entry. Options: ■ **Insert**: Inserts a new QCE before the current row. ■ **Edits**: Edits the QCE. ■ **Move Up**: Moves the QCE up the list. ■ **Move Down**: Moves the QCE down the list. ■ **Delete**: Deletes the QCE. ■ **Add to End of List**: The lowest plus sign adds a new entry at the bottom of the QCE listings.

4.3.4.14 Storm Policing

This storm policers for the switch are configured on this page. There is a unicast storm policer, multicast storm policer, and a broadcast storm policer, only for flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present in the MAC Address table.

1. Navigate to **Configuration** > **QoS** and click **Storm Policing**.
   The Storm Policer Configuration page displays.

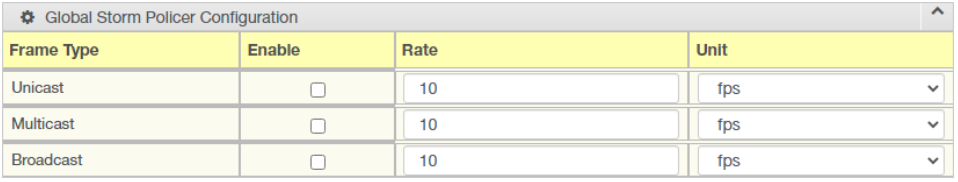


Figure 4.29 Storm Policer Configuration

The following table describes the items in the Global Storm Policer Configuration figure.

Item	Description
Frame Type	Display the frame type for which the configuration below applies.

Item	Description
Enable	Click to enable or disable (default) the global storm policer for the given frame type.
Rate	Enter the string to indicate the rate for the global storm policer (value: 10 to 13128147 fps or kbps, and 1 to 13128 kfps or Mbps). Supported rates are divisible by 10 fps or 25 kbps.
Unit	Click the drop-down menu to select the unit of measure for the global storm policer rate (value: fps, kfps, kbps or Mbps).
Save	Click **Save** to save changes.
Reset	Click **Reset** to undo any changes made locally and revert to previously saved values.

The following table describes the items in the Port Storm Policer Configuration figure.

Port storm policers for all switch ports are configured on this page.

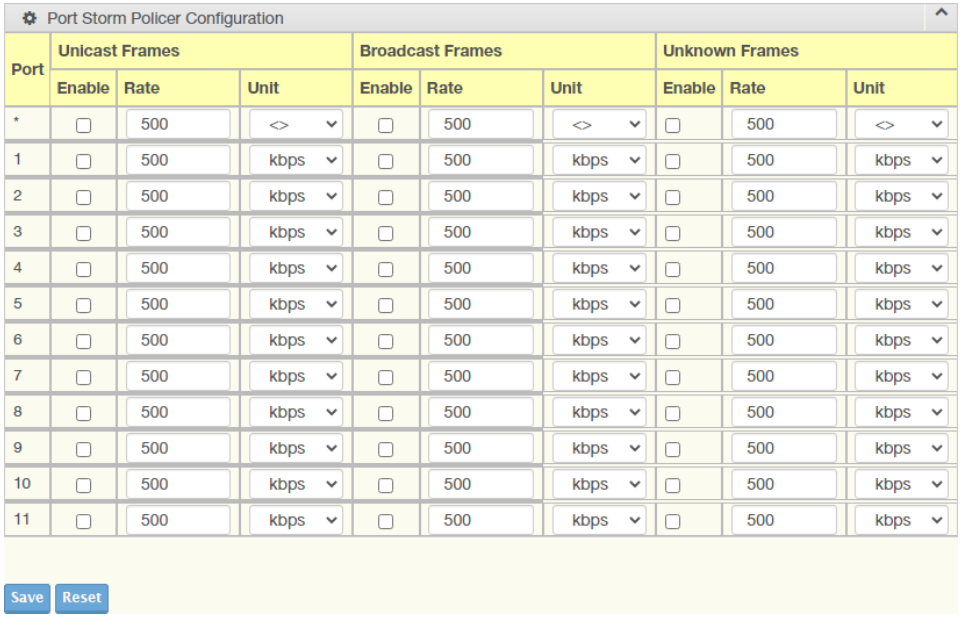


Figure 4.30 Port Storm Policer Configuration

Item	Description
Port	Displays the port number for the configuration below applies.
Enable	Click enable or disable (default) the storm policer for this switch port.
Rate	Enter the string to indicate the rate for the port storm policer (value: 10 to 13128147 fps or kbps, and 1 to 13128 kfps or Mbps). Supported rates are divisible by 10 fps or 25 kbps.
Unit	Click the drop-down menu to select the unit of measurement for the port storm policer rate (value: fps, kfps, kbps or Mbps).
Save	Click **Save** to save changes.
Reset	Click **Reset** to undo any changes made locally and revert to previously saved values.

4.3.5 TSN

4.3.5.1 PTP Check

When using TAS and PSFP between network elements, it is required to have a common global time reference provided by PTP. When booting the device, it will take some time for a configured PTP application to get locked to the common time reference. It may cause malfunctioning of TAS and PSFP if config-change is issued

before PTP time is in a Locked or Locking state. A function which can delay the issue of config-change until PTP is Locked/Locking or a configurable time has passed, can be configured here.

1. Navigate to **Configuration** > **TSN** and click **PTP check**.
   The TSN Configuration page displays.

Figure 4.31 TSN Configuration

The following table describes the items in the TSN Configuration page.

Item	Description
Procedure	Click the drop-down menu to select how to ensure PTP state. Options: ■ None ■ Time only ■ Time and Ptp
Timeout	Enter a string to indicate the maximal number of seconds to wait before config_change is issued.
PTPport	Enter a string to indicate the PTP port to use for sensing PTP status
Save	Click **Save** to save changes.
Reset	Click **Reset** to undo any changes made locally and revert to previously saved values.

4.3.5.2 Frame Preemption

This function provides an overview of TSN Egress Port Frame Preemption Configuration.

1. Navigate to **Configuration** > **TSN** and click **Frame Preemption**.
   The Frame Preemption Configuration page displays.

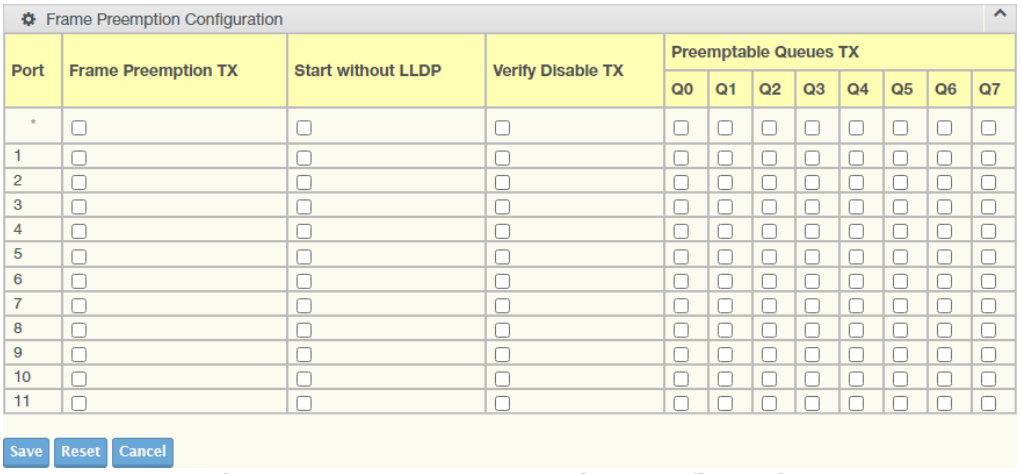


Figure 4.32 Frame Preemption Configuration

The following table describes the items in the Frame Preemption Configuration page.

Item	Description
Port	Displays the logical port for the settings contained in the same row. Please note that Frame Preemption is not supported on ports with maximum speed 25 Gigabit/sec and is also not supported on 10G Gigabit/sec Aquantia Copper port.
Frame Preemption TX	Click to enable or disable (default) the value of the 802.3br aMACMergeEnableTx parameter for the port. This value determines whether frame preemption is enabled (TRUE) or disabled (FALSE) in the MAC Merge sublayer in the transmit direction.
Start without LLDP	Click to enable or disable (default) when this field is checked, Frame Preemption will be active when Frame Preemption TX is checked.
Verify Disable TX	Click to enable or disable (default) the value of the 802.3br aMACMergeVerifyDisableTx parameter for the port. This value determines whether the verify function is disabled (TRUE) or enabled (FALSE) in the MAC Merge sublayer in the transmit direction.
Preemptable Queues	Click to select the parameter to a preemptive status for the priority. If checked, it takes value preemptable if frames queued for the priority are to be transmitted using the preemptable service for the Port. If not checked, it takes value express if frames queued for the priority are to be transmitted using the express service for the Port and preemption is enabled for the Port.
Save	Click **Save** to save changes.
Reset	Click **Reset** to undo any changes made locally and revert to previously saved values.
Cancel	Click **Cancel** to return to the previous menu without saving any updates.

4.3.5.3 TAS

4.3.5.3.1 Ports

This function allows the user to inspect the current TAS configurations, and possibly change them as well.

1. Navigate to **Configuration** > **TSN** > **TAS** and click **Ports**.
   The TAS Configuration Parameters page displays.

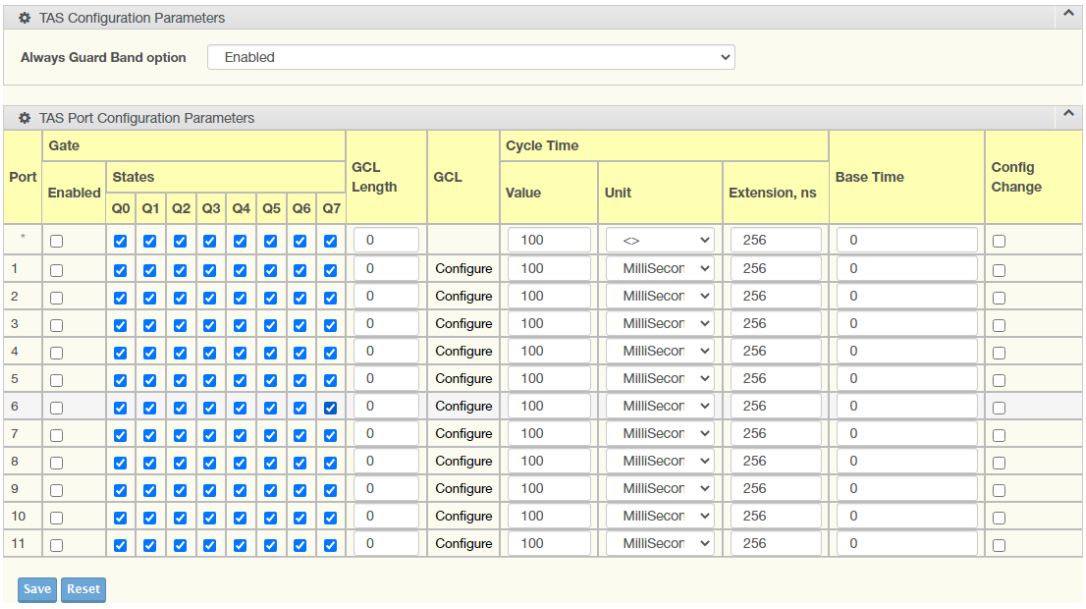


Figure 4.33 TAS Configuration Parameters

The following table describes the items in the TAS Configuration Parameters page.

Item	Description
Always Guard Band	Click the drop-down menu to enable (default) or disable the Always Guard Band option--defines how the values are calculated. If a Gate Control List does not contain SetAndHold and/or SetAndRelease operations the Always Guard Band option has no effect. If a Gate Control List does contain SetAndHold and SetAndRelease operations then: ■ When Always Guard Band is Enabled, a guard band is implemented on all queues, both Express and Preemptible queues. ■ When Always Guard Band is Disabled, a guard band is only implemented on Preemptible queues.
Port	Displays the port number of the device.
Gate Enabled	Click to enabled or disable (default) the parameter which determines whether traffic scheduling is active (true) or inactive (false).
Gate States	Click to enable (default) or disable the initial value of the port open states that is used when no Gate Control List is active on the Port.
GCL Length	Enter an string to indicate the Admin Gate Control List length parameter for the Port (range: 0 to 256). The integer value indicates the number of entries Gate Control Elements in the Gate Control List.
GCL	Displays the link to the Gate Control List parameter configuration.
Cycle Time	
Cycle Time Value	Enter the string to indicate the Admin Cycle Time (range: admin cycle Time 1 to 999999999, cycle time 256 to 999999999 nanoseconds) as defined by the number of units defined in the Unit field. The default value is 100 milliseconds.
Cycle Time Unit	Click the drop-down menu to select unit for the Admin Cycle Time (values: milliseconds, microseconds or nanoseconds).
Cycle Time Extension	Enter a string to indicate the integer in nanoseconds (range: 256 to 999999999) defining the maximum amount of time by which the gating cycle for the Port is permitted to be extended when a new cycle configuration is installed. The default value is 256 nanoseconds.
Base Time	Enter a string to indicate the Admin value of base time, expressed as an IEEE 1588 precision time protocol (PTP) timescale.
Config Change	Click to enable or disable (default) the Configuration Change parameter signals the start of a configuration change. After a successful configuration change, the configured Admin values will become the Oper values, which are displayed in the Monitor/TSN/TAS web page. If the value of parameter Base Time is in the future, the configuration change will be executed at Base Time.
Save	Click **Save** to save changes.
Reset	Click **Reset** to undo any changes made locally and revert to previously saved values.

4.3.5.3.2 Max SDU

This function allows you to inspect the current TAS configurations, and possibly change them as well.

1. Navigate to **Configuration** > **TSN** > **TAS** and click **Max SDU**.

The TAS SDU Configuration page displays.

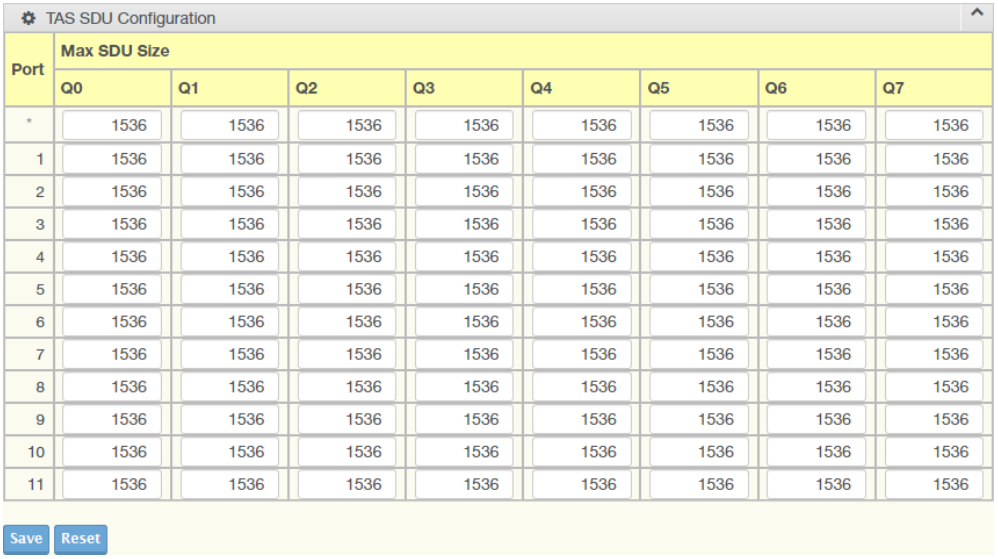


Figure 4.34 TAS SDU Configuration

The following table describes the items in the TAS SDU Configuration page.

Item	Description
Port	Displays the port number of the device.
Maximum SDU	Enter the value of the Maximum SDU size parameter for the traffic class supported by the port (values: unsigned integer in the range 0 to 10240). A value of 0 is interpreted as the Maximum SDU size supported by the underlying MAC: 10240. The default value of the Maximum SDU parameter is 1536. The Maximum SDU size parameter is used to calculate the guard band time = Maximum SDU * 8 / LINK_SPEED (sec) If frame preemption is enabled and a gate operaton is SetAndHold, the guard band time in preemptable queues is automatically selected as the frame preemption minimum fragment size plus 64 bytes. A queue is said to be preemptible, if frame preemption is enabled, and if this queue is not opened in a SetAndHold gate operation.
Save	Click **Save** to save changes.
Reset	Click **Reset** to undo any changes made locally and revert to previously saved values.

