Networking & Communication

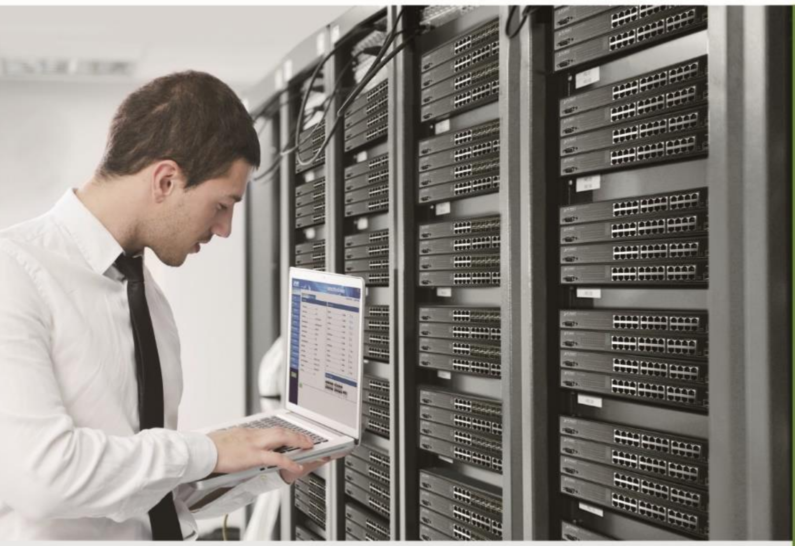
User's Manual

Industrial L2+ Managed TSN Ethernet Switch

► TSN-5225-4T/TSN-5225-4T2S

Industrial Managed TSN Media Converter

► TSN-900-2T2S



www.PLANET.com.tw

Trademarks

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose. PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

FCC Warning

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.

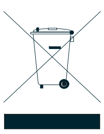
CE Mark Warning

This device is compliant with Class A of CISPR 32. In a residential environment this equipment may cause radio interference.

Energy Saving Note of the Device

This power required device does not support Standby mode operation. For energy savings, please remove the power cable to disconnect the device from the power circuit. Without removing the power cable, the device will still consume power from the power source. In view of Saving the Energy and reducing the unnecessary power consumption, it is strongly suggested to remove the power cable from the device if this device is not intended to be active.

WEEE Warning



To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Revision

User's Manual of PLANET Industrial Managed TSN Device

FOR MODELS: TSN-5225 series and TSN-900-2T2S

REVISION: 1.0 (August, 2024)

Part No: EM-TSN-5225 series_TSN-900-2T2S_v1.0

TABLE OF CONTENTS

1. INTRODUCTION

Thank you for purchasing PLANET TSN-5225-4T or TSN-5225-4T2S Industrial L2+ Managed TSN Ethernet Switch and TSN-900-2T2S Industrial Managed TSN Media Converter. The descriptions of these models are as follows:

TSN-5225-4T	Industrial L2+ 4-Port 10/100/1000T Managed TSN Ethernet Switch
TSN-5225-4T2S	Industrial L2+ 4-Port 10/100/1000T + 2-Port 1G/2.5G SFP Managed TSN Ethernet Switch
TSN-900-2T2S	Industrial 2-Port 10/100/1000T + 2-Port 1G/2.5G SFP Managed TSN Media Converter

"**Industrial Managed TSN Device"** is used as an alternative name in this user's manual. **Industrial Managed TSN Device** comes with multiple Gigabit Ethernet copper ports and SFP fiber optic connectibility, and robust Layer 2+ features in an IP30 rugged metal case.

1.1 Packet Contents

Open the box of the **Industrial Managed TSN Device** and carefully unpack it. The box should contain the following items:

Model Name / Item	TSN-5225-4T	TSN-5225-4T2S	TSN-900-2T2S
Industrial Managed TSN Device	■	■	■
Quick Installation Guide Sheet	■	■	■
DB9 to RJ45 Interface RS232 Console Cable	■	■	■
Wall Mounting Kit	■	■	■
DIN-rail Kit	■	■	■
RJ45 Dust Caps	5	5	3
SFP Dust Caps	-	2	2

If any of these are missing or damaged, please contact your dealer immediately.

1.2 Product Description

Innovative Industrial Managed TSN Device Guarantees Delivery of Time-Sensitive Data

PLANET TSN-5225-4T, TSN-5225-4T2S and TSN-900-2T2S are brand-new Industrial-grade **Time-Sensitive Networking (TSN)** Managed Ethernet Switches and Media Converter. The TSN-5225-4T features **4 10/100/1000BASE-T RJ45 ports**, and the TSN-5225-4T2S comes with **4 10/100/1000BASE-T RJ45 ports** and **2 1G/2.5GBASE-X SFP ports**. The TSN-900-2T2S, with **2 10/100/1000BASE-T RJ45 ports** and **2 1G/2.5GBASE-X SFP ports**, features a rugged IP30 metal case for stable operation in harsh environments and supports all levels of the industrial automation network, from the field bus to the factory backbone. It guarantees end-to-end transmission of high-priority traffic with extremely low latency. With **2 dual-speed SFP fiber slots** the

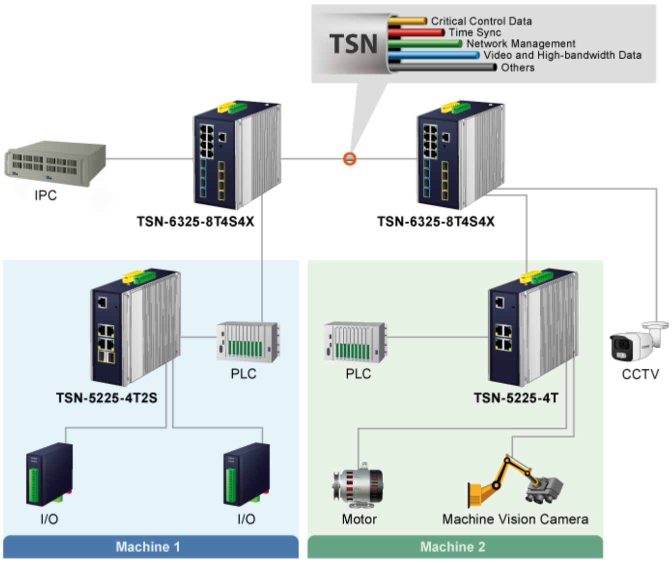
TSN-5225-4T2S and TSN-900-2T2S can flexibly extend the connection distance.

The **Industrial Managed TSN Device** can be installed in any difficult environment as it can operate stably under the temperature range from **-40** to **75 degrees C**. It also allows either DIN-rail or wall mounting for efficient use of cabinet space.

A Simplified Pathway to a TSN-compatible Infrastructure

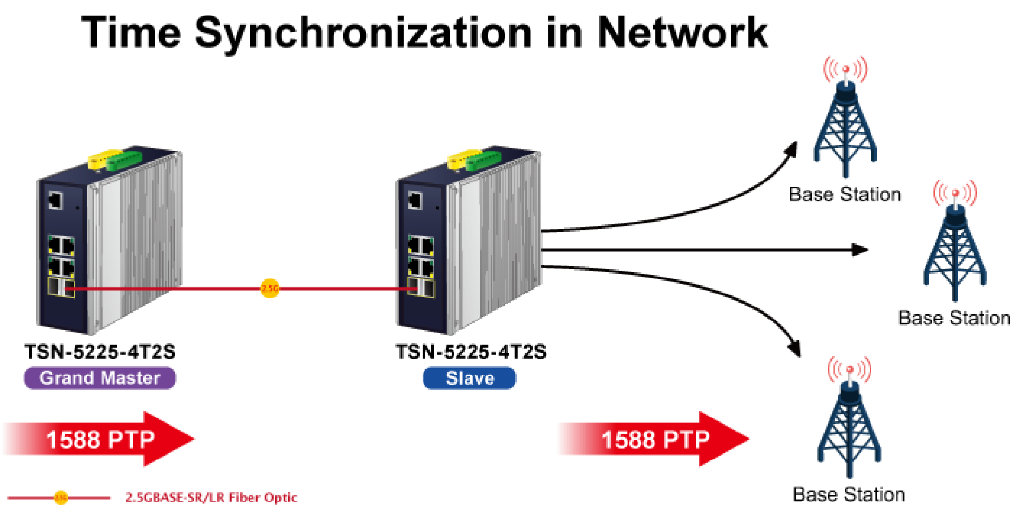
PLANET **Industrial Managed TSN Device** provides real-time, low-latency network communication for industrial automation, 5G NR networks, Industry 4.0, 4K/8K video streaming, and VR/AR gaming industry by using the **Time-sensitive Networking (TSN)** technology and **IEEE 1588 Precision Time Protocol (PTPv2)** for time synchronization on all ports.

The **Industrial Managed TSN Device** supports TSN IEEE standards needed for a complete real-time communication solution. These include IEEE 802.1AS-REV profile for time synchronization, IEEE 802.1Qbv for Enhancements for Scheduled Traffic, IEEE 802.1Qbu Frame Preemption, IEEE 802.3br Interspersing Express Traffic (IET), IEEE 802.1Qci for per-stream filtering and policing (PSFP) and IEEE 802.1CB frame replication and elimination for reliability (FRER) for seamless redundancy.The **Industrial Managed TSN Device** eliminates the need for separating information technology (IT) and operational technology (OT) Ethernet networks, providing a more ubiquitous approach to synchronization and precision timing for today's industrial automation systems.