4.3.5.4 PSFP

4.3.5.4.1 Flow Meter

This function allows you to inspect the current PSFP configurations.

1. Navigate to **Configuration** > **TSN** > **PSFP** and click **Flow Meter**.
   The PSFP Flow Meter Configuration page displays.

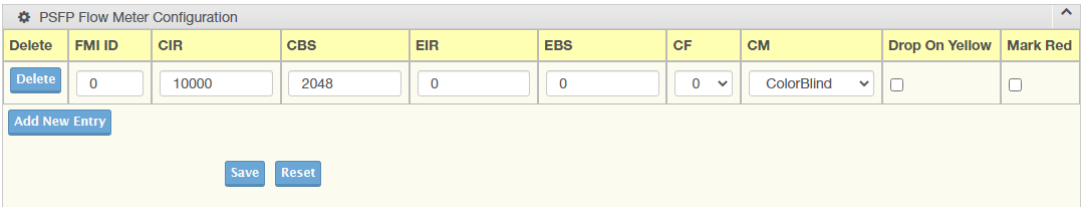


Figure 4.35 PSFP Flow Meter Configuration

The following table describes the items in the PSFP Flow Meter Configuration page.

Item	Description
Delete	Click **Delete** to remove the entry. It will be deleted during the next save.
FMI ID	Enter a string to indicate the FlowMeterInstance parameter is an index into the FlowMeterTable.
CIR	Enter a string to indicate the FlowMeterCIR parameter contains an integer value that represents the CIR value for the flow meter, in bit/s.
CBS	Enter a string to indicate the FlowMeterCBS parameter contains an integer value that represents the CBS value for the flow meter, in octets.
EIR	Additional information required.
EBB	Additional information required.
CF	Additional information required.
CM	Additional information required.
Drop on Yellow	Additional information required.
Mark RED	Click to enable or disable (default) the FlowMeterMarkAllFramesRed parameter contains a Boolean value that indicates whether, if the MarkAllFramesRed function is enabled, all frames are to be discarded (TRUE) or not (FALSE).
Add New Entry	Click **Add New Entry** to add Flow Meter entry.
Save	Click **Save** to save changes.
Reset	Click **Reset** to undo any changes made locally and revert to previously saved values.

4.3.5.4.2 Stream Filter

This function allows you to inspect the current PSFP configurations.

1. Navigate to **Configuration** > **TSN** > **PSFP** and click **Steam Filter**.
   The PSFP Stream Filter Configuration page displays.

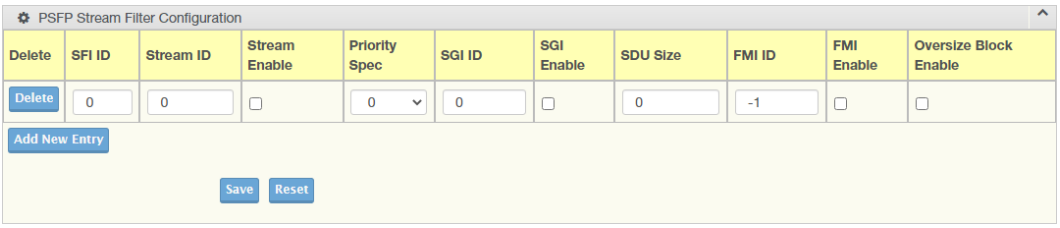


Figure 4.36 PSFP Stream Filter Configuration

The following table describes the items in the PSFP Stream Filter Configuration page.

Item	Description
Delete	Click **Delete** to remove the entry. It will be deleted during the next save.
SFI ID	Enter a string to indicate the Stream Filter Instance parameter is an index into the StreamFilterTable.
Stream ID	The Stream Handle Spec parameter contains a stream identifier specification value. A value of -1 denotes the wild card value; all positive values denote stream identifier values.
Stream Enable	Click to enable or disable (default) the stream function.
Priority Spec	Click the drop-down menu to specify a priority value (value: -1 denotes the wild card value; zero or positive values denote priority).

Item	Description
SGI ID	Enter a string to indicate the Stream Gate Instance parameter contains the index of an entry in the Stream Gate Table.
SDU Size	Enter a string to indicate the MaximumSDUSize parameter specifies the maximum allowed frame size for the stream. Any frame exceeding this value will be dropped. A value of 0 denote that the MaximumSDUSize filter is disabled for this stream.
FMI ID	Enter a string to indicate the FlowMeterInstanceID parameter of an entry in the Flow Meter Table. A value of -1 denotes that no flow meter is assigned; zero or positive values denote flow meter IDs.
FMI Enable	Click to enable or disable (default) the FMI function.
Oversize Block Enable	Click to enable or disable (default) the object to indicate whether the StreamBlockedDueToOversizeFrame function is enabled (TRUE) or disabled (FALSE).
Add New Entry	Click **Add New Entry** to add Stream Filter entry.
Save	Click **Save** to save changes.
Reset	Click **Reset** to undo any changes made locally and revert to previously saved values.

4.3.5.4.3 Stream Gate

This function allows you to inspect the current PSFP configurations, and possibly change them as well.

1. Navigate to **Configuration** > **TSN** > **PSFP** and click **Steam Gate**.
   The PSFP Stream Gate parameters Configuration page displays.

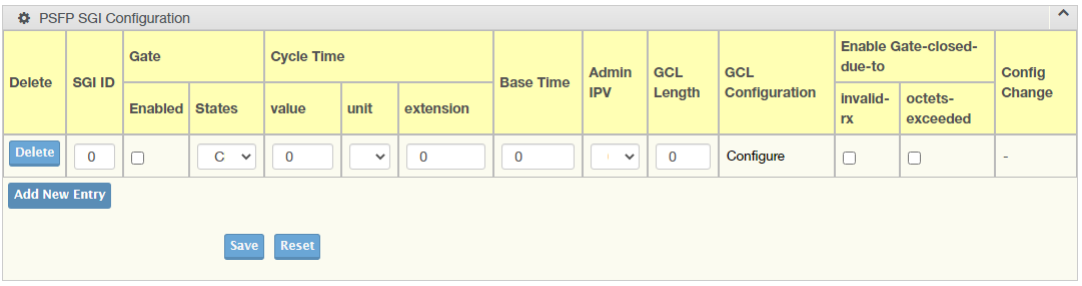


Figure 4.37 PSFP Stream Gate parameters Configuration

The following table describes the items in the PSFP Stream Gate parameters Configuration page.

Item	Description
Delete	Click **Delete** to remove the entry. It will be deleted during the next save.
SGI ID	Enter an string to indicate a parameter for the Stream Gate ID.
Gate Enabled	Click to enable or disable (default) the Gate Enabled parameter determines.
Gate States	Click the drop-down menu to select the administrative value of the GateStates parameter (options: open, closed).
Cycle Time Value	Enter an string to indicate the administrative value of the cycle time for the gate. The time may be specified in either milli seconds, micro seconds or nano seconds as defined by the field Cycle Time unit.
Cycle Time unit	Enter an string to indicate the unit used for specifying the administrative cycle time (values: ns, us or ms).
Cycle Time Extension	Enter an string to indicate the administrative value of the CycleTimeExtension parameter for the gate (value: unsigned integer number of nanoseconds).

Item	Description
Base Time	Enter an string to indicate the administrative value of the BaseTime parameter for the gate (value: a representation of a PTPtime value, consisting of decimal number of seconds since epoch). The time can be given with a resolution of nine decimals.
Admin IPV	Click the drop-down menu to select the administrative value of the IPV parameter for the gate. A value of -1 denotes the null value.
GCL Length	Enter an string to indicate the number of entries in the Gate Control List.
GCL Configuration	Displays the configuration of the Gate Control List.
Enable Gate-closed-due-to invalid-rx	Click to enable or disable (default) whether to close the gate if invalid data is received.
Enable Gate-closed-due-to octets-exceeded	Click to enable or disable (default) whether to close the gate if too many octets are received.
Config Change	The ConfigChange parameter signals the start of a configuration change for the gate when it is set to TRUE. This should only be done when the various administrative parameters are all set to appropriate values.
Add New Entry	Click **Add New Entry** to add Stream Gate entry.
Save	Click **Save** to save changes.
Reset	Click **Reset** to undo any changes made locally and revert to previously saved values.

4.3.5.5 FRER

This function allows you to inspect the current FRER configurations

1. Navigate to **Configuration** > **TSN** and click **FRER**
   The FRER Configuration Parameters page displays.

Figure 4.38 FRER Configuration Parameters

The following table describes the items in the FRER Configuration Parameters page.

Item	Description
Instance	Displays the instance of the identifier.
Mode	Displays the mode of operation: Generation or Recovery.
Enable	Displays the FRER instance status.
Ingress Streams	Enter a string to indicate the list of ingress stream IDs.
FRER VLAN	Displays the VLAN ID that ingress flows get classified to.
Egress Ports	Displays the port numbers that this FRER instance will hit.
Algorithm	Displays the algorithm used by Recovery function. Vector or match.
History Length	Displays the history length of vector algorithm.
Reset Timeout	Displays the reset timeout of Recovery function.
Take-no-sequence	If true, accept all frames whether they are R-tagged or not.
Individual	Displays the individual recovery status.
Terminate	Strip R-Tag from a frame before presenting it on egress.
Enable	Enable/disable Latent error detection.
Error Diff	Displays the latent error detection error difference.
Period	Displays the latent error detection period.

Item	Description
Paths	Displays the latent error detection paths.
Reset Period	Displays the latent error detection reset period.
Oper	Displays the operational state of FRER instance.
Warnings	Displays the operational warnings of FRER instance.
Latent Error	Displays any detected latent errors.
Configuration Buttons	Click to modify an entry. Options: ■ Edit: Edits the FRER instance. ■ Delete: Deletes the FRER instance. ■ Add: Adds new FRER instance.
Refresh	Click **Refresh** to refresh the page immediately.

4.3.6 PTP

This function allows you to configure and inspect the current PTP clock settings.

1. Navigate to **Configuration** and click **PTP**.
   The PTP Clock Configuration page displays.

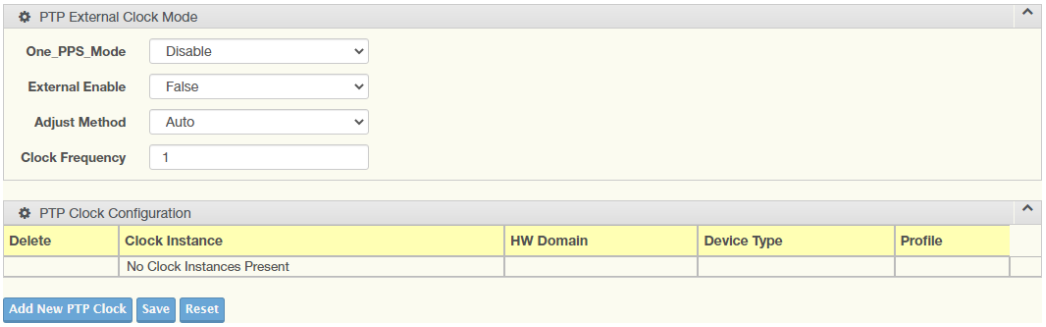


Figure 4.39 PTP Clock Configuration

The following table describes the items in the PTP Clock Configuration page.

Item	Description
One_PPS_Mode	Click the drop-down menu to select the One_pps_mode configuration. The following values are possible: ■ Output: Enable the 1 pps clock output ■ Input: Enable the 1 pps clock input ■ Disable: Disable the 1 pps clock in/out-put
External Enable	Click the drop-down menu to configure the External Clock output. The following values are possible: ■ True: Enable the external clock output ■ False: Disable the external clock output
Adjust Method	Click the drop-down menu to configure the Frequency adjustment configuration. ■ LTC: Select Local Time Counter (LTC) frequency control ■ Single: Select SyncE DPLL frequency control, if allowed by SyncE ■ Independent: Select an oscillator independent of SyncE for frequency control, if supported by the HW ■ Common: Select second DPLL for PTP, Both DPLL have the same (SyncE recovered) clock. ■ Auto: AUTO Select clock control, based on PTP profile and available HW resources.

Item	Description
Clock Frequency	Enter a string to indicate the Clock Frequency. The possible range of values are 1 - 25000000 (1 - 25MHz).

The following table describes the items in the PTP External Clock Configuration page.

Item	Description
Delete	Check this box and click on **Save** to delete the clock instance.
Clock Instance	Indicates the instance number of a particular Clock Instance [0..3]. Click on the **Clock Instance** number to edit the Clock details.
HW Domain	Indicates the HW clock domain used by the clock.
Device Type	Indicates the Type of the Clock Instance. There are five Device Types. 1. Ord-Bound - clock's Device Type is Ordinary-Boundary Clock. 2. P2p Transp - clock's Device Type is Peer to Peer Transparent Clock. 3. E2e Transp - clock's Device Type is End to End Transparent Clock. 4. Master Only - clock's Device Type is Master Only. 5. Slave Only - clock's Device Type is Slave Only.
Profile	Indicates the profile used by the clock.
Add New PTP Clock	Click **Add New PTP Clock** to create a new clock instance.
Save	Click **Save** to save changes.
Reset	Click **Reset** to reset the the page immediately.

4.3.7 NAT

4.3.7.1 SNAT (Source NAT)

Source NAT (SNAT) is the most common form of NAT. SNAT changes the source address of the packets passing through the switch. SNAT is typically used when an internal (private) host needs to initiate a session to an external (public) host. The device acting as an agent between the Internet (public) network and the local (private) network translates in real time the source destination IP address of a client on the network. For this reason, a source IP translation enables a single public address to represent a significantly larger number of private addresses.

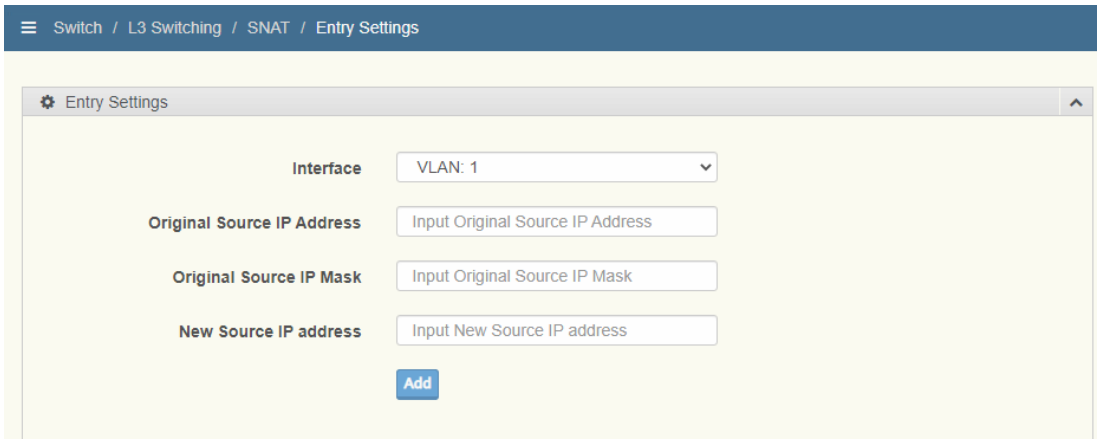


Figure 4.40 SNAT Entry Settings

The following table describes the items in the previous figure.

Item	Description
Interface	Click the drop-down menu to select the interface.
Original Source IP Address	Enter the original IP address to apply this rule. The address is the IP address to allow traffic to an external network.
Original Source IP Mask	Enter the IP netmask to specify the IP address to allow traffic to an external network.
New Source IP address	Enter the public IP address to configure the SNAT rule and specifies the external IP address for which outbound packets are translated.
Save	Click **Save** to save the values and update the screen.

Entry Information settings are informational only:

4.3.7.2 DNAT (Source NAT)

Destination NAT (DNAT) changes the destination address of packets passing through the switch. DNAT is typically used when an external (public) host needs to initiate a session with an internal (private) host.

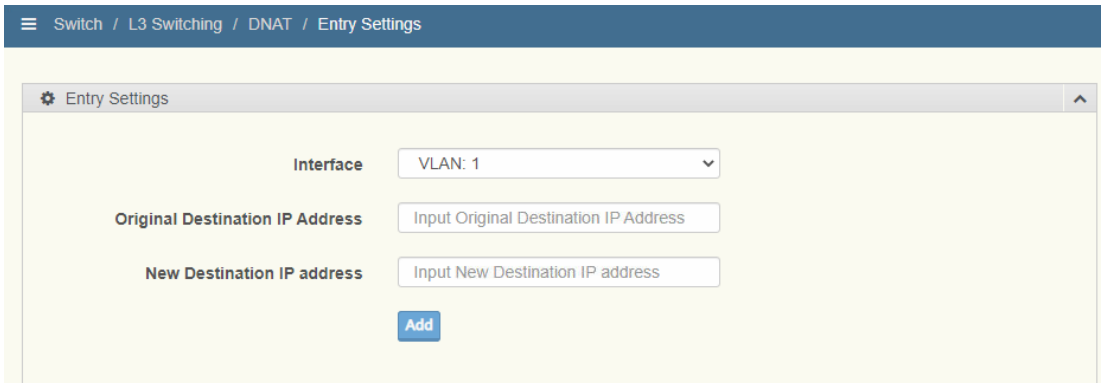


Figure 4.41 DNAT Entry Settings

The following table describes the items in the previous figure.

Item	Description
Interface	Click the drop-down menu to select the interface on which to apply the rule.
Original Destination IP Address	Enter the IP address to specify the public address to be translated. In the packet being inspected, this IP address is the one that appears as the destination IP address of the packet. The packet destination address is the one translated by this DNAT rule.
New Destination IP address	Enter the IP address to specify the destination address on inbound packets to be translated.
Add	Click Save to save the values and update the screen.

Entry Information are informational only as shown in the following:

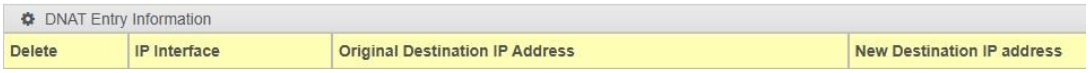


Figure 4.42 DNAT Entry Information

4.3.8 OSPF

Open Shortest Path First (OSPF) is a routing protocol used in IP networks. It employs a link-state routing (LSR) algorithm and belongs to the category of Interior Gateway Protocols (IGPs), operating within a single autonomous system (AS).

When deploying OSPF in a large network, the first step is to divide the network into logical areas. This helps reduce the number of routers exchanging Link State Advertisements (LSAs), improving scalability. Each OSPF interface is defined by assigning an IP interface on the switch to one of these areas. The OSPF interface then handles the sending and receiving of OSPF traffic with neighboring routers.

To further optimize OSPF traffic, you can configure area ranges that summarize multiple subnetwork addresses. This reduces the volume of routing information exchanged between Area Border Routers (ABRs). Additionally, for any OSPF area not directly connected to the backbone area, a virtual link must be established. Virtual links can also serve as redundant paths between areas, helping to prevent network partitioning or enabling backbone area expansion.

4.3.8.1 Global Configuration

This is OSPF router configuration table. It is a general group to configure the OSPF common router parameters.

Figure 4.43 OSPF Mode Configuration

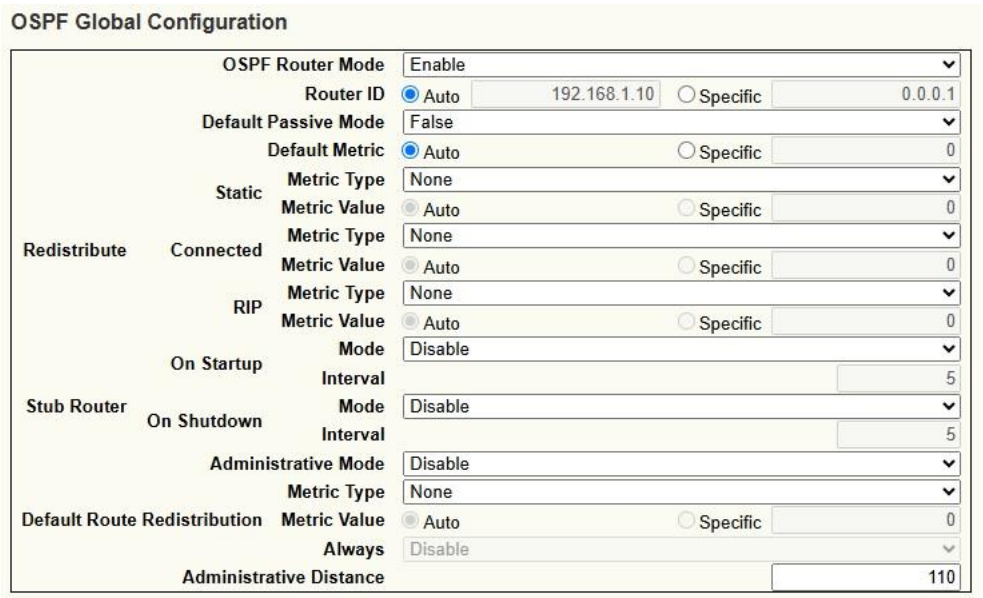


Figure 4.44 OSPF Global Configuration

Item	Description
OSPF Router Mode	Enable/Disable the OSPF router mode.
Router ID	The OSPF Router ID in IPv4 address format(A.B.C.D). When the router's OSPF Router ID is changed, if there is one or more fully adjacent neighbors in current OSPF area, the new router ID will take effect after restart OSPF process. Notice that the router ID should be unique in the Autonomous System and value '0.0.0.0' is invalid since it is reserved for the default algorithm. ■ Auto: The default algorithm will choose the largest IP address assigned to the router. ■ Specific: User specified router ID. The allowed range is from 0.0.0.1 to 255.255.255.254.
Default Passive Mode	Configure all interfaces as passive-interface by default.When an interface is configured as a passive-interface, the OSPF routing updates sending is suppressed, therefore the interface does not establish adjacencies (No OSPF Hellos). The subnet of all interfaces (both passive and active) is advertised by the OSPF router.
Default Metric	User specified default metric value for the OSPF routing protocol. The field is significant only when the arugment 'IsSpecificDefMetric' is TRUE. ■ Auto: The default metric is calculated automatically based on the routing protocols. ■ Specific: User specified default metric. The allowed range is 0 to 16777214.
Static Redistribute Metric Type	The OSPF redistributed metric type for the static routes. ■ None: The static routes are not redistributed. ■ External Type 1: External Type 1 of the static routes. ■ External Type 2: External Type 2 of the static routes.

Item	Description
Static Redistribute Metric Value	User specified metric value for the static routes. The field is significant only when the argument 'StaticRedistIsSpecificMetric' is TRUE. The allowed range is 0 to 16777214. ■ Auto: The redistributed metric is the same as the original metric value. ■ Specific: User specified metric for the static routes.
Connected Redistribute Metric Type	The OSPF redistributed metric type for the connected interfaces. ■ None: The connected interfaces are not redistributed. ■ External Type 1: External Type 1 of the connected interfaces routes. ■ External Type 2: External Type 2 of the connected interfaces routes.
Connected Redistribute Metric Value	User specified metric value for the connected interfaces. The field is significant only when the argument 'ConnectedRedistIsSpecificMetric' is TRUE. The allowed range is 0 to 16777214. ■ Auto: The redistributed metric is the same as the original metric value. ■ Specific: User specified metric for the connected routes.
RIP Redistribute Metric Type	The OSPF redistributed metric type for the RIP routes. The field is significant only when the RIP protocol is supported on the device. ■ None: The RIP routes are not redistributed. ■ External Type 1: External Type 1 of the RIP routes. ■ External Type 2: External Type 2 of the RIP routes.
RIP Redistribute Metric Value	User specified metric value for the RIP routes. The field is significant only when the RIP protocol is supported on the device and argument 'RipRedistIsSpecificMetric' is TRUE.. The allowed range is 0 to 16777214. ■ Auto: The redistributed metric is the same as the original metric value. ■ Specific: User specified metric for the RIP routes.
Stub router during startup period	Configures OSPF to advertise a maximum metric during startup for a configured period of time.
Stub router on startup interval time	User specified time interval (seconds) to advertise itself as stub area. The field is significant only when the on-startup mode is enabled.. The allowed range is 5 to 86400 seconds.
Stub router during shutdown period	Configures OSPF to advertise a maximum metric during shutdown for a configured period of time. The device advertises a maximum metric when the OSPF router mode is disabled and notice that the mechanism also works when the device reboots but not for the'reload default' case.
Stub router on shutdown interval time	User specified time interval (seconds) to wait till shutdown completed. The field is significant only when the on-shutdown mode is enabled.. The allowed range is 5 to 100 seconds.

Item	Description
Stub router administrative mode	Configures OSPF stub router mode administratively applied, for an indefinite period.
Default Route Redistribution Metric Type	The OSPF redistributed metric type for a default route. ■ None: The default route are not redistributed. ■ External Type 1: External Type 1 of the default route. ■ External Type 2: External Type 2 of the default route.
Default Route Redistribution Metric value	User specified metric value for a default route. The field is significant only when the argument 'DefaultRouteRedistIsSpecificMetric' is TRUE. The allowed range is 0 to 16777214. ■ Auto: The redistributed metric is the same as the original metric value. ■ Specific: User specified metric for the default route.
Default Route Redistribution Always	Specifies to always advertise a default route into all external-routing capable areas. Otherwise, the router only to advertise the default route when the advertising router already has a default route.
Administrative Distance	The OSPF administrative distance.

4.3.8.2 Network Area

The OSPF protocol limits the broadcast of messages—specifically Link State Advertisements (LSAs)—to defined areas in order to reduce their impact on network performance. Before assigning an Area ID to an OSPF interface, you must first define the Area ID in this table.

Each entry represents a logical group of OSPF routers that exchange LSAs to maintain a consistent view of the network topology. You can configure the area as one of the following:

- Normal Area: Allows both internal and external LSAs.
- Stub Area: Blocks external LSAs to reduce routing overhead.
- Not-So-Stubby Area (NSSA): Blocks external LSAs but can import external routes into the area.

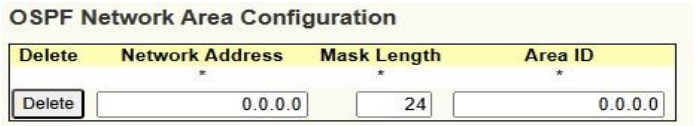


Figure 4.45 OSPF Network Area Configuration

Item	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Network Address	IPv4 network address.
Mask Length	IPv4 network mask length.
Area ID	The OSPF area ID.

4.3.8.3 Passive Interface

This is OSPF router interface configuration table.

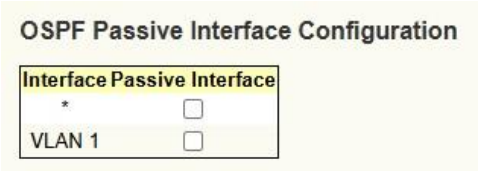


Figure 4.46 OSPF Passive Interface Configuration

Item	Description
Interface	Interface identification
Passive Interface	Enable the interface as OSPF passive-interface.

4.3.8.4 Stub Area

This is OSPF stub area configuration table. The configuration is used to reduce the link-state database size and therefore the memory and CPU requirement by forbidding some LSAs.

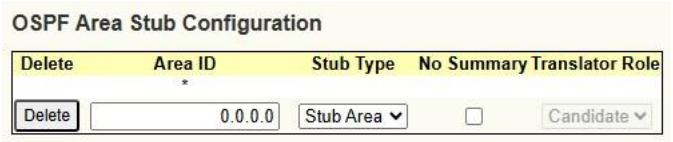


Figure 4.47 OSPF Area Stub Configuration

Item	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Area ID	The OSPF area ID.
Stub Type	The OSPF stub configured type. ■ Stub Area: Configure the area as stub area. ■ NSSA: Configure the area as not-so-stubby area (NSSA). ■
No Summary	The value is true to configure the inter-area routes do not inject into this stub area.
Translator Role	The OSPF NSSA translator role. ■ Candidate: this NSSA-ABR router will participate in the translator election. ■ Never: this NSSA-ABR router never translates. ■ Always: this NSSA-ABR router always translatates.

4.3.8.5 Area Authentication

This is OSPF area authentication configuration table. It is used to applied the authentication to all the interfaces belong to the area.

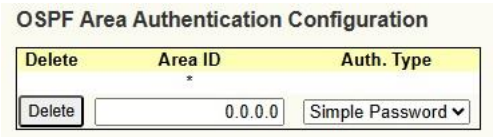


Figure 4.48 OSPF Area Authentication Configuration

Item	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Area ID	The OSPF area ID.
Auth. Type	The authentication type on an area is applied to all the interfaces belong to that area. The authentication type on an IP interface or a virtual link overrides the authentication type on an area and is useful if different interfaces in the same area use different authentication types. Specify the authenticaton type. ■ Simple Password: Simple password authentication. ■ Message Digest: MD5 digest authentication.

4.3.8.6 Area Range

This is OSPF area range configuration table. It is used to summarize the intra area paths from a specific address range in one summary-LSA(Type-3) and advertised to other areas or configure the address range status as 'DoNotAdvertise' which the summary-LSA(Type-3) is suppressed. The area range configuration is used for Area Border Routers (ABRs) and only router-LSAs(Type-1) and network-LSAs (Type-2) can be summarized. The AS-external-LSAs(Type-5) cannot be summarized because the scope is OSPF autonomous system (AS). The AS-external-LSAs(Type-7) cannot be summarized because the feature is not supported yet.

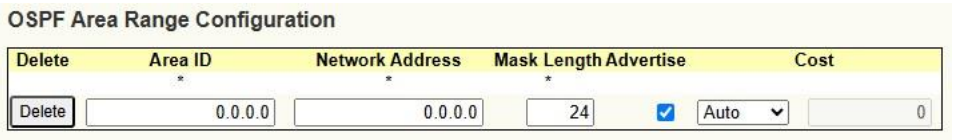


Figure 4.49 OSPF Area Range Configuration

Item	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Area ID	The OSPF area ID.
Network Address	IPv4 network address.

Item	Description
Mask Length	IPv4 network mask length.
Advertised	When the value is true, it summarizes intra area paths from the address range in one summary-LSA(Type-3) and advertised to other areas. Otherwise, the intra area paths from the address range are not advertised to other areas.
Auto/Specific	When 'Auto' is selected, the cost value is set to 0 automatically and isn't allowed to be configured.
Cost	User specified cost (or metric) for this summary route. It is allowed to be configured only when 'Specific' is selected. The allowed range is 0 to 16777215 and the default setting is 'auto cost' mode.

4.3.8.7 Interfaces

This is interface configuration parameter table.

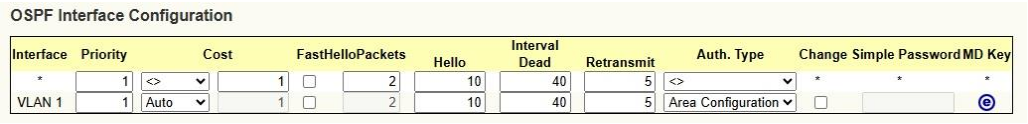


Figure 4.50 OSPF Interface Configuration

Item	Description
Interface	Interface identification.
Priority	User specified router priority for the interface. The allowed range is 0 to 255 and the default value is 1.
Cost	User specified cost for this interface. It's link state metric for the interface. The allowed range is 1 to 65535 and the default setting is 'auto cost' mode.
FastHelloPackets	How many Hello packets will be sent per second. The allowed range is 1 to 10.
Hello Interval	How many Hello packets will be sent per second. The allowed range is 1 to 65535
Dead Interval	The time interval (in seconds) between hello packets. The allowed range is 1 to 65535
Retransmit Interval	The time interval (in seconds) between link-state advertisement(LSA) retransmissions for adjacencies.
Auth. Type	The authentication type. ■ Simple Password: It's using a plain text authentication. A password must be configured, but the password can be read by sniffer the packets. ■ Message Digest: It's message-digest algorithm 5 (MD5) authentication. Keying material must also be configured. This is the most secure method. ■ Null Authentication: No authentication. ■ Area Configuration: Refer to Area authentication setting.
Change Simple Password	It is used to change the simple password (fill with plain text). The allowed input length is 1 to 8.
MD Key	Click the icon to edit the message digest key for the entry.

4.3.8.8 Virtual Link

All OSPF areas must be connected to the backbone area. If an area lacks a direct physical connection to the backbone, a virtual link can be configured to establish a logical path.

To connect an isolated area, the virtual link can traverse a single non-backbone area to reach the backbone. This requires specifying two endpoints:

- One on the Area Border Router (ABR) connecting the isolated area to the intermediate non-backbone area.
- The other on the ABR linking that same non-backbone area to the backbone.
- Note: Virtual links cannot be configured through stub or NSSA (Not-So-Stubby Area) areas.