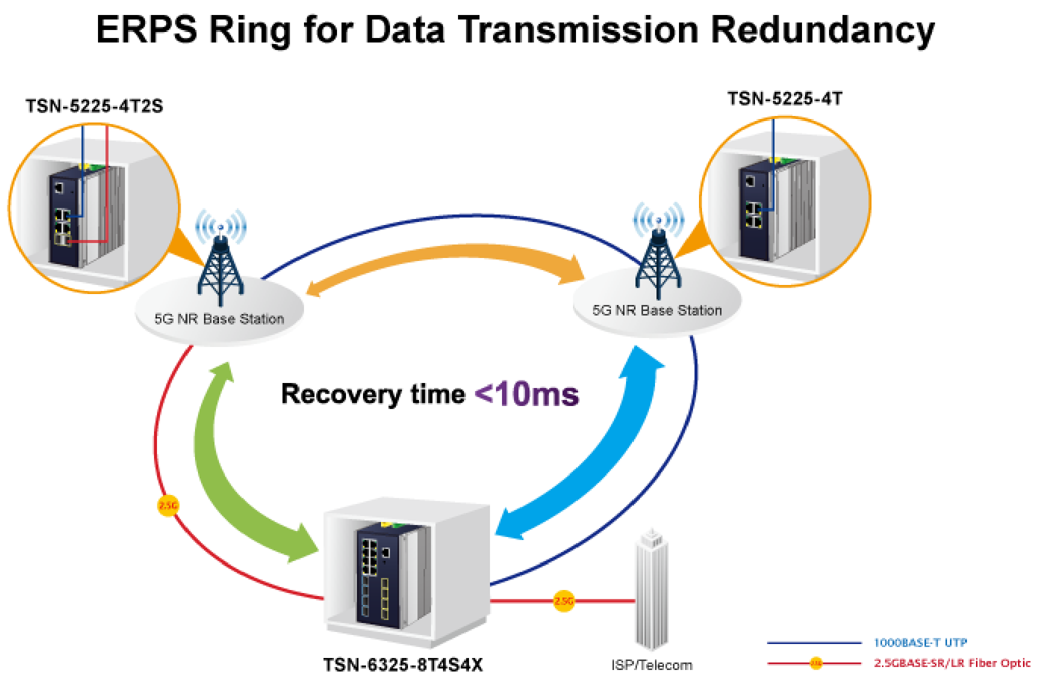
1588 Time Protocol for Industrial Computing Networks

The **Industrial Managed TSN Device** features IEEE 1588v2 PTP (Precision Time Protocol) with hardware-based time stamping for precise time synchronization of networks, and support for **Boundary Clock**, **End to End** and **Peer to Peer Transparent Clock** modes. It is ideal for telecom and carrier Ethernet applications, supporting MEF service delivery and timing over packet solutions for IEEE 1588 and synchronous Ethernet.



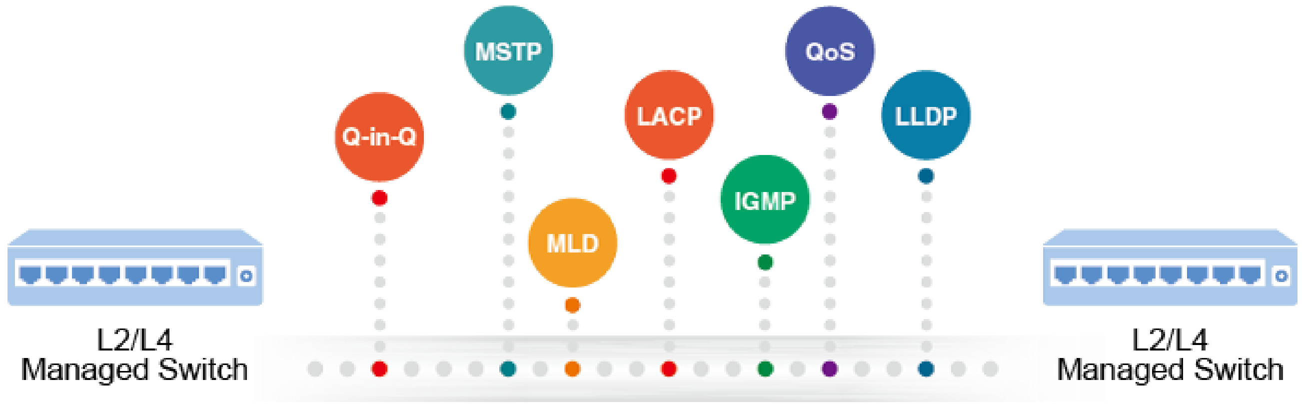
Redundant Ring, Fast Recovery for Critical Network Applications

The **Industrial Managed TSN Device** supports redundant ring technology and features strong, rapid self-recovery capability to prevent interruptions and external intrusions. It incorporates advanced **ITU-T G.8032 ERPS (Ethernet Ring Protection Switching)** technology, Spanning Tree Protocol (802.1s MSTP), and **redundant power** input system into customer's industrial automation network to enhance system reliability and uptime in harsh factory environments. In a simple ring network, the recovery time of data link can be as fast as 10ms.



Robust Layer 2 Features

The **Industrial Managed TSN Device** can be programmed for advanced Layer 2 switch management functions such as dynamic port link aggregation, 802.1Q tagged VLAN, Q-in-Q VLAN, private VLAN, Multiple Spanning Tree Protocol (MSTP), Layer 2 to Layer 4 QoS, bandwidth control, IGMP snooping and MLD snooping. Via the aggregation of supporting ports, the **Industrial Managed TSN Device** allows the operation of a high-speed trunk group that comes with multiple ports and supports fail-over as well.



Cybersecurity Network Solution to Minimize Security Risks

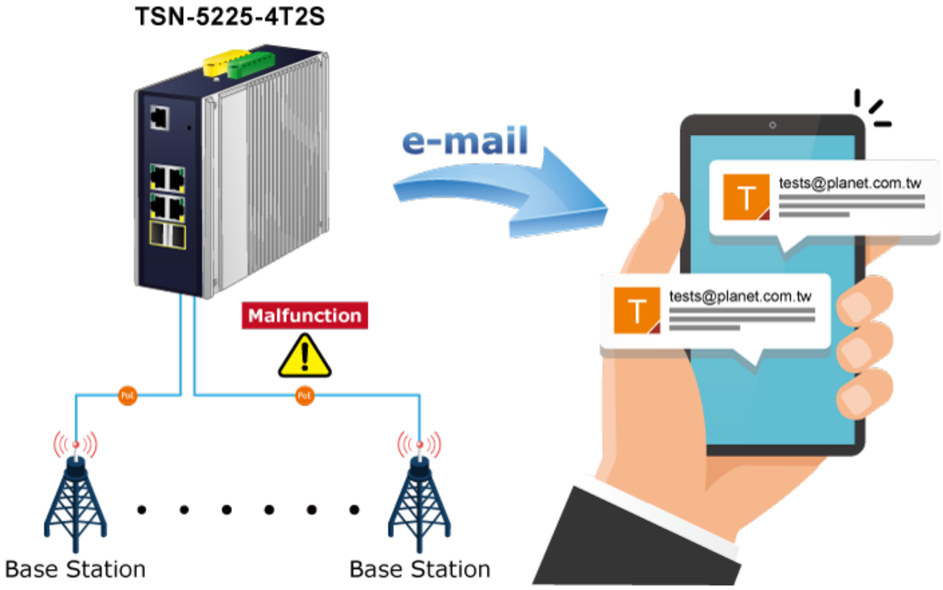
The cybersecurity features that virtually need no effort and cost to have include the protection of the switch management and the enhanced security of the mission-critical network. Both SSHv2 and TLSv1.2 protocols are utilized to provide strong protection against advanced threats. The network administrator can now construct highly-secure corporate networks with considerably less time and effort than before.

Modbus TCP Provides Flexible Network Connectivity for Factory Automation

With the supported **Modbus TCP/IP** protocol, the **Industrial Managed TSN Device** can easily integrate with **SCADA** systems, **HMI** systems and other data acquisition systems in factory floors. It enables administrators to remotely monitor the industrial Ethernet switch's **operating information**, **port information,** communication status, and DI and DO status, thus easily achieving enhanced monitoring and maintenance of the entire factory.