Virtual links can also be used for redundancy, creating backup paths to the backbone to prevent network partitioning, or to logically merge two separated backbone areas.

To set up a virtual link, specify the transit area used for the connection and the router ID of the neighboring ABR.

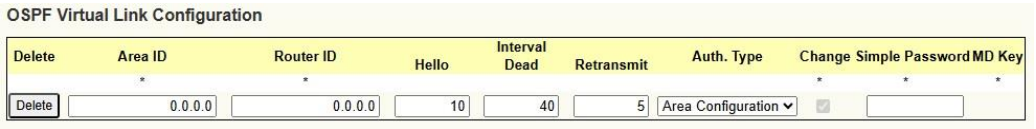


Figure 4.51 OSPF Virtual Link Configuration

Item	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Area ID	OSPF Area ID.
Router ID	OSPF router ID.
Hello Interval	How many Hello packets will be sent per second. The allowed range is 1 to 65535
Dead Interval	The time interval (in seconds) between hello packets. The allowed range is 1 to 65535
Retransmit Interval	The time interval (in seconds) between link-state advertisement(LSA) retransmissions for adjacencies. The allowed range is 3 to 65535
Auth. Type	The authentication type. ■ Simple Password: It's using a plain text authentication. A password must be configured, but the password can be read by sniffer the packets. Message Digest: It's message-digest algorithm 5 (MD5) authentication. Keying material must also be configured. This is the most secure method. ■ Null Authentication: No authentication. ■ Area Configuration: Refer to Area authentication setting.
Change Simple Password	It is used to change the simple password (fill with plain text). The allowed input length is 1 to 8.
MD Key	Click the icon to edit the message digest key for the entry.

4.3.9 Multicast

Multicast forwarding allows a single packet to be forwarded to multiple destinations. The service is based on L2 switch receiving a single packet addressed to a specific Multicast address. Multicast forwarding creates copies of the packet, and transmits the packets to the relevant ports.

4.3.9.1 IGMP Snooping

IGMP Snooping is defined as the process of listening to Internet Group Management Protocol (IGMP) network traffic. IGMP Snooping allows a network switch to listen in on the IGMP conversation between hosts and routers and maintain a map of which links need which IP multicast streams. Multicasts can be filtered from the links which do not need them in turn controlling which ports receive specific multicast traffic.

4.3.9.1.1 Profile Table

This page provides IPMC Profile related configurations. The IPMC profile is used to deploy the access control on IP multicast streams. It is allowed to create at maximum 64 Profiles with at maximum 128 corresponding rules for each.

Figure 4.52 IPMC Profile Configuration

Item	Description
Global Profile Mode	Enable/Disable the Global IPMC Profile. System starts to do filtering based on profile settings only when the global profile mode is enabled.
Delete	Check to delete the entry. The designated entry will be deleted during the next save
Profile Name	The name used for indexing the profile table. Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.
Profile Description	Additional description, which is composed of at maximum 64 alphabetic and numeric characters, about the profile. No blank or space characters are permitted as part of description. Use "_" or "-" to separate the description sentence.
Rule	When the profile is created, click the edit button to enter the rule setting page of the designated profile. Summary about the designated profile will be shown by clicking the view button. You can manage or inspect the rules of the designated profile by using the following buttons: : List the rules associated with the designated profile. : Adjust the rules associated with the designated profile.

4.3.9.1.2 Address Entry

This page provides address range settings used in IPMC profile.

The address entry is used to specify the address range that will be associated with IPMC Profile. It is allowed to create at maximum 128 address entries in the system.

Figure 4.53 IPMC Profile Address Configuration

Item	Description
Delete	Check to delete the entry. The designated entry will be deleted during the next save
Entry Name	The name used for indexing the address entry table. Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.
Start Address	The starting IPv4/IPv6 Multicast Group Address that will be used as an address range.
End Address	The ending IPv4/IPv6 Multicast Group Address that will be used as an address range.

4.3.9.1.3 IGMP Snooping

This page provides IGMP Snooping related configuration.

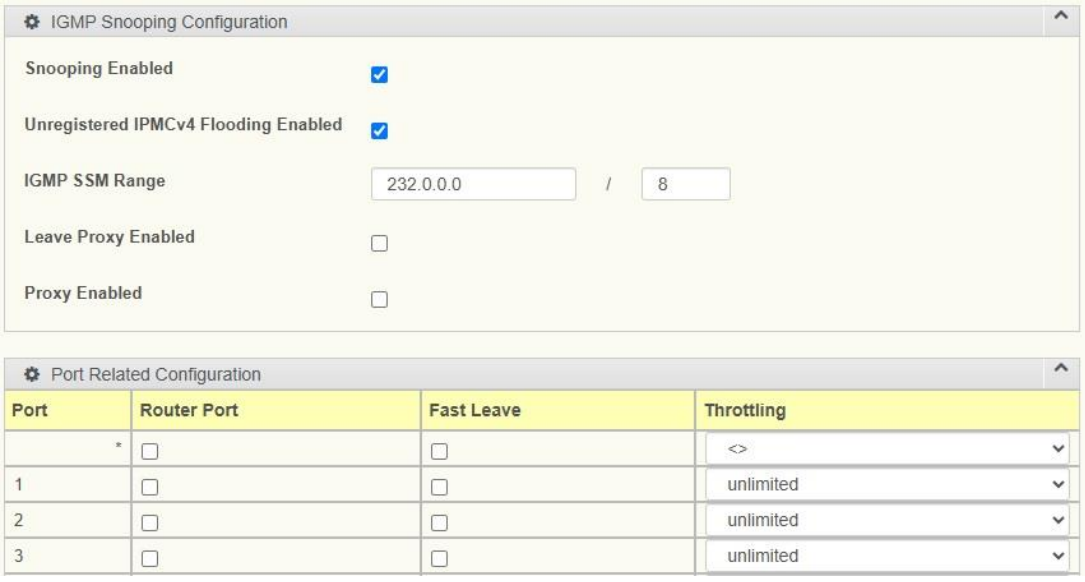


Figure 4.54 IGMP Snooping Configuration

Item	Description
Delete	Check to delete the entry. The designated entry will be deleted during the next save
Snooping Enabled	Enable the Global IGMP Snooping.
Unregistered IPMCv4 Flooding Enabled	Enable unregistered IPMCv4 traffic flooding. The flooding control takes effect only when IGMP Snooping is enabled. When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting.
IGMP SSM Range	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range. Assign valid IPv4 multicast address as prefix with a prefix length (from 4 to 32) for the range.
Leave Proxy Enabled	Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
Proxy Enabled	Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast Leave	Enable the fast leave on the port. System will remove group record and stop forwarding data upon receiving the IGMPv2 leave message without sending last member query messages. It is recommended to enable this feature only when a single IGMPv2 host is connected to the specific port.
Throttling	Enable to limit the number of multicast groups to which a switch port can belong.

4.3.9.1.4 MLD Snooping

This page provides MLD Snooping related configuration.

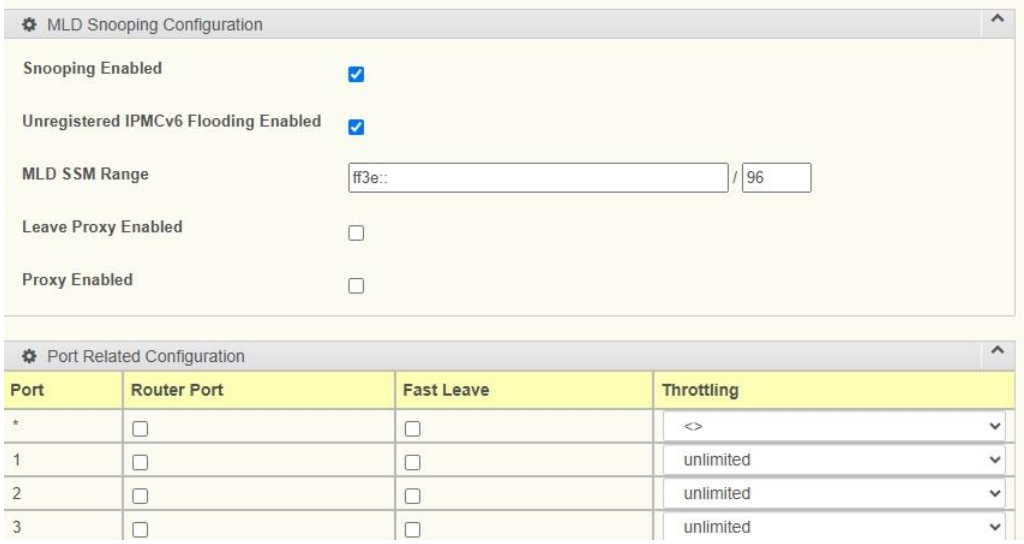


Figure 4.55 MLD Snooping Configuration

Item	Description
Snooping Enabled	Enable the Global MLD Snooping.
Unregistered IPMCv6 Flooding Enabled	Enable unregistered IPMCv6 traffic flooding. The flooding control takes effect only when MLD Snooping is enabled. When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.
MLD SSM Range	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range. Assign valid IPv6 multicast address as prefix with a prefix length (from 8 to 128) for the range.
Leave Proxy Enabled	Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
Proxy Enabled	Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier.If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast Leave	Enable the fast leave on the port. System will remove group record and stop forwarding data upon receiving the MLDv1 leave message without sending last member query messages.It is recommended to enable this feature only when a single MLDv1 host is connected to the specific port.
Throttling	Enable to limit the number of multicast groups to which a switch port can belong.

4.3.10 Link Aggregation

Link Aggregation is a method for combining multiple network connections in parallel in order to increase throughput beyond the capability of a single connection, and to provide redundancy in case one of the links should fail.

The device supports the following Aggregation links :

- Static LAGs (Port Trunk) – Force aggregared selected ports to be a trunk group.
- Link Aggregation Control Protocol (LACP) LAGs - LACP LAG negotiate Aggregated Port links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a LAG between them.

4.3.10.1 Static Aggregation

This page is used to configure the Aggregation hash mode. This mode applies to the whole network element

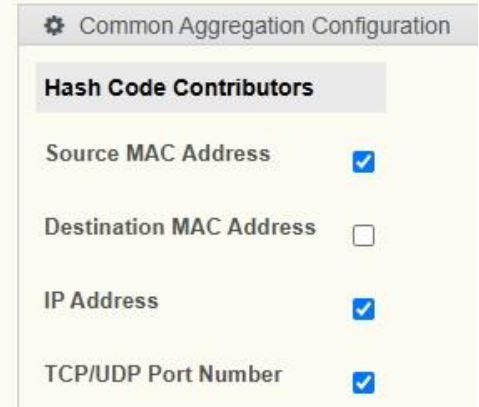


Figure 4.56 Common Aggregation Configuration

Item	Description
Source MAC Address	The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled.
Destination MAC Address	The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled.
IP Address	The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled.
TCP/UDP Port Number	The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled.

4.3.10.2 Static Aggregation Group Configuration

This page is used to configure the aggregation groups.

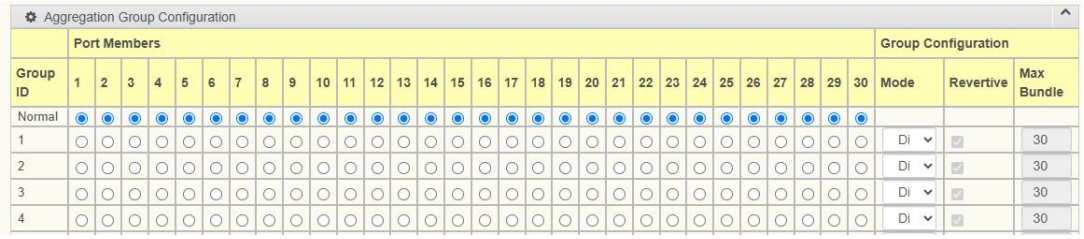


Figure 4.57 Common Aggregation Group Configuration

Item	Description
Group ID	Indicates the aggregation group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.
Port Members	Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.
Mode	This parameter determines the mode for the aggregation group. Disabled: The group is disabled. ■ Static: The group operates in static aggregation mode. ■ LACP (Active): The group operates in LACP active aggregation mode. See IEEE 801.AX-2014, section 6.4.1 for details. ■ LACP (Passive): The group operates in LACP passive aggregation mode. See IEEE 801.AX-2014, section 6.4.1 for details.
Revertive	This parameter only applies to LACP-enabled groups. It determines if the group will perform automatic link (re-)calculation when links with higher priority becomes available.
Max Bundle	This parameter only applies to LACP-enabled groups. It determines the maximum number of active bundled LACP ports allowed in an aggregation.

4.3.10.3 LACP Configuration

Link Aggregation Control Protocol (LACP) – LACP enables the negotiation of link aggregation (LAG) between ports on different devices. It allows switches to automatically detect and group ports that are part of the same LAG, ensuring proper aggregation and optimized bandwidth utilization.

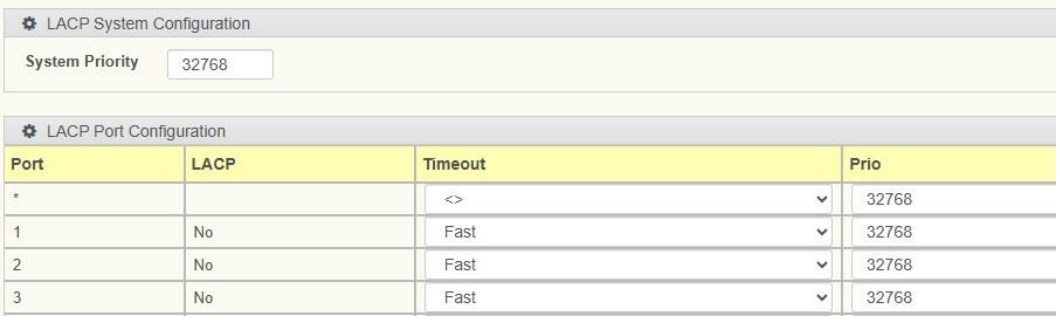


Figure 4.58 LACP Configuration

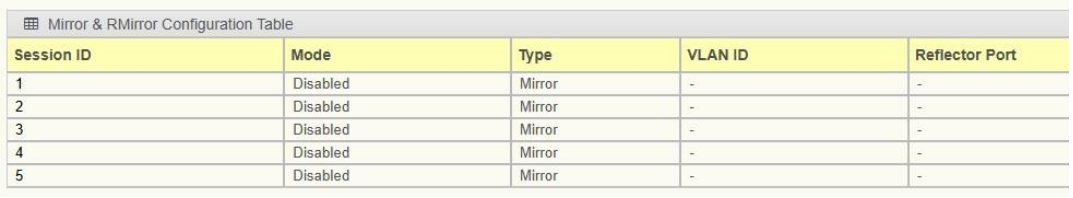
Item	Description
Port	The switch port number.
LACP	Show whether LACP is currently enabled on this switch port.
Timeout	The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.
Prio	The Prio controls the priority of the port, range 1-65535. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.

4.3.11 Port Mirror

Mirroring is a feature for switched port analyzer. The administrator can use the Mirroring to debug network problems. The selected traffic can be mirrored or copied on a destination port where a network analyzer can be attached to analyze the network traffic.

Remote Mirroring is an extend function of Mirroring. It can extend the destination port in other switch. So the administrator can analyze the network traffic on the other switches.

Select session ID to configure.



Session ID	Mode	Type	VLAN ID	Reflector Port
1	Disabled	Mirror	-	-
2	Disabled	Mirror	-	-
3	Disabled	Mirror	-	-
4	Disabled	Mirror	-	-
5	Disabled	Mirror	-	-

Figure 4.59 Mirror Configuration

Item	Description
Mode	To Enabled/Disabled the mirror or Remote Mirroring function.
Type	Select switch type.
Mirror	The switch is running on mirror mode. The source port(s) and destination port are located on this switch.
RMirror source	The switch is a source node for monitor flow. The source port(s), reflector port are located on this switch.
RMirror destination	The switch is an end node for monitor flow. The destination port(s) is located on this switch.

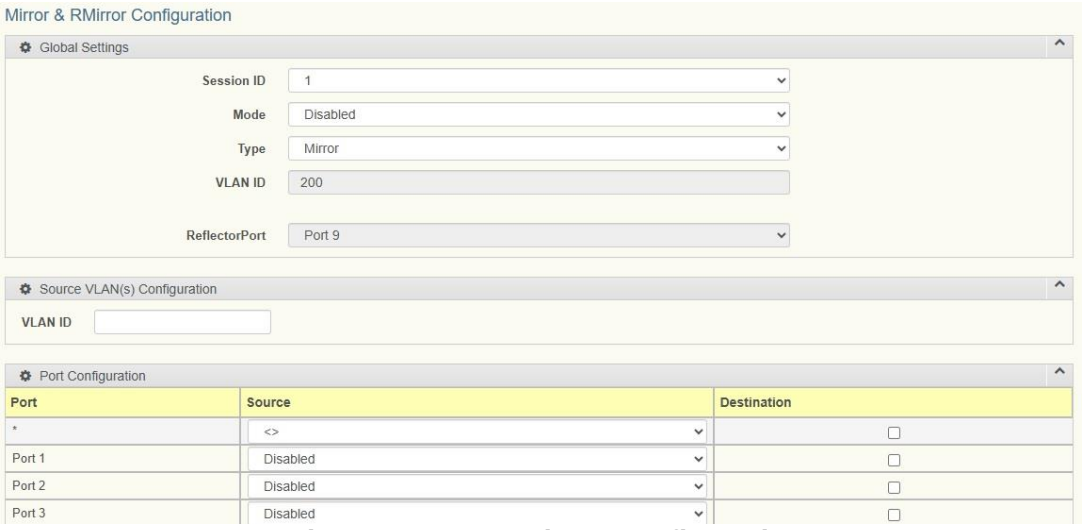


Figure 4.60 Port Mirror Configuration

Item	Description
VLAN ID	The VLAN ID points out where the monitor packet will copy to. The default VLAN ID is 200.
Reflector Port	The reflector port is a method to redirect the traffic to Remote Mirroring VLAN. Any device connected to a port set as a reflector port loses connectivity until the Remote Mirroring is disabled. In the stacking mode, you need to select switch ID to select the correct device. If you shut down a port, it cannot be a candidate for reflector port. If you shut down the port which is a reflector port, the remote mirror function cannot work. Note1: The reflector port needs to select only on Source switch type. Note2: The reflector port needs to disable MAC Table learning and STP. Note3: The reflector port only supports on pure copper ports.
Source VLAN(s) Configuration	The switch can supports VLAN-based Mirroring. If you want to monitor some VLANs on the switch, you can set the selected VLANs on this field. Note1: The Mirroring session shall have either ports or VLANs as sources, but not both.

Item	Description
Port	The logical port for the settings contained in the same row.
Source	Select mirror mode. ■ Disabled Neither frames transmitted nor frames received are mirrored. ■ Both Frames received and frames transmitted are mirrored on the Destination port. ■ Rx only Frames received on this port are mirrored on the Destination port. Frames transmitted are not mirrored. ■ Tx only Frames transmitted on this port are mirrored on the Destination port. Frames received are not mirrored.
Destination	Select destination port. This checkbox is designed for mirror or Remote Mirroring. The destination port is a switched port that you receive a copy of traffic from the source port. Note1: On mirror mode, the device only supports one destination port. Note2: The destination port needs to disable MAC Table learning.

4.3.12 Spanning Tree

The Spanning Tree Protocol (STP) is a network protocol to ensure loop-free topology for any bridged Ethernet local area network.

The EKI managed switch supports the following STP protocols:

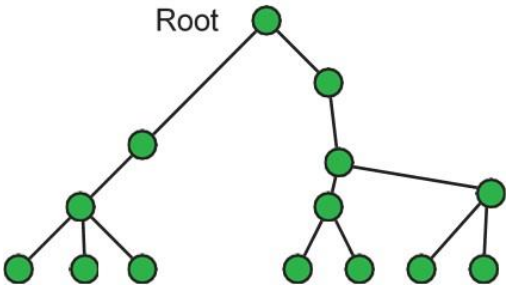
- STP (Spanning Tree Protocol): Establishes a single active path between network nodes and prevents loops by blocking redundant paths.
- RSTP (Rapid Spanning Tree Protocol): Enhances STP by providing faster convergence times and improved detection of network topology changes, while still preventing loops.
- MSTP (Multiple Spanning Tree Protocol): Extends RSTP functionality by supporting VLAN-based topology mapping. MSTP enables a separate spanning tree instance for each VLAN group, optimizing path usage and blocking redundant paths within each instance.

4.3.12.1 Rapid Spanning Tree Protocol (RSTP)

The network protocol Rapid Spanning Tree Protocol (RSTP: IEEE 802.1w) is an advancement over Spanning Tree Protocol (STP: IEEE802.1D) which promotes loop-free topology and high availability within Ethernet networks.

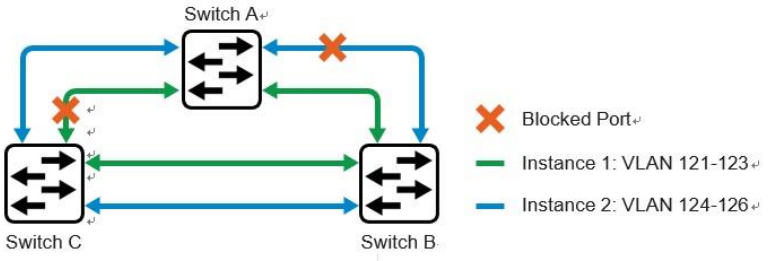
When compared to traditional daisy chain topology, RSTP networks offer high availability. In the event of network failure, devices can continue communicating as data is rerouted around the failure.

By using multiple switches, RSTP prevents network loops by blocking redundant paths on a network.



4.3.12.2 Multiple RSTP (MSTP)

Another form of redundancy in topologies that include redundancy is the use of Multiple Spanning Tree Protocol (MSTP). As an extension of RSTP, MSTP enables VLANs to be grouped into a spanning-tree instance. This provides multiple forwarding paths for data traffic, enabling load balancing.



4.3.12.3 STP Bridge Configuration

This page allows you to configure the Spanning Tree Protocol (STP) settings. These settings apply to all STP bridge instances on the switch.

Figure 4.61 STP Bridge Configuration - Basic

Basic Settings

Item	Description
Protocol Version	The MSTP / RSTP / STP protocol version setting.
Bridge Priority	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.
Hello Time	The interval between sending STP BPDU's. Valid values are in the range 1 to 10 seconds, default is 2 seconds. Note: Changing this parameter from the default value is not recommended, and may have adverse effects on your network.
Forward Delay	The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.
Max Age	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, *and* MaxAge must be <= (FwdDelay-1)*2.
Maximum Hop Count	This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.
Transmit Hold Count	The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.

Figure 4.62 STP Bridge Configuration – Advanced

Advanced Settings

Item	Description
Edge Port BPDU Filtering	Control whether a port explicitly configured as Edge will transmit and receive BPDUs.
Edge Port BPDU Guard	Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.
Port Error Recovery	Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.
Port Error Recovery Timeout	The time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

4.3.12.4 STP CIST Port Configuration

This page allows the user to inspect the current STP CIST port configurations, and possibly change them as well.

This page contains settings for physical and aggregated ports.

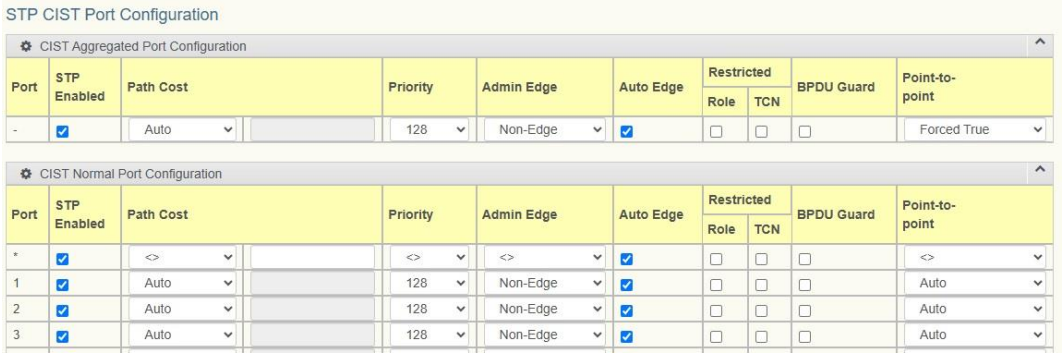


Figure 4.63 STP CIST Configuration

Item	Description
Port	The switch port number of the logical STP port.
STP Enabled	Controls whether STP is enabled on this switch port.
Path Cost	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above). Lower priority is better.
operEdge (state flag)	Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (having *operEdge* true) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. .
AdminEdge	Controls whether the *operEdge* flag should start as set or cleared. (The initial *operEdge* state when a port is initialized).
AutoEdge	Controls whether the bridge should enable automatic edge detection on the bridge port. This allows *operEdge* to be derived from whether BPDU's are received on the port or not.
Restricted Role	If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI , even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity.
Restricted TCN	If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information.
BPDU Guard	If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not effect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.
Point-to-Point	Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

4.3.13 Security

The Security function allows for the configuration of SSH, HTTPS, Port Security, , Access Control List(ACL) and AAA.

4.3.13.1 SSH

Secure Shell (SSH) is a protocol providing secure (encrypted) management connection to a remote device.

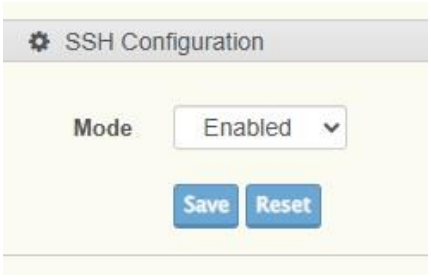


Figure 4.64 SSH Configuration

Item	Description
Mode	Indicates the SSH mode operation. Possible modes are: ■ Enabled: Enable SSH mode operation. ■ Disabled: Disable SSH mode operation

4.3.13.2 HTTPS

The HTTP page allows you to combine all kinds of AAA lists to the HTTP line. Attempts to access the switch's Web UI from HTTP are first authenticated.

Figure 4.65 HTTPS Configuration

Item	Description
Mode	Indicates the HTTPS mode operation. Possible modes are: ■ Enabled: Enable HTTPS mode operation. ■ Disabled: Disable HTTPS mode operation
Automatic Redirect	Indicate the HTTPS redirect mode operation. It is only significant when "HTTPS Mode Enabled" is selected. When the redirect mode is enabled, the HTTP connection will be redirected to HTTPS connection automatically. Notice that the browser may not allow the redirect operation due to the security consideration unless the switch certificate is trusted to the browser. You need to initialize the HTTPS connection manually for this case. Possible modes are: ■ Enabled: Enable HTTPS redirect mode operation. ■ Disabled: Disable HTTPS redirect mode operation.
Certificate Maintain	The operation of certificate maintenance. Possible operations are: ■ None: No operation. ■ Delete: Delete the current certificate. ■ Upload: Upload a certificate PEM file. Possible methods are: Web Browser or URL. ■ Generate: Generate a new self-signed RSA certificate.
Certificate Pass Phrase	Enter the pass phrase in this field if your uploading certificate is protected by a specific passphrase.
Certificate Upload	Upload a certificate PEM file into the switch. The file should contain the certificate and private key together. If you have two separated files for saving certificate and private key. Use the Linux cat command to combine them into a single PEM file. For example, cat my.cert my.key > my.pem Notice that the RSA certificate is recommended since most of the new version of browsers has removed support for DSA in certificate, e.g. Firefox v37 and Chrome v39. Possible methods are: ■ Web Browser: Upload a certificate via Web browser. ■ URL: Upload a certificate via URL, the supported protocols are HTTP, HTTPS, TFTP and FTP.
Certificate Status	Display the current status of certificate on the switch. Possible statuses are: Switch secure HTTP certificate is presented. Switch secure HTTP certificate is not presented. Switch secure HTTP certificate is generating ....

4.3.13.3 Port Security

The Port Security page allows you to configure port isolation behavior.

Port Security allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Port Security is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken depending on violation mode. The violation mode can be one of the four different described below.

The Port Security configuration consists of two sections, a global and a per-port.

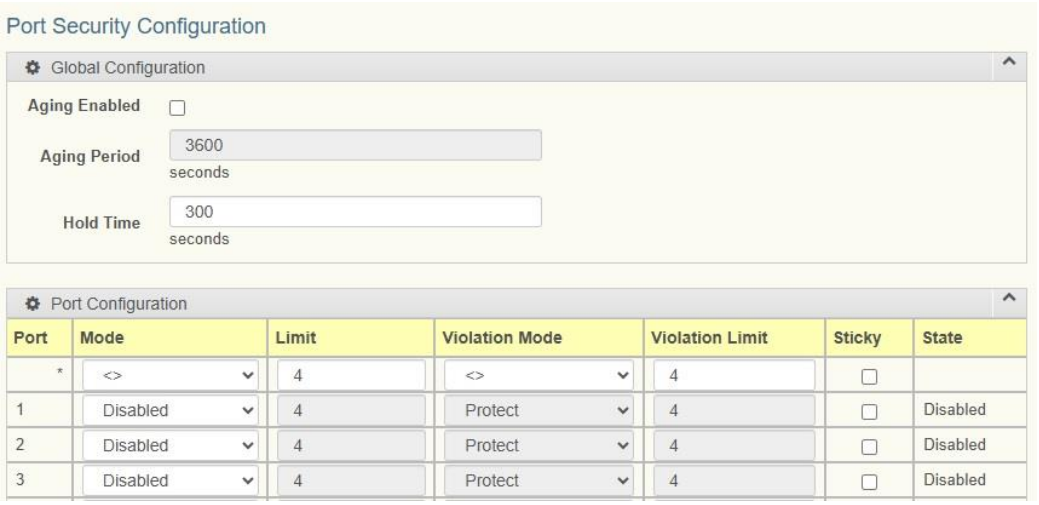


Figure 4.66 Port Security Configuration

Global Configuration

Item	Description
Aging Enabled	If checked, secured MAC addresses are subject to aging as discussed under Aging Period .
Aging Period	If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying functionality for securing MAC addresses, they may have other requirements to the aging period. The underlying functionality will use the shorter requested aging period of all modules that have aging enabled. The Aging Period can be set to a number between 10 and 10000000 seconds with a default of 3600 seconds.
Hold Time	The hold time - measured in seconds - is used to determine how long a MAC address is held in the MAC table if it has been found to violate the limit. Valid range is between 10 and 10000000 seconds with a default of 300 seconds. The reason for holding a violating MAC address in the MAC table is primarily to ensure that the same MAC address doesn't give rise to continuous notifications (if notifications on violation count is enabled).

Port Configuration

Item	Description
Port	The port number to which the configuration below applies.
Mode	Controls whether Port Security is enabled on this port. Notice that other modules may still use the underlying port security features without enabling Port Security on a given port.
Limit	The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1023. Default is 4. If the limit is exceeded, an action is taken corresponding to the violation mode.
Violation Mode	If Limit is reached, the switch can take one of the following actions: ■ Protect: Do not allow more than Limit MAC addresses on the port, but take no further action. ■ Restrict: If Limit is reached, subsequent MAC addresses on the port will be counted and marked as violating. Such MAC addreses are removed from the MAC table when the hold time expires. At most Violation Limit MAC addresses can be marked as violating at any given time. ■ Shutdown: If Limit is reached, one additional MAC address will cause the port to be shut down. This implies that all secured MAC addresses be removed from the port, and no new addresses be learned.
Violation Limit	The maximum number of MAC addresses that can be marked as violating on this port. This number cannot exceed 1023. Default is 4. It is only used when Violation Mode is Restrict.
Sticky	Enables sticky learning of MAC addresses on this port. When the port is in sticky mode, all MAC addresses that would otherwise have been learned as dynamic are learned as sticky. Sticky MAC addresses are part of the running-config and can therefore be saved to startup-config. Sticky MAC addresses survive link changes (in contrast to Dynamic, which will have to be learned again). They also survive reboots if running-config is saved to startup-config.
State	This column shows the current Port Security state of the port. The state takes one of four values: ■ Disabled: Port Security is disabled on the port. ■ Ready: The limit is not yet reached. This can be shown for all violation modes. ■ Limit Reached: Indicates that the limit is reached on this port. This can be shown for all violation modes. ■ Shutdown: Indicates that the port is shut down by Port Security. This state can only be shown if violation mode is set to Shutdown.