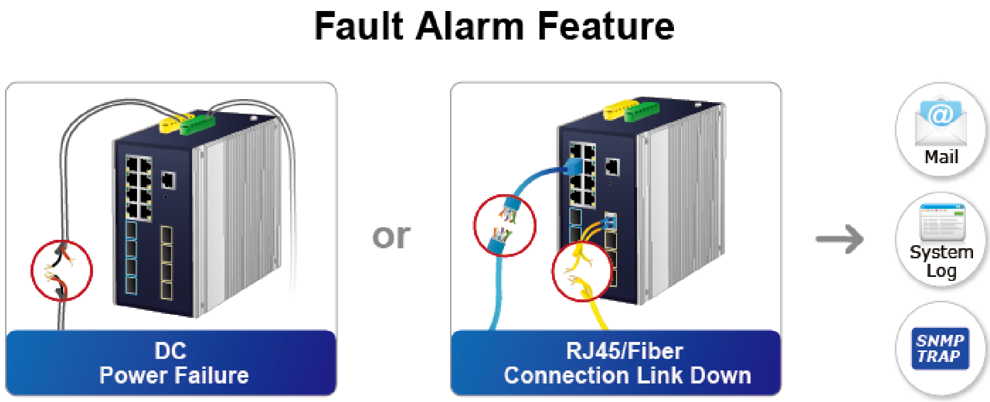
SMTP/SNMP Trap Event Alert

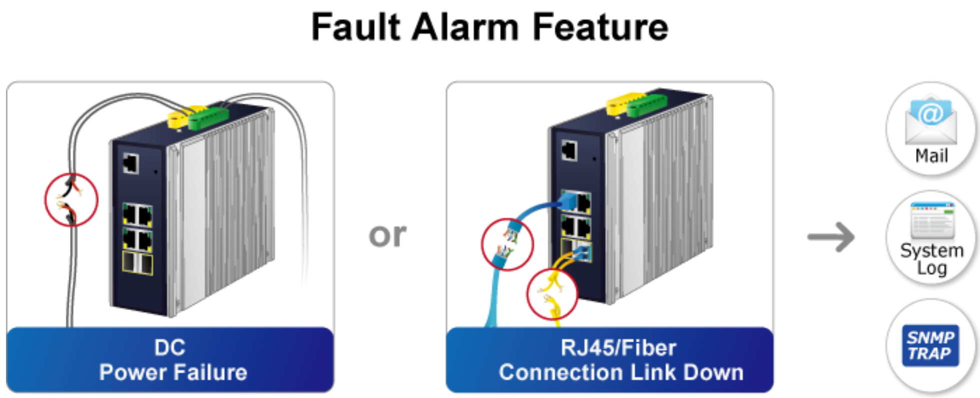
The **Industrial Managed TSN Device** provides event alert function to help to diagnose the abnormal device owing to whether or not there is a break of the network connection, or the rebooting response.



Effective Alarm Alert for Better Protection

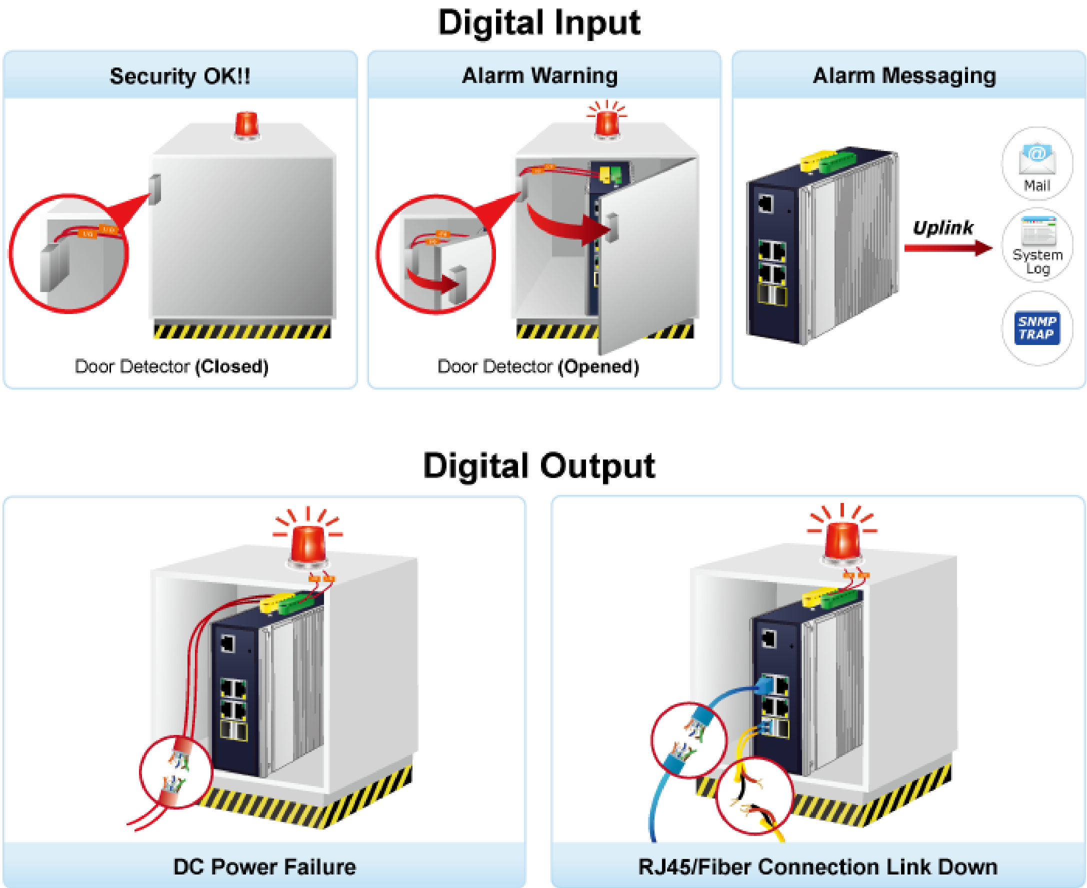
The **Industrial Managed TSN Device** supports a Fault Alarm feature which can alert the users when there is something wrong with the switches. With this ideal feature, the users would not have to waste time to find where the problem is. It will help to save time and human resource.





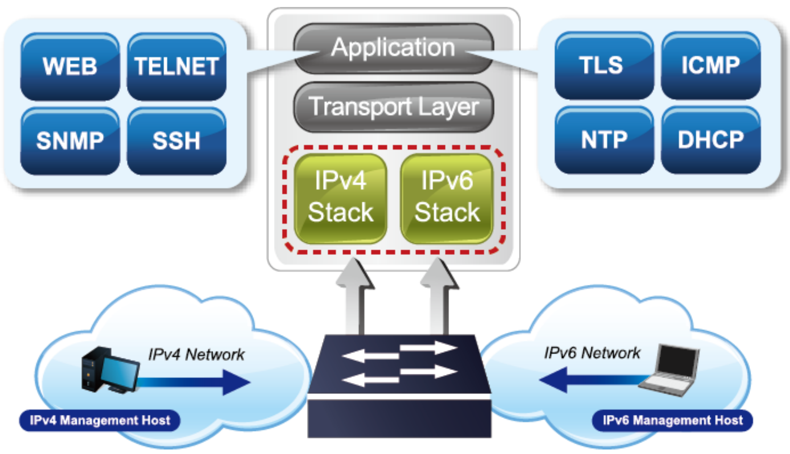
Digital Input and Digital Output for External Alarm

The **Industrial Managed TSN Device** supports Digital Input and Digital Output on its front panel. This external alarm enables users to use Digital Input to detect and log external device status (such as door intrusion detector), and send event alarm to the administrators. The Digital Output could be used to alarm the administrators if the **Industrial Managed TSN Device**'s port shows link down, link up or power failure.



IPv6/IPv4 Dual Stack

Supporting both IPv6 and IPv4 protocols, the **Industrial Managed TSN Device** helps data centers, campuses, telecoms, and more to experience the IPv6 era with the lowest investment as its network facilities need not be replaced or overhauled if the IPv6 FTTx edge network is set up.



Efficient Management

For efficient management, the **Industrial Managed TSN Device** is equipped with console, Web and SNMP management interfaces.

- With the built-in **Web-based** management interface, the **Industrial Managed TSN Device** offers an easy-to-use, platform-independent management and configuration facility.
- For **text-based** management, it can be accessed via Telnet and the console port.
- For standard-based monitor and management software, it offers SNMPv3 connection which encrypts the packet content at each session for secure remote management.

Powerful Network Security

The **Industrial Managed TSN Device** offers comprehensive Layer 2 to Layer 4 **Access Control List (ACL)** for enforcing security to the edge. It can be used to restrict network access by denying packets based on source and destination IP address, TCP/UDP ports or defined typical network applications. Its protection mechanism also comprises **802.1X Port-based** and **MAC-based** user and device authentication. With the **private VLAN** function, communication between edge ports can be prevented to ensure user privacy.