4.3.13.4 Access Control List (ACL)

ACL (Access Control List) is a table that defines access permissions through a set of rules known as ACEs (Access Control Entries). Each ACE specifies whether certain traffic—such as from a specific user, group, program, or process—is allowed or denied access to a network resource or service. Every traffic object that can be controlled contains a reference to an ACL, which defines its access rights. The configuration of ACLs can become complex, especially when ACEs are prioritized to handle multiple conditions.In networking, ACLs are typically used to manage access to network services or ports on a host or server. They define which devices are allowed or denied access to specific services. ACLs are commonly used to control inbound traffic and often function similarly to firewalls.

ACE (Access Control Entry) defines individual permission rules within an ACL. Each ACE is associated with a unique ID and specifies whether to permit or deny certain types of network traffic.

There are three ACE frame types:

- Ethernet Type
- ARP
- IPv4

Each ACE can be finely configured with a variety of parameters to support specific applications and use cases.

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 512 on each switch. Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed and the priority is highest.

Figure 4.67 Access Control List Configuration

Item	Description
ACE	Indicates the ACE ID.
Ingress Port	Indicates the ingress port of the ACE. Possible values are: ■ All: The ACE will match all ingress port. ■ Port: The ACE will match a specific ingress port.
Policy / Bitmask	Indicates the policy number and bitmask of the ACE.

Item	Description
Frame Type	Indicates the frame type of the ACE. Possible values are: ■ Any: The ACE will match any frame type. ■ EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. ■ ARP: The ACE will match ARP/RARP frames. ■ IPv4: The ACE will match all IPv4 frames. ■ IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol. ■ IPv4/UDP: The ACE will match IPv4 frames with UDP protocol. ■ IPv4/TCP: The ACE will match IPv4 frames with TCP protocol. ■ IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. ■ IPv6: The ACE will match all IPv6 standard frames.
Action	Indicates the forwarding action of the ACE. ■ Permit: Frames matching the ACE may be forwarded and learned. ■ Deny: Frames matching the ACE are dropped. ■ Filter: Frames matching the ACE are filtered.
Rate Limiter	Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.
Port Redirect	Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.
Mirror	Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are: ■ Enabled: Frames received on the port are mirrored. ■ Disabled: Frames received on the port are not mirrored. The default value is "Disabled".
Counter	The counter indicates the number of times the ACE was hit by a frame.
Modification Buttons	You can modify each ACE (Access Control Entry) in the table using the following buttons: : Inserts a new ACE before the current row. : Edits the ACE row. : Moves the ACE up the list. : Moves the ACE down the list. : Deletes the ACE. : The lowest plus sign adds a new entry at the bottom of the ACE listings.

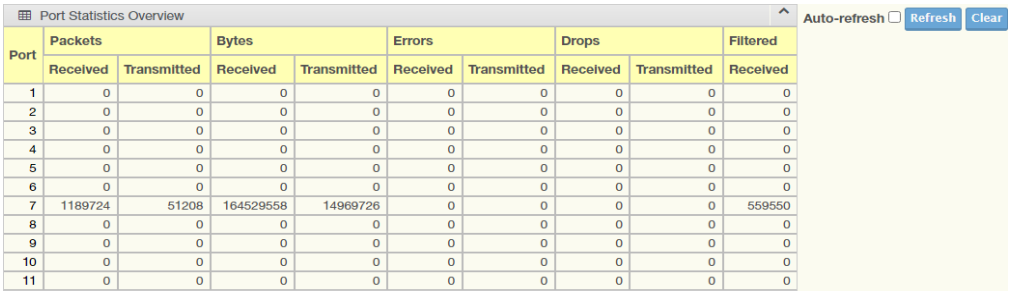
4.4 Monitor

4.4.1 Ports

4.4.1.1 Traffic Overview

This page provides an overview of general traffic statistics for all switch ports.

1. Navigate to **Monitor** > **Ports** and click **Traffic Overview**. The Port Statistics Overview page displays.



Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	1189724	51208	164529558	14969726	0	0	0	0	559550
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0

Figure 4.68 Port Statistics Overview

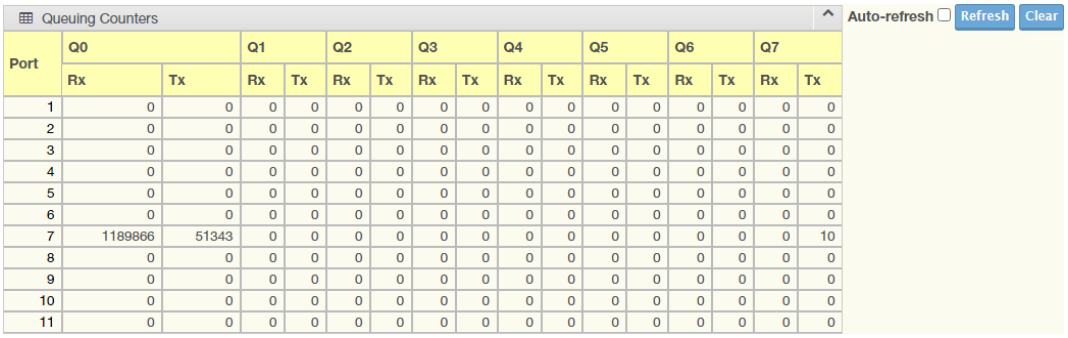
The following table describes the items in the Port Statistics Overview page.

Item	Description
Port	Displays the logical port for the entry.
Packets	Displays the number of received and transmitted packets per port.
Bytes	Displays the number of received and transmitted bytes per port.
Errors	Displays the number of frames received in error and the number of incomplete transmissions per port.
Drops	Displays the number of frames discarded due to ingress or egress congestion.
Filtered	Displays the number of received frames filtered by the forwarding process.
Auto-refresh	Click to enable or disable the automatic refresh function for the page. Automatic refresh occurs every 3 seconds.
Refresh	Click **Refresh** to refresh the page immediately.
Clear	Click **Clear** to clear the counters for all ports.

4.4.1.2 QoS Statistics

This page provides statistics for the different queues for all switch ports.

1. Navigate to **Monitor** > **Ports** and click **QoS Statistics**.
   The QoS Statistics page displays.



Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	1189866	51343	0	0	0	0	0	0	0	0	0	0	0	0	0	10
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 4.69 QoS Statistics

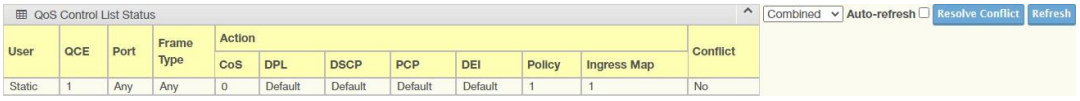
The following table describes the items in the QoS Statistics page.

Item	Description
Port	Displays the logical port for the settings contained in the same row.
Qn	Displays the QoS queues per port for listing. Q0 is the lowest priority queue.
Rx/Tx	Displays the number of received and transmitted packets per queue.
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click **Refresh** to refresh the page immediately.
Clear	Click **Clear** to clear the counters for all ports.

4.4.1.3 QCL Status

This page shows the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations.

1. Navigate to **Monitor** > **Ports** and click **QCL Status**.
   The QCL Status page displays.



User	QCE	Port	Frame Type	Action							Conflict
				CoS	DPL	DSCP	PCP	DEI	Policy	Ingress Map	
Static	1	Any	Any	0	Default	Default	Default	Default	1	1	No

Figure 4.70 QCL Status

The following table describes the items in the QCL Status page.

Item	Description
User	Displays the QCL user entry.

Item	Description
QCE	Displays the QCE identifier for the entry.
Port	Displays the port configured for the QCE entry.
Frame Type	Displays the type of frame. Values: ■ **Any:** Match any frame type. ■ **Ethernet:** Match EtherType frames. ■ **LLC:** Match (LLC) frames. ■ **SNAP:** Match (SNAP) frames. ■ **IPv4:** Match IPv4 frames. ■ **IPv6:** Match IPv6 frames.
Action	Displays the classification action taken on ingress frame if parameters configured are matched with the frame's content. Values: ■ **CoS:** Classify Class of Service. ■ **DPL:** Classify Drop Precedence Level. ■ **DSCP:** Classify DSCP value. ■ **PCP:** Classify PCP value. ■ **DEI:** Classify DEI value. ■ **Policy:** Classify ACL Policy number. ■ **Ingress Map:** Classify Ingress Map ID.
Conflict	Displays the conflict status of the QCL entry. Yes: if resources required to add a QCE may not be available. No: there are no conflicts.
Combined	Click the drop-down menu to select the QCL status. Options: ■ Combined ■ Static ■ Voice VLAN ■ Conflict
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Resolve Conflict	Click **Resolve Conflict** to release the resources required to add QCL entry, in case the conflict status for any QCL entry is **yes**.
Refresh	Click **Refresh** to refresh the page.

4.4.1.4 Detailed Statistics

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

1. Navigate to **Monitor** > **Ports** and click **Detailed Statistics**.

The Detailed Port Statistics page displays.

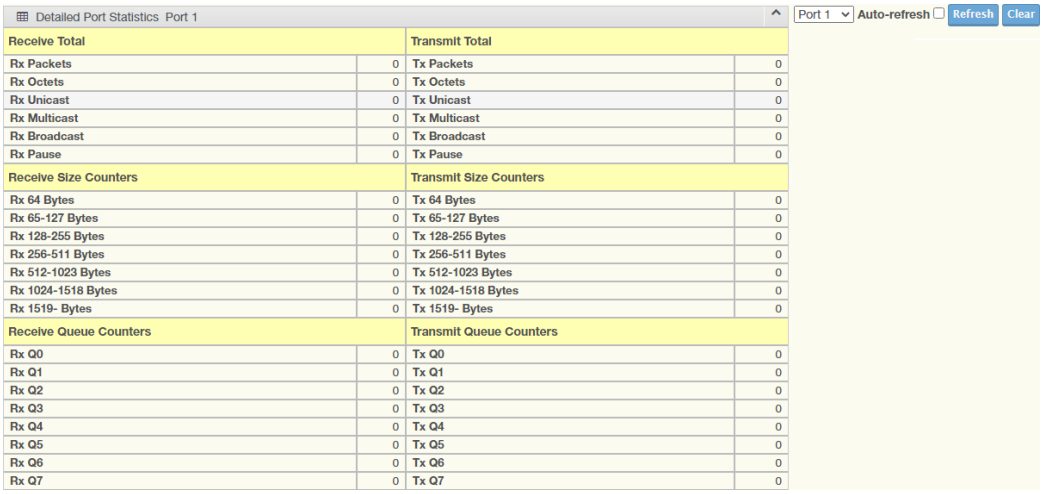


Figure 4.71 Detailed Port Statistics

The following table describes the items in the Detailed Port Statistics page.

Item	Description
Rx and Tx Packets	Displays the number of received and transmitted packets.
Rx and Tx Octets	Displays the number of received and transmitted bytes. Includes FCS, but excludes framing bits.
Rx and Tx Unicast	Displays the number of received and transmitted unicast packets.
Rx and Tx Multicast	Displays the number of received and transmitted multicast packets.
Rx and Tx Broadcast	Displays the number of received and transmitted broadcast packets.
Rx and Tx Pause	Displays the count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.
Receive and Transmit Size Counters	Displays the number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.
Receive and Transmit Queue Counters	Displays the number of received and transmitted packets per input and output queue.
Refresh	Click **Refresh** to refresh the page immediately.
Clear	Click **Clear** to clear the counters for the selected port.
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

The following table describes the items in the Receive and Transmist Error Counters table.

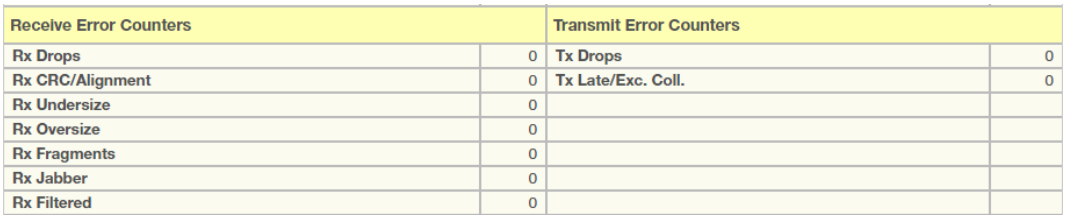


Figure 4.72 Receive and Transmit Error Counters Table

Item	Description
Rx Drops	Displays the number of frames dropped due to lack of receive buffers or egress congestion.
Rx CRC/Alignment	Displays the number of frames received with CRC or alignment errors.

Item	Description
Rx Undersize	Displays the number of short frames (longer than the configured maximum frame length for this port) received with valid CRC.
Rx Oversize	Displays the number of long frames (longer than the configured maximum frame length for this port) received with valid CRC.
Rx Fragments	Displays the number of short frames (smaller than 64 bytes) received with invalid CRC.
Rx Jabber	Displays the number of long frames received with invalid CRC.
Rx Filtered	Displays the number of received frames filtered by the forwarding process.
Tx Drops	Displays the number of frames dropped due to output buffer congestion.
Tx Late/Exc. Coll.	Displays the number of frames dropped due to excessive or late collisions.

The following table describes the items in the Receive and Transmist MM Counters table.

Receive MM Counters		Transmit MM Counters	
Rx MM Fragments	0	Tx MM Fragments	0
Rx MM Assembly Ok	0	Tx MM Hold	0
Rx MM Assembly Errors	0		
Rx MM SMD Errors	0		

Figure 4.73 Receive and Transmit MM Counters Table

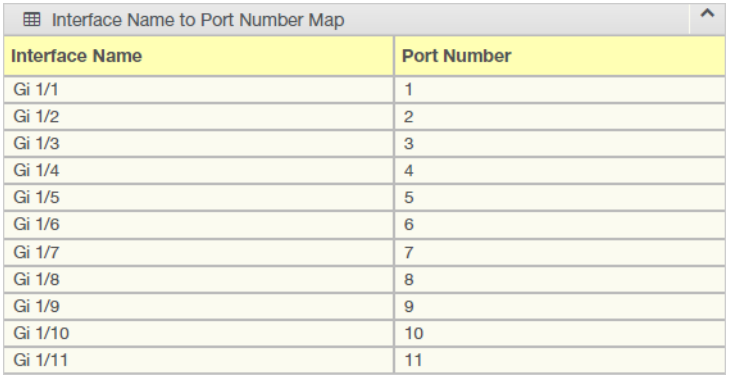
Item	Description
Rx MM Fragments	Displays the count of received MAC frame fragments.
Rx MM Assembly Ok	Displays the count of MAC frames that were successfully reassembled and delivered to MAC.
Rx MM Assembly Errors	Displays the count of MAC frames with reassembly errors. The counter is incremented when the ASSEMBLY_ERROR state of the Receive Processing State Diagram is entered.
Rx MM SMD Errors	Displays the count of received MAC frames / MAC frame fragments rejected due to unknown SMD value or arriving with an SMD-C when no frame is in progress. The counter is incremented each time the BAD_FRAG state of the Receive Processing State Diagram is entered.
Tx MM Fragments	Displays the count of transmitted MAC frame fragments.
Tx MM Hold	Displays the count of times MM_CTL.request(HOLD) primitive assertion caused preemption of a preemptable MAC frame.

4.4.1.5 Name Map

Many Web pages use a port number to express an interface, whereas CLI uses interface names. The table on this page provides a means to convert from one to the other.

1. Navigate to **Monitor** > **Ports** and click **Name Map**.

The Interface Name to Port Number Map page displays.



Interface Name to Port Number Map

Interface Name	Port Number
Gi 1/1	1
Gi 1/2	2
Gi 1/3	3
Gi 1/4	4
Gi 1/5	5
Gi 1/6	6
Gi 1/7	7
Gi 1/8	8
Gi 1/9	9
Gi 1/10	10
Gi 1/11	11

Figure 4.74 Interface Name to Port Number Map

The following table describes the items in the Interface Name to Port Number Map page.

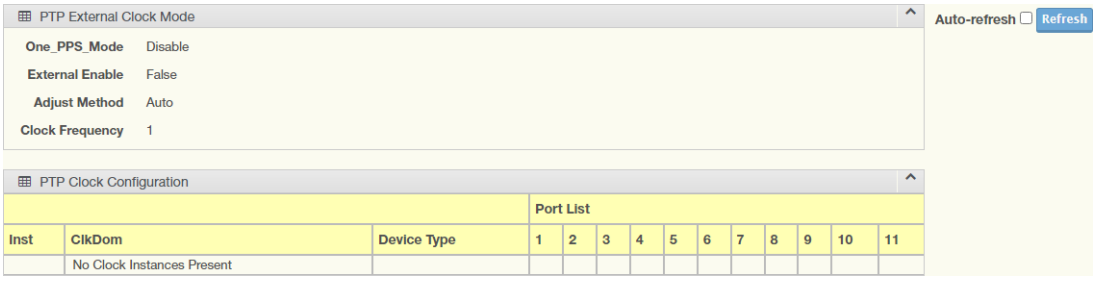
Item	Description
Interface Name	Displays the name of the interface entry.
Port Number	Displays the number identifying the port corresponding to the interface.

4.4.2 PTP

4.4.2.1 PTP

Many Web pages use a port number to express an interface, whereas CLI uses interface names. The table on this page provides a means to convert from one to the other.

1. Navigate to **Monitor** > **PTP** and click **PTP**.
   The PTP External Clock Mode page displays.



PTP External Clock Mode

One_PPS_Mode	Disable
External Enable	False
Adjust Method	Auto
Clock Frequency	1

Auto-refresh Refresh

PTP Clock Configuration

			Port List									
Inst	ClkDom	Device Type	1	2	3	4	5	6	7	8	9	10	11
	No Clock Instances Present												

Figure 4.75 PTP External Clock Mode

The following table describes the items in the PTP External Clock Mode page.

Item	Description
One_PPS_Mode	Displays the name of the interface entry.
External Enable	Displays the number identifying the port corresponding to the interface.

Item	Description
Adjust Method	Displays the current frequency adjustment configuration. Options: Shows the current Frequency adjustment configuration. ■ LTC: Use Local Time Counter (LTC) frequency control ■ Single: Use SyncE DPLL frequency control, if allowed by SyncE ■ Independent: Use an oscillator independent of SyncE for frequency control, if supported by the HW ■ Common: Use second DPLL for PTP, Both DPLL have the same (SyncE recovered) clock. ■ Auto: AUTO Select clock control, based on PTP profile and available HW resources.
Clock Frequency	Displays the current clock frequency (values: 1 to 25000000 [1 - 25MHz]).
PTP Clock Description	
Inst	Displays the instance of a clock instance for the entry.
ClkDom	Displays the clock domain for the instance entry.
Device Type	Displays the clock instance type: ■ Ord-Bound - Clock's Device Type is Ordinary-Boundary Clock. ■ P2p Transp - Clock's Device Type is Peer to Peer Transparent Clock. ■ E2e Transp - Clock's Device Type is End to End Transparent Clock. ■ Master Only - Clock's Device Type is Master Only. ■ Slave Only - Clock's Device Type is Slave Only.
Port List	Displays the port(s) configured for the instance.
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click **Refresh** to refresh the page immediately.

4.4.2.2 802.1AS Statistics

The function provides the means to inspect the current PTP configuration.

1. Navigate to **Monitor** > **PTP** and click **802.1AS Statistics**.
   The 802.1AS Clock Instance Specific Statistics page displays.

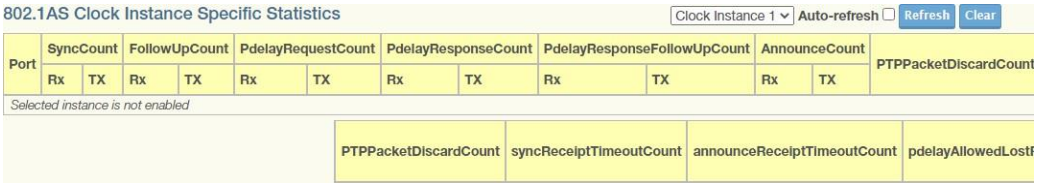


Figure 4.76 802.1AS Clock Instance Specific Statistics

Note! *The previous figure was distorted to accommodate the current layout.*

The following table describes the items in the 802.1AS Clock Instance Specific Statistics page.

Item	Description
Clock	Click to display the configured values.

Item	Description
Refresh	Click **Refresh** to refresh the page immediately.
Clear	Click to clear the statistics.
SyncCount	Displays the counter that increments every time synchronization information is transmitted.
FollowUpCount	Displays the counter that increments every time a Follow_Up message is transmitted.
PdelayRequestCount	Displays the counter that increments every time a Pdelay_Req message is transmitted.
PdelayResponse Count	Displays the counter that increments every time a Pdelay_Resp message is transmitted.
PdelayResponse FollowUpCount	Displays the counter that increments every time a Pdelay_Resp_Follow_Up message is transmitted.
AnnounceCount	Displays the counter that increments every time an Announce message is transmitted.

4.4.3 VLANs

4.4.3.1 Membership

The function provides an overview of membership status of VLAN users.

1. Navigate to **Monitor** > **VLANs** and click **Membership**.
   The VLAN Membership Status page displays.

Figure 4.77 VLAN Membership Status

The following table describes the items in the VLAN Membership Status page.

Item	Description
Start from VLAN	
First Page	Click the icon to display the first page.
Next Page	Click the icon to display the next page in the list.
VLAN ID	Displays the VLAN ID for the port entry.
Port Members	Displays the status of the port: ■ Included in a VLAN ■ Forbidden ■ Forbidden and attempted included in VLAN A row of check boxes for each port is displayed for each VLAN ID.
Select Users	Click the drop-down menu to select the VLAN users. Options: ■ Admin ■ NAS ■ GVRP ■ MVR ■ RMirror
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click **Refresh** to refresh the page immediately.

4.4.3.2 Ports

The function provides an overview of the VLAN port status.

1. Navigate to **Monitor** > **VLANs** and click **Ports**.
   The VLAN Port Status for Combined users page displays.

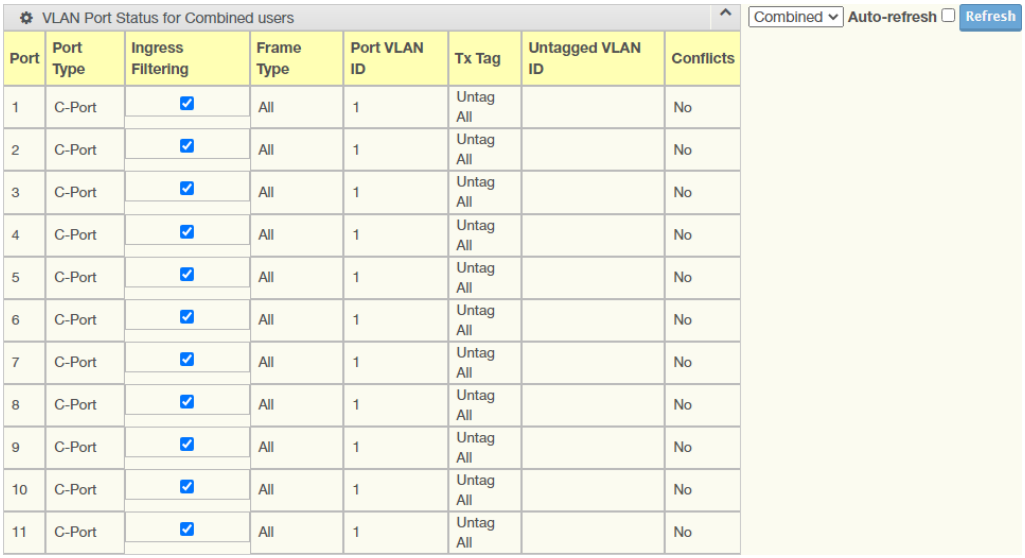


Figure 4.78 VLAN Membership Status

The following table describes the items in the VLAN Port Status for Combined users page.

Item	Description
Port	Displays the port settings of the entry.
Port Type	Displays the port type as configured by a user. Values: ■ Unaware ■ C-Port ■ S-Port ■ S-Custom-Port
Ingress Filtering	Displays if ingress filtering is enabled or disabled for the entry.
Frame Type	Displays the acceptable frame type as configured by a user. Values: ■ All ■ Taged ■ Untagged
Port VLAN ID	Displays the port VLAN ID as configured for the entry.
Tx Tag	Displays the TX Tag requirements as configured for the entry. Values: ■ Tag All ■ Tag PVID ■ Tag UVID ■ Untag All ■ Untag PVID ■ Untag UVID
Untagged VLAN ID	Displays whether Tx Tag is overridden and set to Tag or Untag UVID. The field is empty if not overridden by the selected user.
Conflicts	Displays whether a port conflict exists (Yes).

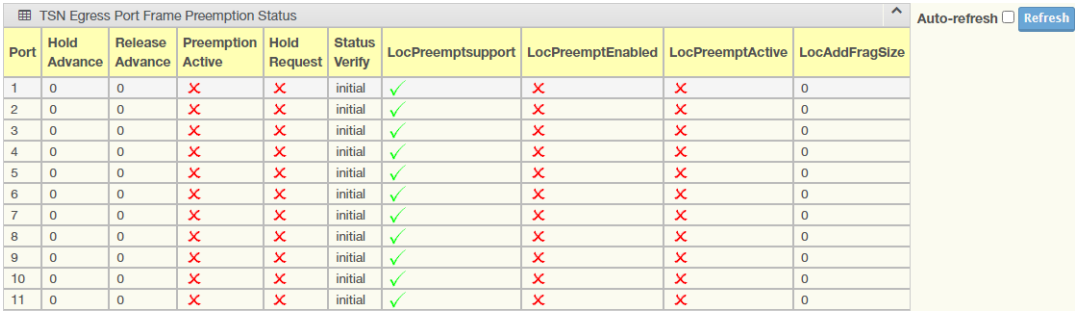
Item	Description
Select Users	Click the drop-down menu to select the VLAN users. Options: ■ Admin ■ NAS ■ GVRP ■ MVR ■ MSTP ■ ERPS ■ VCL ■ RMirror
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click **Refresh** to refresh the page immediately.

4.4.4 TSN

4.4.4.1 Frame Preemption

The function provides an overview of TSN egress port frame preemption status.

1. Navigate to **Monitor** > **TSN** and click **Frame Preemption**.
   The TSN Egress Port Frame Preemption Status page displays.



Port	Hold Advance	Release Advance	Preemption Active	Hold Request	Status Verify	LocPreemptsupport	LocPreemptEnabled	LocPreemptActive	LocAddFragSize
1	0	0	✕	✕	initial	✓	✕	✕	0
2	0	0	✕	✕	initial	✓	✕	✕	0
3	0	0	✕	✕	initial	✓	✕	✕	0
4	0	0	✕	✕	initial	✓	✕	✕	0
5	0	0	✕	✕	initial	✓	✕	✕	0
6	0	0	✕	✕	initial	✓	✕	✕	0
7	0	0	✕	✕	initial	✓	✕	✕	0
8	0	0	✕	✕	initial	✓	✕	✕	0
9	0	0	✕	✕	initial	✓	✕	✕	0
10	0	0	✕	✕	initial	✓	✕	✕	0
11	0	0	✕	✕	initial	✓	✕	✕	0

Figure 4.79 TSN Egress Port Frame Preemption Status

The following table describes the items in the TSN Egress Port Frame Preemption Status page.

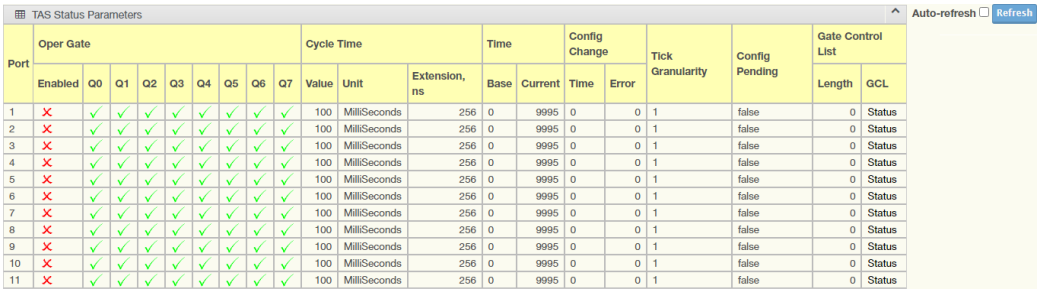
Item	Description
Port	Displays the logical port of the entry.
Hold Advance	Displays the value of the holdAdvance parameter for the Port in nanoseconds.
Release Advance	Displays the value of the releaseAdvance parameter for the Port in nanoseconds.
Preemption Active	Displays the value is active (TRUE) when preemption is operationally active for the Port, and idle (FALSE) otherwise.
Hold Request	Displays the value is hold (TRUE) when the sequence of gate operations for the Port has executed a Set-And-Hold-MAC operation, and release (FALSE) when the sequence of gate operations has executed a Set-And-Release-MAC operation.
Status Verify	Displays the status of the MAC Merge sublayer verification for the given device.
LocPreemptsupport	Displays the value is TRUE when preemption is supported on the port, and FALSE otherwise.

Item	Description
LocPreemptEnabled	Displays the value is TRUE when preemption is enabled on the port, and FALSE otherwise.
LocPreemptActive	Displays the value is TRUE when preemption is operationally active on the port, and FALSE otherwise.
LocAddFragSize	Displays the value of the 802.3br LocAddFragSize parameter for the port.
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click **Refresh** to refresh the page immediately.

4.4.4.2 TAS

The function provides an overview of TSN egress port frame preemption status.

1. Navigate to **Monitor** > **TSN** and click **TAS**.
   The TAS Status Parameters page displays.



Port	Oper Gate									Cycle Time			Time		Config Change		Tick Granularity	Config Pending	Gate Control List	
	Enabled	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Value	Unit	Extension, ns	Base	Current	Time	Error			Length	GCL
1	✕	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	9995	0	0	1	false	0	Status
2	✕	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	9995	0	0	1	false	0	Status
3	✕	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	9995	0	0	1	false	0	Status
4	✕	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	9995	0	0	1	false	0	Status
5	✕	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	9995	0	0	1	false	0	Status
6	✕	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	9995	0	0	1	false	0	Status
7	✕	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	9995	0	0	1	false	0	Status
8	✕	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	9995	0	0	1	false	0	Status
9	✕	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	9995	0	0	1	false	0	Status
10	✕	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	9995	0	0	1	false	0	Status
11	✕	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	9995	0	0	1	false	0	Status

Figure 4.80 TAS Status Parameters

The following table describes the items in the TAS Status Parameters page.

Item	Description
Port	Displays the logical port of the entry.
Oper Gate Enabled	Displays the whether traffic scheduling is active (true) or inactive (false).
Oper Gate States	Displays the current state of the gate associated with each queue for the Port.
Cycle Time Value	Displays the operational value of the gating cycle for the Port.
Cycle Time Unit	Displays the operational Cycle Time unit.
Cycle Time Extension	Displays the integer number of nanoseconds, defining the maximum amount of time by which the gating cycle for the Port is permitted to be extended when a new cycle configuration is installed.
Base Time	Displays the operational value of base time, expressed as an IEEE 1588 precision time protocol (PTP) timescale.
Current Time	Displays the current time (seconds), in PTPtime, as maintained by the local system. The value is a representation of a PTPtime value, consisting of a 48-bit integer number of seconds and a 32-bit integer number of nanoseconds.
Config Change Time	Displays the PTPtime at which the next config change is scheduled to occur.
Config Change Error	Displays the counter of the number of times that a re-configuration of the traffic schedule has been requested with the old schedule still running and the requested base time was in the past.
Tick Granularity	Displays the granularity of the cycle time clock, represented as an unsigned number of tenths of nanoseconds.

Item	Description
Config Pending	Displays the value of the ConfigPending state machine variable.
GCL Length	Displays the operational value of the gate control list length parameter for the Port.
GCL	Displays the link to the GCL parameter status.
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click **Refresh** to refresh the page immediately.

4.4.4.3 PSFP

Global Parameters

The function provides an overview of the current PSFP configurations.

Navigate to **Monitor** > **TSN** > **PSFP** and click **Global Parameters**.

The PSFP Stream Parameter Status page displays.

Figure 4.81 PSFP Stream Parameter Status

The following table describes the items in the PSFP Stream Parameter Status page.

Item	Description
Max Stream Filter Instances	Displays the maximum number of stream filter instances that are supported by this Bridge component.
Max Stream Gate Instances	Displays the maximum number of stream gate instances that are supported by this Bridge component.
Max Flow Meter Instances	Displays the maximum number of flow meter instances that are supported by this Bridge component.
Supported List Max	Displays the maximum value supported by this Bridge component of the AdminControlListLength and OperControlListLength parameters.
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click **Refresh** to refresh the page immediately.

Stream Filter Status

The function provides an overview of the current PSFP configurations.