Advanced IP Network Protection

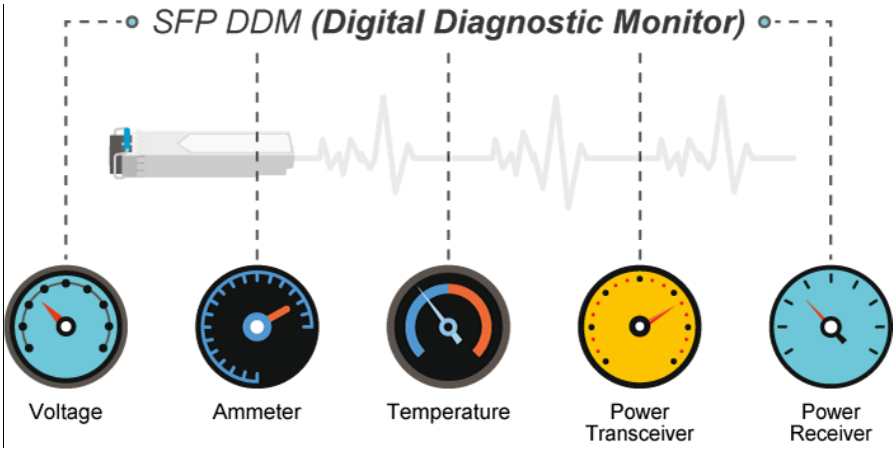
The **Industrial Managed TSN Device** also provides **DHCP Snooping**, **IP Source Guard** and **Dynamic ARP Inspection** functions to prevent IP snooping from attack and discard ARP packets with invalid MAC address. The network administrators can now construct highly-secure corporate networks with considerably less time and effort than before.

Excellent Traffic Control

The **Industrial Managed TSN Device** is loaded with powerful traffic management and QoS features to enhance connection services by telecoms and ISPs. The QoS features include wire-speed Layer 4 traffic classifiers and bandwidth limit that are particularly useful for multi-tenant units, multi-business units, Telco and network service providers' applications. It also empowers the industrial environment to take full advantage of the limited network resources and guarantees the best performance in VoIP and video conferencing transmission.

Intelligent SFP Diagnosis Mechanism (TSN-5225-4T2S and TSN-900-2T2S only)

The **Industrial Managed TSN Device** supports SFP-DDM (digital diagnostic monitor) function that greatly helps network administrator to easily monitor real-time parameters of the SFP transceivers, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage.



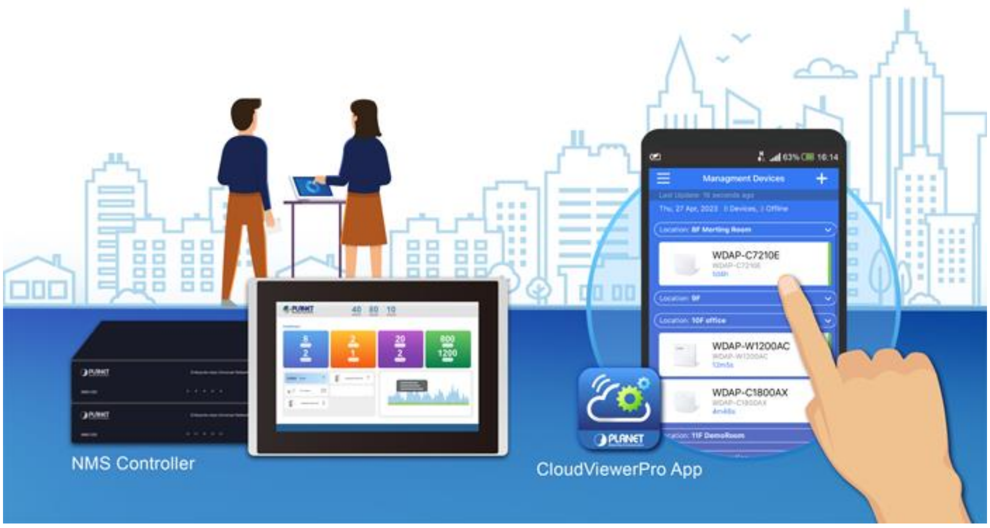
Common_Intelligent-SFP_SFP+-Diagnosis-Mechanism.png

Layer 3 IPv4 and IPv6 Software VLAN Routing for Secure and Flexible Management

To help customers stay on top of their businesses, the **Industrial Managed TSN Device** not only provides ultra high transmission performance and excellent Layer 2 technologies, but also IPv4/IPv6 software VLAN routing feature which allows to crossover different VLANs and different IP addresses for the purpose of having a highly-secure, flexible management and simpler networking application.

Remote Management Solution

PLANET's **Universal Network Management System** (UNI-NMS) and NMSViewerPro/CloudViewerPro app support IT staff by remotely managing all network devices and monitoring PDs' operational statuses. Thus, they're designed for both the enterprises and industries where deployments of PDs can be as remote as possible, without having to go to the actual location once a bug or faulty condition is found. With the UNI-NMS or NMSViewerPro/CloudViewerPro app, all kinds of businesses can now be speedily and efficiently managed from one platform.



Flexibility and Extension Solution

The additional two mini-GBIC slots built in the **Industrial Managed TSN Device** support dual-speed 1000/2500BASE-X SFP (small form-factor pluggable) fiber-optic modules (TSN-5225-4T2S and TSN-900-2T2S only), meaning the administrator now can flexibly choose the suitable SFP transceiver according to not only the transmission distance but also the transmission speed required. The distance can be extended from 300meters to 2km (multi-mode fiber) and to 10/20/30/40/60/70/80/120 kilometers (single-mode fiber or WDM fiber). They are well suited for applications within the enterprise data centers and distributions.

1.3 How to Use This Manual

This User's Manual is structured as follows:

Section 2, **INSTALLATION**

The section explains the functions of the **Industrial Managed TSN Device** and how to physically install the **Industrial Managed TSN Device**.

Section 3, **SWITCH MANAGEMENT**

The section contains the information about the software function of the **Industrial Managed TSN Device**.

Section 4, **WEB CONFIGURATION**

The section explains how to manage the **Industrial Managed TSN Device** by Web interface.

Section 5, **SWITCH OPERATION**

The chapter explains how to do the switch operation of the **Industrial Managed TSN Device**.

Section 6, **TROUBLESHOOTING**

The chapter explains how to do troubleshooting of the **Industrial Managed TSN Device**.

Appendix A

The section contains cable information of the **Industrial Managed TSN Device**.

Appendix B

The section contains glossary information of the **Industrial Managed TSN Device**.

1.4 Product Features

- **Physical Port**
  - **4 10/100/1000BASE-T** Gigabit Ethernet RJ45 ports (TSN-5225-4T only)
  - **4 10/100/1000BASE-T** Gigabit Ethernet RJ45 ports and **2 1000/2500BASE-X SFP** slots for SFP type auto detection (TSN-5225-4T2S only)
  - **2 10/100/1000BASE-T** Gigabit Ethernet RJ45 ports and **2 1000/2500BASE-X SFP** slots for SFP type auto detection (TSN-900-2T2S only)
  - One RJ45 console interface for basic management and setup

- **Industrial Hardened Design**
  - Dual power input, redundant power with reverse polarity protection
    - DC 9 to 48V input or AC 24V input
    - Active-active redundant power failure protection
    - Backup of catastrophic power failure on one supply
    - Fault tolerance and resilience
  - DIN-rail and wall-mountable designs
  - IP30 aluminum case
  - Supports 5000V DC Ethernet ESD protection
  - -40 to 75 degrees C operating temperature

- **Digital Input and Digital Output**
  - 2 Digital Input (DI)
  - 2 Digital Output (DO)
  - Integrates sensors into auto alarm system
  - Transfers alarm to IP network via email and SNMP trap

- **Time Sensitive Networking**
  - **High Precision Time Synchronization**
    - IEEE1588 (Time Stamping)
    - 802.1AS-Rev gPTP default profile
  - **Shapers**
    - 802.1Qbv Enhancements for Scheduled Traffic
    - 802.1Qch (Cyclic Queuing and Forwarding)
  - **TSN Stream Policing**
    - 802.1Qci (Per Stream Filtering and Policing)
  - **Redundancy**
    - 802.1CB FRER for seamless redundancy
    - Also standard Linear and Ring protection
  - **Delay Reduction**
    - IEEE 802.1Qbu Frame Preemption
    - IEEE 802.3br Interspersing Express Traffic (IET)

- **Layer 3 IP Routing Features**
  - Supports maximum 32 static routes and route summarization

- **Layer 2 Features**
  - Prevents packet loss with back pressure (half-duplex) and IEEE 802.3x pause frame flow control (full-duplex)
  - High performance of Store-and-Forward architecture, and runt/CRC filtering eliminates erroneous packets to optimize the network bandwidth
  - Storm control support
    - Broadcast/Multicast/Unknown unicast
  - Supports **VLAN**
    - IEEE 802.1Q tagged VLAN
    - Supports provider bridging (VLAN Q-in-Q IEEE 802.1ad)
    - Private VLAN Edge (PVE)
    - Protocol-based VLAN
    - MAC-based VLAN
    - Protocol-based VLAN
    - Voice VLAN
    - VLAN Translation
    - GVRP (GARP VLAN Registration Protocol)
  - Supports **Spanning Tree Protocol**
    - IEEE 802.1D Spanning Tree Protocol (STP)
    - IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
    - IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), spanning tree by VLAN
    - BPDU Guard
  - Supports **Link Aggregation**
    - 802.3ad Link Aggregation Control Protocol (LACP)
    - Cisco ether-channel (static trunk)
    - Maximum2 trunk groups with 4 ports per trunk group (TSN-5225-4T only)
    - Maximum 3 trunk groups with 6 ports per trunk group (TSN-5225-4T2S and TSN-900-2T2S only)
  - Provides port mirror (many-to-1)
  - Port mirroring to monitor the incoming or outgoing traffic on a particular port
  - Loop protection to avoid broadcast loops
  - Supports ERPS (Ethernet Ring Protection Switching)
  - Compatible with Cisco Uni-directional link detection(UDLD) that monitors a link between two switches and blocks the ports on both ends of the link if the link fails at any point between the two devices
  - Link Layer Discovery Protocol (LLDP) and LLDP-MED