Navigate to **Monitor** > **TSN** > **PSFP** and click **Stream Filter Status**.

The TPSFP Stream Filter Status page displays.

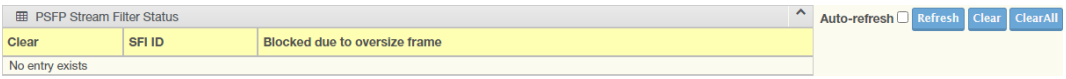


Figure 4.82 PSFP Stream Filter Status

The following table describes the items in the PSFP Stream Filter Status page.

Item	Description
Clear	Click to clear the entry for the next Clear operation.
SFI ID	Displays the stream filter instance ID.

Item	Description
Blocked Due to Oversize Frame	Displays if the filter is blocked due to oversize frame.
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click **Refresh** to refresh the page immediately.
Clear	Click **Clear** to clear the counters for the selected port.
Clear All	Click **Clear All** to clear the blocked flags for all entries.

Stream Filter Statistics

The function provides an overview of the current PSFP configurations.

Navigate to **Monitor** > **TSN** > **PSFP** and click **Stream Filter Statistics**.

The PSFP Stream Filter Statistics page displays.

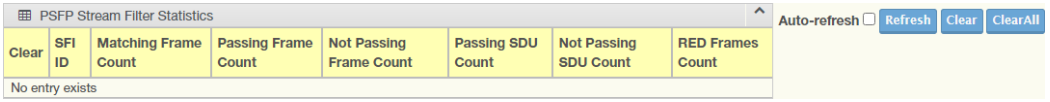


Figure 4.83 PSFP Stream Filter Statistics

The following table describes the items in the PSFP Stream Filter Statistics page.

Item	Description
Clear	Click to clear the entry for the next Clear operation.
SFI ID	Displays the maximum number of stream filter instances that are supported by this Bridge component.
Matching Frame Count	Displays the counts received frames that match this stream filter.
Passing Frame Count	Displays the counts received frames that pass the gate associated with this stream filter
Not Passing Frame Count	Displays the counts received frames that do not pass the gate associated with this stream filter.
Passing SDU Count	Displays the counts received frames that pass the SDU size filter specification associated with this stream filter.
Not Passing SDU Count	Displays the counts received frames that do not pass the SDU size filter specification associated with this stream filter.
RED Frames Count	Displays the counts received random early detection (RED) frames associated with this stream filter.
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click **Refresh** to refresh the page immediately.
Clear	Click **Clear** to clear the counters for the selected port.
Clear All	Click **Clear All** to clear the blocked flags for all entries.

Stream Gate Status

The function provides an overview of the current PSFP configurations.

Navigate to **Monitor** > **TSN** > **PSFP** and click **Stream Gate Status**.

The PSFP SGI Status page displays.

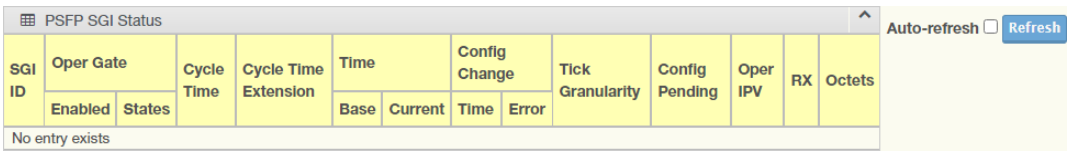


Figure 4.84 PSFP SGI Status

The following table describes the items in the PSFP SGI Status page.

Item	Description
SGI ID	Displays the instance parameter.
Oper Gate Enabled	Displays the active (true) / inactive (false) state of the parameter.
Oper Gate States	Displays the operational value indicating an open or closed gate.
Cycle Time Numerator	Displays the operational numerator value indicating the cycle time as a rational number of seconds. The numerator and denominator together represent the cycle time as a rational number.
Cycle Time Denominator	Displays the operational denominator value indicating the cycle time as a rational number of seconds. The numerator and denominator together represent the cycle time as a rational number.
Cycle Time Extension	Displays the operational value of the CycleTimeExtension parameter in nanoseconds.
Base Time	Displays the operational value of the BaseTime paramter. The value is a representation of a PTPtime value, consisting of a 48-bit integer number of seconds and a 32-bit integer number of nanoseconds.
Current Time	Displays the current time, in PTPtime, as maintained by the local system.
Config Change Time	Displays the PTPtime at which the next config change is scheduled to occur.
Config Change Error	Displays the number of times that a re-configuration of the traffic schedule has been requested with the old schedule still running and the requested base time was in the past.
Tick Granularity	Displays the granularity of the cycle time clock, represented as an unsigned number of tenths of nanoseconds.
Config Pending	Displays the value of the ConfigPending state machine variable.
Oper IPV	Displays the operational value of the IPV parameter.
GCL Length	Displays the operational value of the ListMax parameter.
GCL Status	Displays the link to the GCL parameter status.
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click **Refresh** to refresh the page immediately.

4.4.4.4 FRER

FRER Status

The function provides an overview of the current FRER status.

Navigate to **Monitor** > **TSN** > **FRER** and click **FRER Status**.

The FRER Status page displays.

Figure 4.85 FRER Status

The following table describes the items in the FRER Status page.

Item	Description
Instance	Displays the FRER instance.
Oper	Displays the operational state. ■ Green: active ■ Red: disabled or internal error detected.

Item	Description
Warning	Displays any operation warnings. ■ Off: no warning detected ■ Yellow: warnings detected, use tooltip for further details.
Latent Error	Displays any latent errors ■ Green: no error detected ■ Red: latent errors detected
Statistics	Click to reset the statistics counter.
Reset Function	Click to reset the function. If this FRER instance is in generation mode, this is used to reset the sequence number of the sequence generator. If this FRER instance is in recovery mode, this is used to reset the recovery function. It resets both possible individual recovery functions and the compound recovery functions.
Reset Latent Error	Click to clear a sticky latent error.
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click **Refresh** to refresh the page immediately.
Clear All	Click **Clear All** to clear the blocked flags for all entries.

FRER Statistics

The function provides an overview of the current FRER statistics counters.

Navigate to **Monitor** > **TSN** > **FRER** and click **FRER Statistics**.

The FRER Statistics page displays.

Figure 4.86 FRER Statistics

The following table describes the items in the FRER Statistics page.

Item	Description
Clear	Click to mark an entry for clearance during the following Clear operation.
Instance	Displays the FRER instance ID.
Mode	Displays the operation mode (Generation or Recovery).
Egress Port	Displays the list of egress port numbers.
Ingress Stream	Displays the list of ingress stream IDs.
Out of Order	Displays the out of order counters.
Roque	Displays the receiving roque counters.
Passed	Displays the receiving passed counters.
Discarded	Displays the Receiving discarded counters.
Lost	Displays the receiving lost counters.
Tagless	Displays the receiving tagless counters.
Recovery Reset	Displays the receiving reset counters.
Latent Error Reset	Displays the receiving latent error counters.
Generation Reset	Displays the generation reset counters.
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click **Refresh** to refresh the page immediately.
Clear	Click **Clear** to clear the counters for the selected port.

4.5 Maintenance

4.5.1 Restart Device

The function allows for the restart of the device. After a restart, the switch boots normally.

1. Navigate to **Maintenance** and click **Restart Device**.
   The Restart Device page displays.
2. Click **Yes** to reboot the switch. Any configuration changes you have made since the last time you issued a save will be lost.
   Click **No** to cancel the reboot.

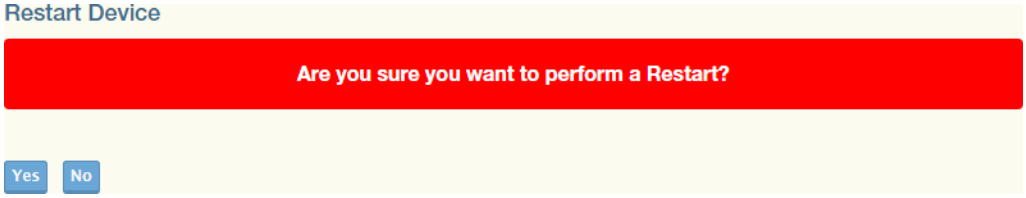


Figure 4.87 Restart Device

4.5.2 Factory Defaults

The function allows for the rest of the device to its factory default configuration.

1. Navigate to **Maintenance** and click **Restart Device**.
   The Factory Defaults page displays.
2. Click **Yes** to reset the device to it's original factory defaults. All changes that have been made will be lost, even if you have issued a save.
   Reset settings take effect after a system reboot.
   Click **No** to cancel the reboot.

Figure 4.88 Factory Defaults

4.5.3 Software

4.5.3.1 Upload

The function allows for the updating of the firmware controlling the switch.

1. Navigate to **Maintenance** > **Software** and click **Upload**.
   The Software Upload page displays.
2. Click **Select File...** to browse for a software image and select it.

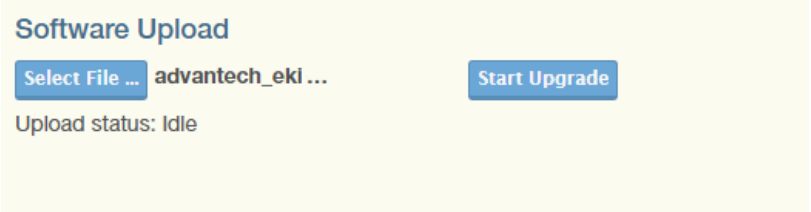


Figure 4.89 Software Upload

After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and the switch restarts.

Warning! *While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. Do not restart or power off the device at this time or the switch may fail to function afterwards.*

4.5.3.2 Image Select

The page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image.

1. Navigate to **Maintenance** > **Software** and click **Image Select**.
   The Software Image Selection page displays.

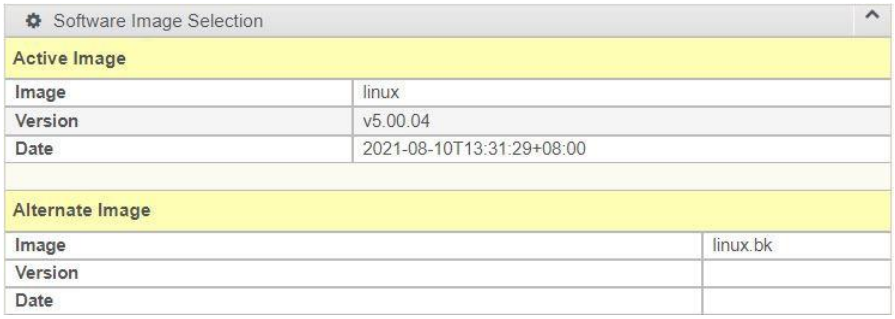


Figure 4.90 Firmware Selection

The following table describes the items in the Software Image Selection page.

Item	Description
Image	Displays the name of the firmware image since its last update.
Version	Displays the version of the firmware image.
Date	Displays the production date of the firmware.
Active Alternative Image	Click **Activate Alternative Image** to use the alternate image. This button may be disabled depending on system state.
Cancel	Click **Cancel** to discontinue activating the backup image. Returns to the previous page.

4.5.4 Configuration

4.5.4.1 Save startup-config

Note! The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

3. The page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image.
    1. Navigate to **Maintenance** > **Configuration** and click **Save startup-config**.
       The Save Running Configuration to startup-config page displays.
    2. Click **Save Configuration** to FLASH the configuration changes to be saved across a system reboot. All changes submitted since the previous save or system reboot will be retained by the switch.

Figure 4.91 Save Running Configuration to Startup-config

4.5.4.2 Download Configuration

The function allows you to download any of the files on the device to a browser.

1. Navigate to **Maintenance** > **Configuration** and click **Download**.
   The Download Configuration page displays.
2. Click a listed file name to select it.
3. Click **Download Configuration** to start the download.

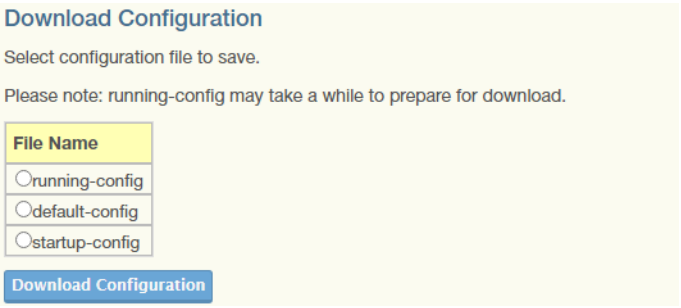


Figure 4.92 Download Configuration

Download of running-config may require time to complete, as the file must be prepared for download.

4.5.4.3 Upload Configuration

The function allows you to upload a file to the device with the exception of the default-config file as it is read-only.

1. Navigate to **Maintenance** > **Configuration** and click **Upload**.
   The Upload Configuration page displays.
2. Click **Choose File** to select a source file.
3. Select the destination file on the File Name (target) column.
4. If the destination is the running-config, the upload applies to the configuration in one of two methods:
   – Replace mode: The current configuration is fully replaced with the configuration in the uploaded file.
   – Merge mode: The uploaded file is merged into running-config.

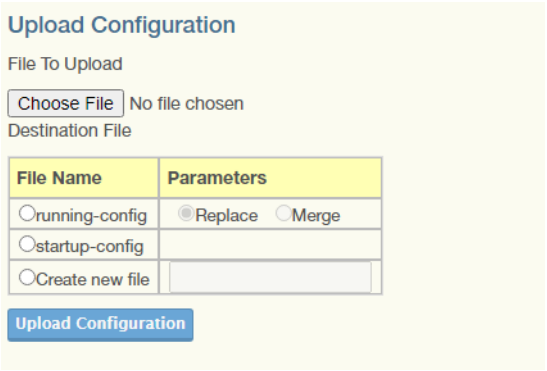


Figure 4.93 Upload Configuration

If the flash file system is full (i.e. contains default-config and 32 other files, usually including startup-config), it is not possible to create new files. Instead an existing file must be overwritten or another file must be deleted.

4.5.4.4 Activate Configuration

The function allows you select a configuration file to activate.

1. Navigate to **Maintenance** > **Configuration** and click **Activate**.
   The Activate Configuration page displays.
2. Click a file from the File Name table to select and activate.
3. Click **Activate Configuration** to start the process.

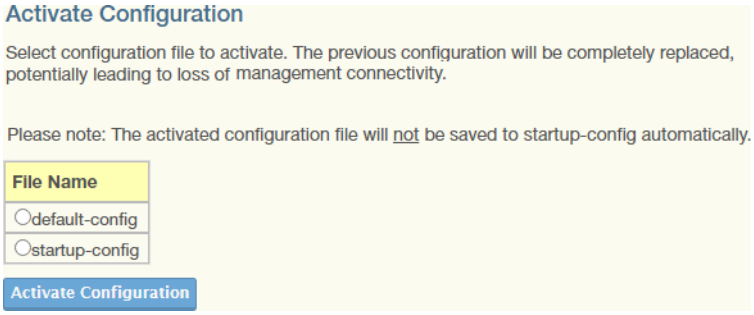


Figure 4.94 Activate Configuration

4.5.4.5 Delete Configuration File

The function allows you select a configuration file to delete.

1. Navigate to **Maintenance** > **Configuration** and click **Delete**.
   The Delete Configuration File page displays.
2. Click a file from the File Name table to select and delete.
3. Click **Delete Configuration file** to start the process.

Chapter 5

Troubleshooting

5.1 Troubleshooting

- Verify that the device is using the right power cord/adapter (DC 48V); please do not use a power adapter with DC output higher than 48V, or the device may be damaged.
- Select the proper UTP/STP cable to construct the user network. Use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable for RJ-45 connections that depend on the connector type the switch equipped: 100R Category 3, 4 or 5 cable for 10Mbps connections, 100R Category 5 cable for 100Mbps connections, or 100R Category 5e/above cable for 1000Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).

  R = replacement letter for Ohm symbol.
- **Diagnosing LED Indicators:** To assist in identifying problems, the switch can be easily monitored through panel indicators, which describe common problems the user may encounter, so the user can be guided towards possible solutions.
- If the power indicator does not light on when the power cord is plugged in, you may have a problem with power cord. Check for loose power connections, power losses, or surges, at the power outlet. If you still cannot resolve the problem, contact a local dealer for assistance.
- If the LED indicators are normal and the connected cables are correct but packets still cannot be transmitted, please check the user system's Ethernet device configuration or status.

ADVANTECH

Enabling an Intelligent Planet

www.advantech.com

Please verify specifications before quoting. This guide is intended for reference purposes only.