- **Quality of Service**
  - Ingress shaper and egress rate limit per port bandwidth control
  - 8 priority queues on all switch ports
  - Traffic classification
    - IEEE 802.1p CoS
    - ToS/DSCP/IP Precedence of IPv4/IPv6 packets
    - IP TCP/UDP port number
    - Typical network application
  - Strict priority and Weighted Round Robin (WRR) CoS policies
  - Supports QoS and In/Out bandwidth control on each port
  - Traffic policing on the switch port
  - DSCP remarking
  - Voice VLAN

- **Multicast**
  - Supports IPv4 IGMP snooping v1, v2 and v3
  - Supports IPv6 MLD snooping v1 and v2
  - Querier mode support
  - IPv4 IGMP snooping port filtering
  - IPv6 MLD snooping port filtering
  - MVR (Multicast VLAN Registration)

- **Security**
  - Authentication
    - IEEE 802.1x Port-based/MAC-based network access authentication
    - Built-in RADIUS client to co-operate with the RADIUS servers
    - TACACS+ login users access authentication
    - RADIUS/TACACS+ users access authentication
  - Access Control List
    - IP-based Access Control List (ACL)
    - MAC-based Access Control List
  - Source MAC/IP address binding
  - **DHCP Snooping** to filter un-trusted DHCP messages
  - **Dynamic ARP Inspection** discards ARP packets with invalid MAC address to IP address binding
  - **IP Source Guard** prevents IP spoofing attacks
  - IP address access management to prevent unauthorized intruder

- **Management**
  - IPv4 and IPv6 dual stack management
  - Switch Management Interfaces
    - Console/Telnet command line interface
    - HTTP web switch management
    - SNMP v1 and v2c switch management
    - SSHv2, TLSv1.2 and SNMPv3 secure access
  - **IPv6** IP Address/NTP/DNS management
  - Built-in Trivial File Transfer Protocol (TFTP) client
  - BOOTP and DHCP for IP address assignment
  - System Maintenance
    - Firmware upload/download via HTTP
    - Configuration upload/download through HTTP
    - Reset button for system reboot or reset to factory default
    - Dual Images
  - DHCP Relay
  - DHCP Option82
  - DHCP Server Mode support
  - User Privilege levels control
  - NTP (Network Time Protocol)
  - Network Diagnostic
    - ICMPv6/ICMPv4 Remote Ping
  - SMTP/Syslog remote alarm
  - Four RMON groups (history, statistics, alarms and events)
  - SNMP trap for interface Link up and Link down notification
  - System Log
  - **SFP-DDM** (Digital Diagnostic Monitor) (TSN-5225-4T2S and TSN-900-2T2S only)
  - PLANET Smart Discovery Utility for deployment management
  - PLANET NMS system and NMSViewerPro/CloudViewerPro for deployment management

1.5 Product Specifications

Product	TSN-5225-4T	TSN-5225-4T2S	TSN-900-2T2S
Hardware Specifications			
Copper Ports	4 10/100/1000BASE-T RJ45 auto-MDI/MDI-X ports	4 10/100/1000BASE-T RJ45 auto-MDI/MDI-X ports	2 10/100/1000BASE-T RJ45 auto-MDI/MDI-X ports (Ports 3 to 4)
SFP Port	-	2 1000/2500BASE-X SFP ports (Ports 5 to 6)	2 1000/2500BASE-X SFP ports (Ports 1 to 2)
Console	1 x RJ45-to-RS232 serial port (115200, 8, N, 1)		
Reset Button	< 5 sec: System reboot > 5 sec: Factory default		
Connector	Removable 6-pin terminal block for power input Pin 1/2 for Power 1, Pin 3/4 for fault alarm, Pin 5/6 for Power 2 Removable 6-pin terminal block for DI/DO interface Pin 1/2 for DI 1 & 2, Pin 3/4 for DO 1 & 2, Pin 5/6 for GND		
Alarm	One relay output for power failure. Alarm relay current carry ability: 1A @ 24V DC		
Digital Input (DI)	2 digital input: Level 0: -24~2.1V (±0.1V) Level 1: 2.1~24V (±0.1V) Input load to 24V DC, 10mA max.		
Digital Output (DO)	2 digital output: Open collector to 24VDC, 100mA		
Enclosure	IP30 aluminum case		
Installation	DIN-rail or wall mounting		
SDRAM	1024Mbytes		
Flash Memory	64Mbytes		
Dimensions (W x D x H)	60 x 135 x 135 mm		
Weight	962g	986g	949g
Power Requirements	DC 9~48V, 1.5A max.		
	AC 24V, 1A max.		
Power Consumption	DC input: Max. 8.36 watts /28.53BTU (system on) Max. 9.89 watts /33.75BTU (Full loading)	DC input: Max. 6.05 watts /20.64BTU (system on) Max. 9.8 watts /33.44BTU (Full loading)	DC input: Max. 7.39 watts /25.22BTU (system on) Max. 10.18 watts /34.74BTU (Full loading)
	AC 24V input: Max. 6.2 watts /21.16BTU (system on) Max. 7.9 watts /26.96BTU (Full loading)	AC 24V input: Max. 5.4 watts /18.43BTU (system on) Max. 9.2 watts /31.39BTU (Full loading)	AC 24V input: Max. 5.4 watts /18.43BTU (system on) Max. 8.1 watts /27.64BTU (Full loading)
ESD Protection	5KV DC		
Surge Protection	6KV DC		

LED Indicators	System: Power 1 (Green), Power 2 (Green) Fault Alarm (Red) Ring (Green), Ring Owner (Green) DIDO (Red) Per 10/100/1000T RJ45 Port: 1000Mbps LNK/ACT (Green) 10/100Mbps LNK/ACT (Amber)		
Switching Specifications			
Switch Architecture	Store-and-Forward		
Switch Fabric	8Gbps/non-blocking	18Gbps/non-blocking	14Gbps/non-blocking
Throughput	5.95Mpps@64Bytes	13.3Mpps@64Bytes	10.41Mpps@64Bytes
Address Table	8K entries, automatic source address learning and aging		
Shared Data Buffer	32Mbits		
Jumbo Frame	10K bytes		
Flow Control	IEEE 802.3x pause frame for full duplex Back pressure for half duplex		
Layer 3 Functions			
IP Interfaces	Max. 8 VLAN interfaces		
Routing Table	Max. 32 routing entries		
Routing Protocols	IPv4 software static routing IPv6 software static routing		
Layer 2 Functions			
Port Configuration	Port disable/enable Auto-negotiation 10/100/1000Mbps full and half duplex mode selection Flow control disable/enable Port link capability control		
Port Status	Display each port's speed duplex mode, link status, flow control status, auto-negotiation status, trunk status		
Port Mirroring	TX/RX/Both Many-to-1 monitor Mirror – Remote Switched Port Analyzer (Cisco RSPAN) Supports up to 5 sessions		
VLAN	IEEE 802.1Q tagged VLAN IEEE 802.1ad Q-in-Q tunneling Private VLAN Edge (PVE) MAC-based VLAN Protocol-based VLAN Voice VLAN IP Subnet-based VLAN MVR (Multicast VLAN registration) GVRP Up to 4K VLAN groups, out of 4096 VLAN IDs		
Link Aggregation	IEEE 802.3ad LACP/static trunk Maximum 2 trunk groups with 4 ports per trunk group		
Spanning Tree Protocol	IEEE 802.1D Spanning Tree Protocol IEEE 802.1w Rapid Spanning Tree Protocol IEEE 802.1s Multiple Spanning Tree Protocol BPDU Guard, BPDU filtering and BPDU transparent		

IGMP Snooping	IPv4 IGMP (v1/v2/v3) snooping IPv4 IGMP querier mode support Supports 255 IGMP groups
MLD Snooping	IPv6 MLD (v1/v2) snooping, IPv6 MLD querier mode support Supports 255 MLD groups
Bandwidth Control	Per port bandwidth control Ingress: 100Kb~3276Mbps Egress: 100Kb~3281Mbps
Ring	Supports ERPS, and complies with ITU-T G.8032 Recovery time < 10ms @ 3 nodes Recovery time < 50ms @ 16 nodes Supports major ring and sub-ring
Synchronization	IEEE 1588v2 PTP(Precision Time Protocol) - PTP Master - PTP Slave - Boundary clock - Ordinary Clock - Peer-to-peer transparent clock - End-to-end transparent clock
QoS	Ingress Shaper and Egress Rate Limit per port bandwidth control 8 priority queues on all switch ports Traffic classification: −IEEE 802.1p CoS −IP TOS / DSCP / IP Precedence −IP TCP/UDP port number −Typical network application Traffic-policing policies on the switch port DSCP remarking
Time-Sensitive Networking Protocols	**High Precision Time Synchronization** - IEEE1588 (Time Stamping) - 802.1AS-Rev gPTP default profile **Shapers** - 802.1Qbv (Time-aware Scheduling) - 802.1Qch (Cyclic Queuing and Forwarding) **TSN Stream Policing** - 802.1Qci (Per Stream Filtering and Policing) **Redundancy** - 802.1CB (Frame Replication and Elimination for Redundancy for seamless redundancy) - Also standard Linear and Ring protection **Delay Reduction** - IEEE 802.1Qbu Frame Preemption, - IEEE 802.3br Interspersing Express Traffic (IET)
Security Functions	
Access Control List	IP-based ACL/MAC-based ACL ACL based on: - MAC Address - IP Address - Ethertype - Protocol Type - VLAN ID - DSCP

	- 802.1p Priority Up to 512 entries
Security	Port security IP source guard, up to 512 entries Dynamic ARP inspection, up to 1K entries Command line authority control based on user level Static MAC address, up to 64 entries
AAA	RADIUS client TACACS+ client
Network Access Control	IEEE 802.1x port-based network access control MAC-based authentication Local/RADIUS authentication
Management	
Basic Management Interfaces	Console; Telnet; Web browser; SNMP v1, v2c
Secure Management Interfaces	SSHv2, TLSv1.2, SNMPv3
System Management	Firmware upgrade by HTTP protocol through Ethernet network Configuration upload/download through HTTP Remote Syslog System log LLDP protocol NTP PLANET Smart Discovery Utility PLANET NMS PLANET NMSViewerPro/CloudViewerPro
Event Management	Remote syslog Local system log SMTP
SNMP MIBs	RFC 1213 MIB-II RFC 1493 Bridge MIB RFC 1643 Ethernet MIB RFC 2863 Interface MIB RFC 2665 Ether-Like MIB RFC 2819 RMON MIB (Group 1, 2, 3 and 9) RFC 2737 Entity MIB RFC 2618 RADIUS Client MIB RFC 2863 IF-MIB RFC 2933 IGMP-STD-MIB RFC 3411 SNMP-Frameworks-MIB RFC 4292 IP Forward MIB RFC 4293 IP MIB RFC 4836 MAU-MIB IEEE 802.1X PAE LLDP
Standards Conformance	
Regulatory Compliance	FCC Part 15 Class A CE: EN55032 EN55035

Stability Testing	IEC60068-2-32 (free fall) IEC60068-2-27 (shock) IEC60068-2-6 (vibration)
Standards Compliance	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX/100BASE-FX IEEE 802.3ab Gigabit 1000T IEEE 802.3z Gigabit SX/LX (TSN-5225-4T2S and TSN-900-2T2S) IEEE 802.3bz 2.5GBASE-X (TSN-5225-4T2S and TSN-900-2T2S) IEEE 802.3x flow control and back pressure IEEE 802.3ad port trunk with LACP IEEE 802.1D Spanning Tree Protocol IEEE 802.1w Rapid Spanning Tree Protocol IEEE 802.1s Multiple Spanning Tree Protocol IEEE 802.1p Class of Service IEEE 802.1Q VLAN tagging IEEE 802.1X Port Authentication Network Control IEEE 802.1ab LLDP IEEE 802.3ah OAM IEEE 1588 PTPv2 IEEE 802.1ag Connectivity Fault Management (CFM) IEEE 802.1AS - Timing and Synchronization for Time-sensitive Applications IEEE 802.1Qbu Frame Preemption, IEEE 802.3br Interspersing Express Traffic (IET) IEEE 802.1Qci Per-Stream Filtering and Policing (PSFP) IEEE 802.1Qbv Enhancements for Scheduled Traffic IEEE 802.1CB Frame Replication and Elimination for Reliability (FRER) RFC 768 UDP RFC 783 TFTP RFC 791 IP RFC 792 ICMP RFC 2068 HTTP RFC 1112 IGMP v1 RFC 2236 IGMP v2 RFC 3376 IGMP v3 RFC 2710 MLD v1 RFC 3810 MLD v2 ITU-T G.8032 ERPS Ring
Environment	
Operating	-40 ~ 75 degrees C
Storage	-40 ~ 85 degrees C
Humidity	5 ~ 95% (non-condensing)

2. INSTALLATION

2.1 Hardware Description

The **Industrial Managed TSN Device** provides three different running speeds – 10Mbps, 100Mbps, 1000Mbps or 2500Mbps and automatically distinguishes the speed of incoming connection.

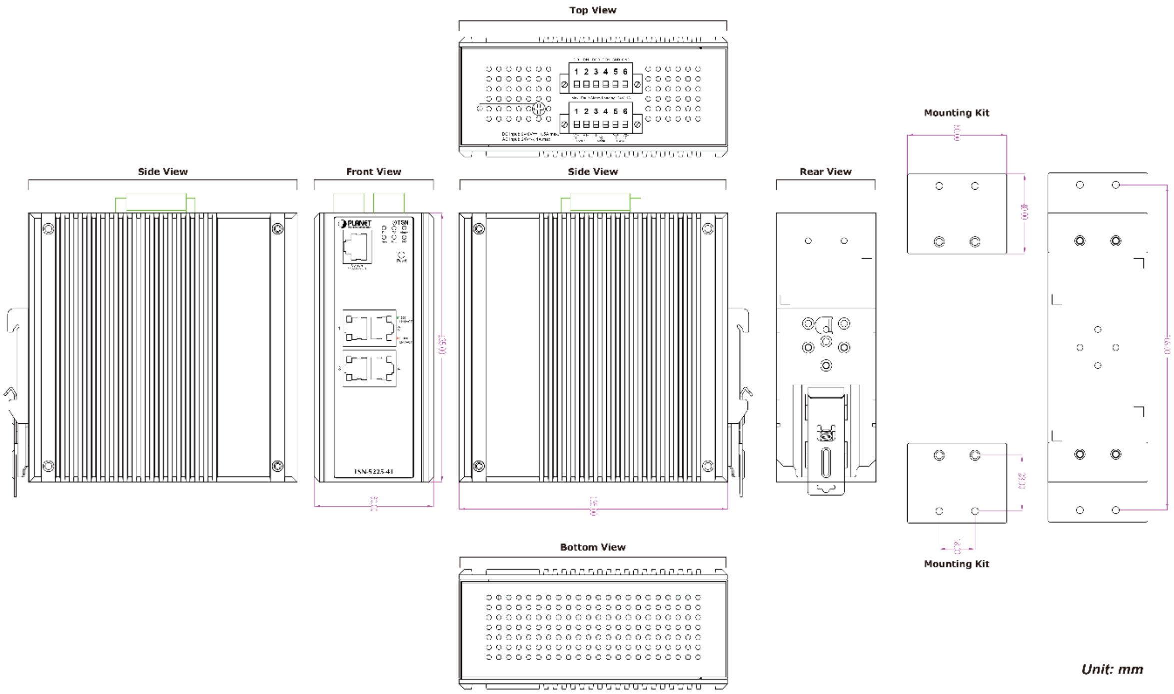
This section describes the hardware features of **Industrial Managed TSN Device**. For easier management and control of the **Industrial Managed TSN Device**, familiarize yourself with its display indicators and ports. Front panel illustrations in this chapter display the unit LED indicators. Before connecting any network device to the **Industrial Managed TSN Device**, read this chapter carefully.

Model Name / Item	TSN-5225-4T	TSN-5225-4T2S	TSN-900-2T2S
10/100/1000BASE-T Copper	4	4	2
1000/2500BASE-X SFP	-	2	2
Power Inpuit	9-48V DC x 2 or 24V AC		

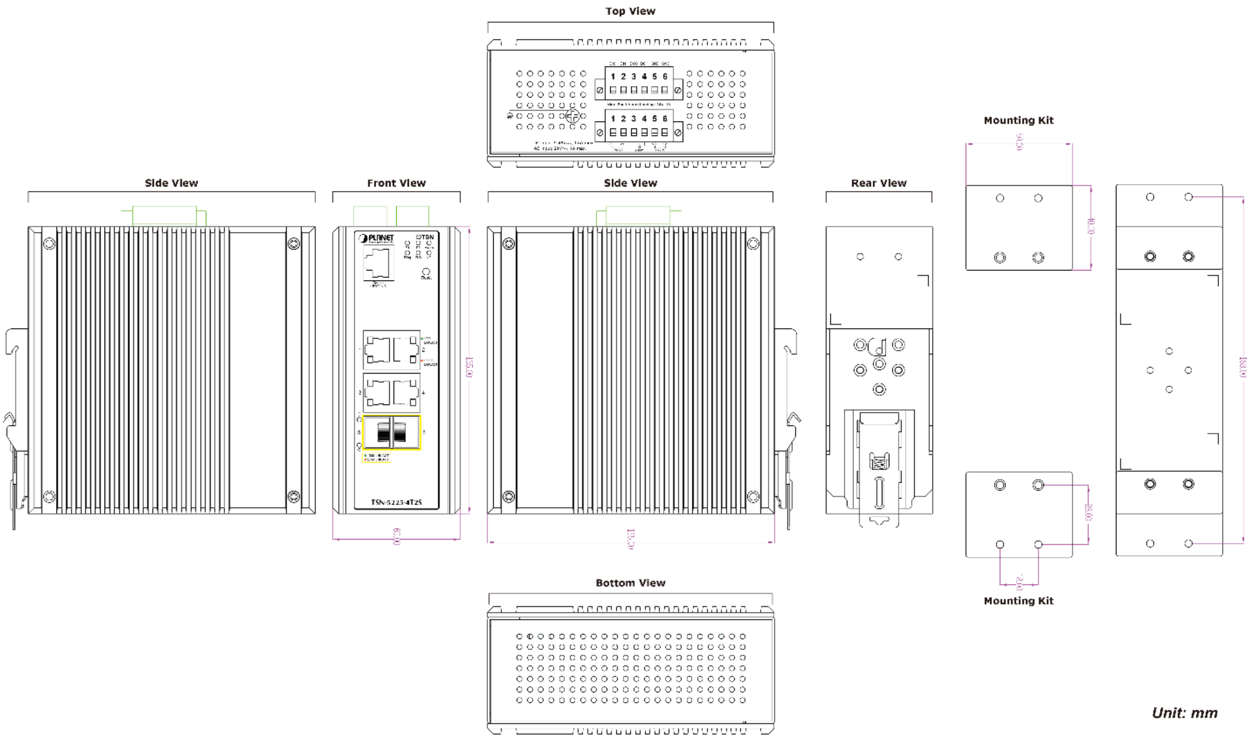
2.1.1 Physical Dimensions

- **TSN-5225-4T**

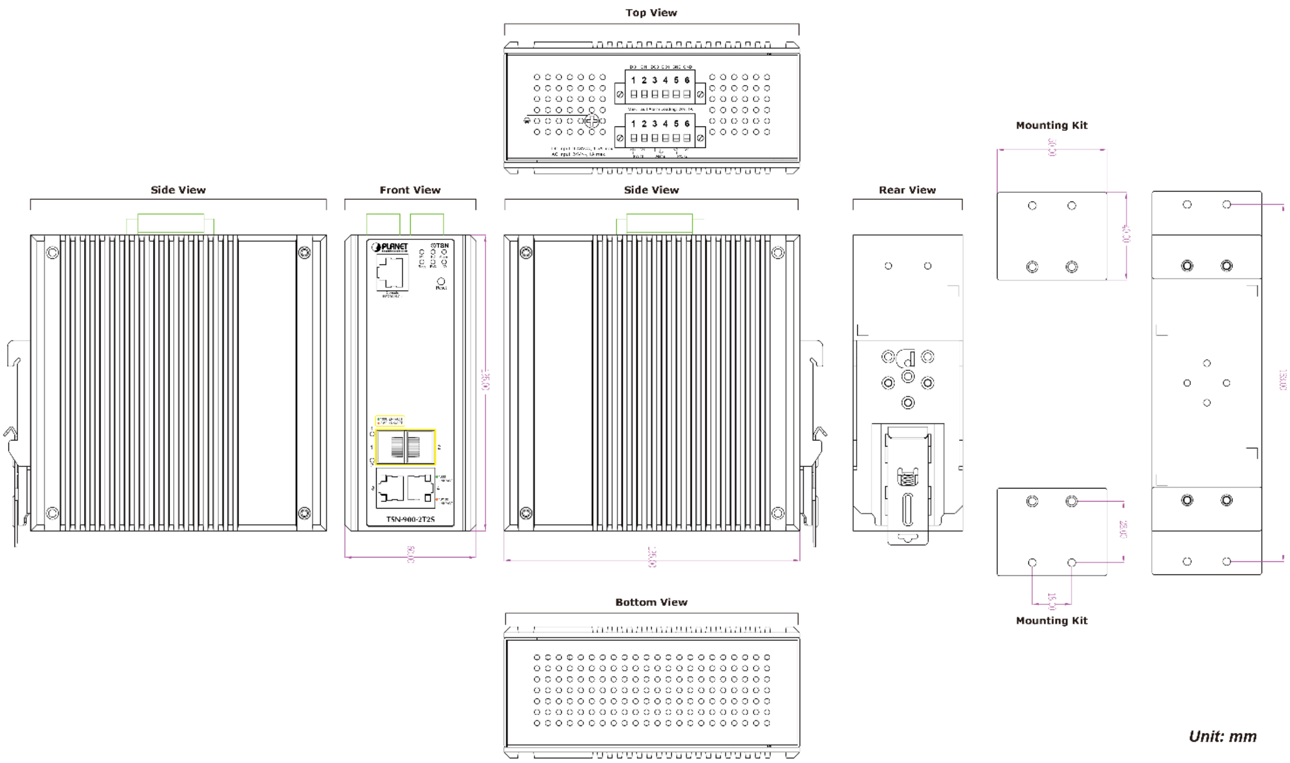
  Dimensions (W x D x H) : 60 x 135 x 135mm



TSN-5225-4T2S



TSN-900-2T2S



2.1.2 Front Panel

The front panel provides a simple interface monitoring the **Industrial Managed TSN Device**. Figure 2-1-1 and Figure 2-1-2 show the front panels of the **Industrial Managed TSN Device**.

TSN-5225-4T/TSN-5225-4T2S/TSN-900-2T2S

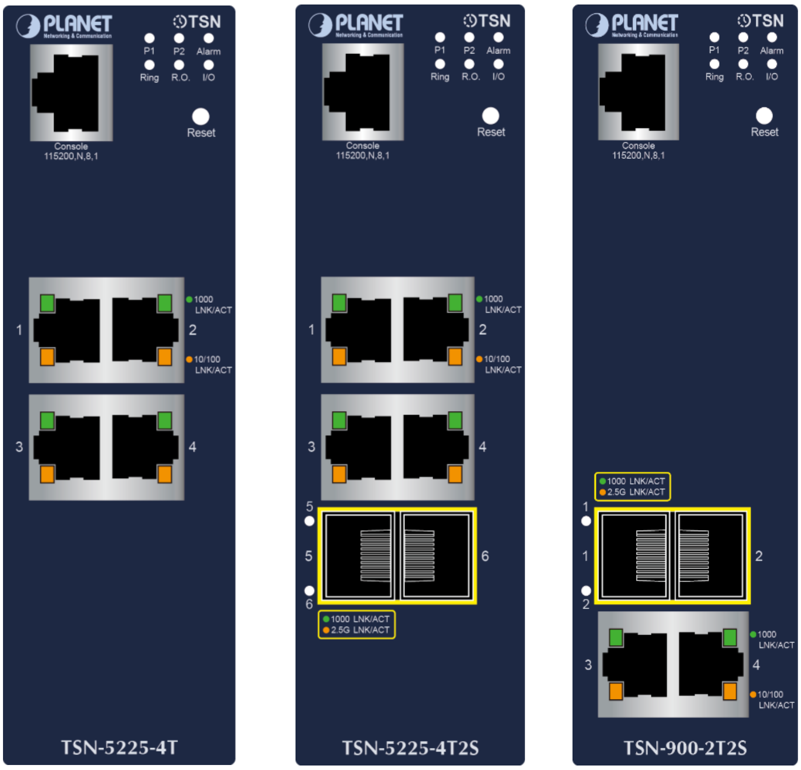


Figure 2-1-1: Front Panel of **Industrial Managed TSN Device**

- **Gigabit TP Interface**

  10/100/1000BASE-T Copper, RJ45 twisted-pair: Up to 100 meters.

- **SFP Slot** (TSN-5225-4T2S and TSN-900-2T2S only)

  1000/2500BASE-X mini-GBIC slot, SFP (Small-form Factor Pluggable) transceiver module: From 550 meters to 2km (multi-mode fiber) and to 10/20/30/40/50/70/120 kilometers (single-mode fiber).

- **Console Port**

  The console port is an RJ45 port connector. It is an interface for connecting a terminal directly. Through the console port, it provides rich diagnostic information including IP address setting, factory reset, port management, link status and system setting. Users can use the attached DB9 to RJ45 console cable in the package and connect to the console port on the device. After the connection, users can run any terminal emulation program (Hyper Terminal, ProComm Plus, Telix, Winterm and so on) to enter the startup screen of the device.

- **Reset Button**

  On the upper left side of the front panel, the reset button is designed for rebooting the **Industrial Managed TSN Device** without turning off and on the power. The following is the summary table of reset button functions:

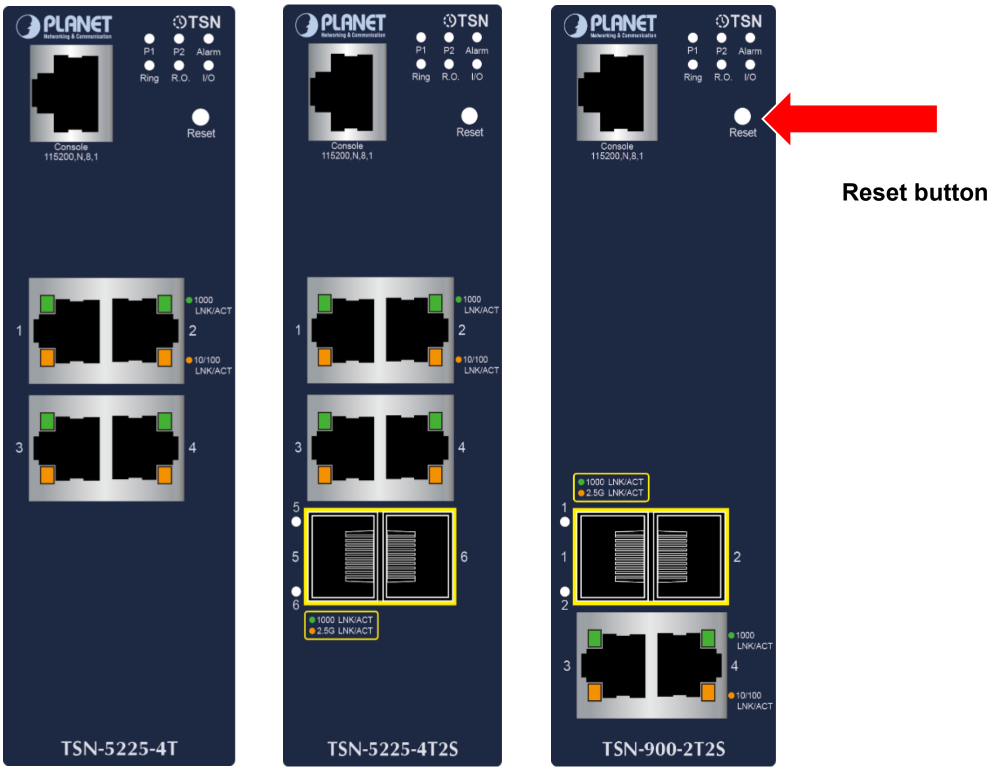


Figure 2-1-2: Reset Button of **Industrial Managed TSN Device**

Reset Button Pressed and Released	Function
< 5 sec: System Reboot	Reboot the **Industrial Managed TSN Device**.
> 5 sec: Factory Default	Reset the **Industrial Managed TSN Device** to Factory Default configuration. The **Industrial Managed TSN Device** will then reboot and load the default settings as shown below: ◦ Default Username: **admin** ◦ Default Password: **sw + the last 6 characters of the MAC ID in lowercase** (TSN-5225-4T/TSN-5225-4T2S only) ◦ Default Password: **mc + the last 6 characters of the MAC ID in lowercase** (TSN-900-2T2S only) ◦ Default IP Address: **192.168.0.100** ◦ Subnet Mask: **255.255.255.0** ◦ Default Gateway: **192.168.0.254**

Find the MAC ID on your device label. The default password is "sw" or "mc" followed by the last six lowercase characters of the MAC ID.

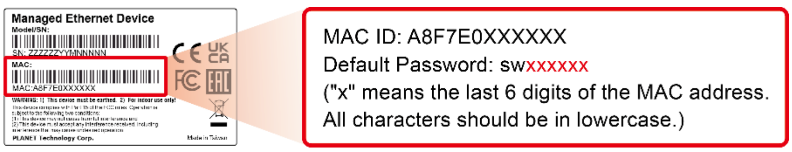


Figure 2-1-3: TSN-5225-4T MAC ID Label

Enter the default username and password, then set a new password according to the rule-based prompt and confirm it. Upon success, press any key to return to the login prompt. Log in with "admin" and the "new password" to access the CLI.

2.1.3 LED Indications

The front panel LEDs indicate instant statuses of power and ring, R.O., DI/DO and fault; they help monitor and troubleshoot when needed. Figures 2-1-4 and 2-1-5 show the LED indications of the **Industrial Managed TSN Device**.

TSN-5225-4T/TSN-5225-4T2S/TSN-900-2T2S

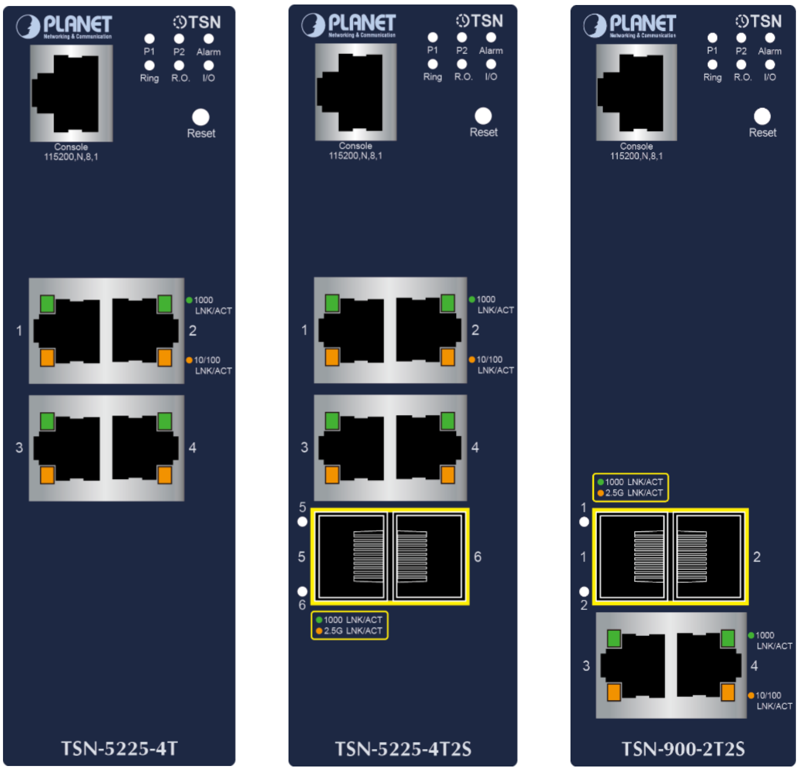


Figure 2-1-4: Industrial Managed TSN Device LEDs on Front Panel

- **System**

LED	Color	Function
P1	Green	**Lights** to indicate that the switch has power.
P2	Green	**Lights** to indicate that the switch has power.
Alarm	Red	**Lights** to indicate Power failure
Ring	Green	**Lights** to indicate that the ERPS Ring has been created successfully.
R.O.	Green	**Lights** to indicate that the Ring Owner has been enabled.
I/O	Red	Blinks to indicate that switch DC or port has failed or DI has event.

■ **Per 10/100/1000BASE-T Port with PoE (Port-1~Port-4 for TSN-5225 series and Port-3~Port-4 for TSN-900-2T2S)**

LED	Color	Function	
1000 LNK/ACT	**Green**	**Lights**	Indicating the port is running at **1000Mbps** and successfully established.
		Blinks	Indicating that the switch is actively sending or receiving data over that port.
10/100 LNK/ACT	**Amber**	**Lights**	Indicating the port is running at **10/100Mbps** and successfully established.
		Blinks	Indicating that the switch is actively sending or receiving data over that port.

■ **Per 1G/2.5GBASE-X SFP Interface (Port-5~Port-6 for TSN-5225-4T2S and Port-1~Port-2 for TSN-900-2T2S)**

LED	Color	Function	
1G LNK/ACT	**Green**	**Lights**	Indicating the port is successfully established at **1000Mbps**.
		Blinks	Indicating that the switch is actively sending or receiving data over that port.
2.5G LNK/ACT	**Amber**	**Lights**	Indicating the port is successfully established at **2500Mbps**.
		Blinks	Indicating that the switch is actively sending or receiving data over that port.

2.1.4 Switch Upper Panel

The Upper Panel of the **Industrial Managed TSN Device** comes with a DC inlet power socket and one terminal block connector with 6 contacts.

■ **DC Power Connector for Industrial Managed TSN Device**

The top panels of the **Industrial Managed TSN Device** contain a DC power connector, which accepts DC power input voltage from **9V to 48V DC**. Connect the power cable to the **Industrial Managed TSN Device** at the input terminal block.

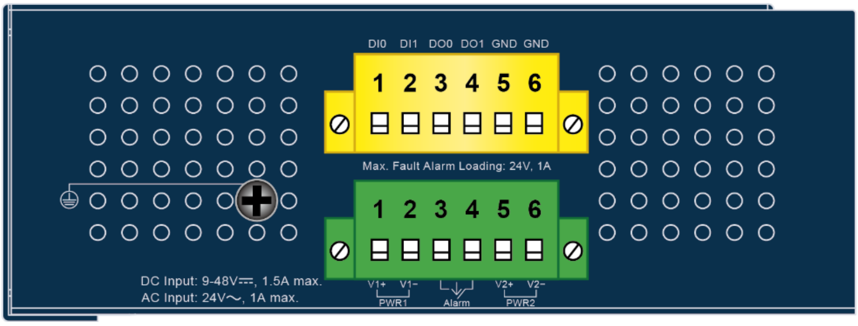


Figure 2-1-5: Industrial Managed TSN Device Upper Panel

2.1.5 Wiring the DC Power Input

The Upper Panel of the **Industrial Managed TSN Device** indicates an inlet power socket and consists of one green terminal block connector within 6 contacts. Please follow the steps below to insert the power wire.

1. Insert positive/negative DC power wires into Contacts 1 and 2 for Power 1, or Contacts 5 and 6 for Power 2.
   - DC 9-48V, AC 24V

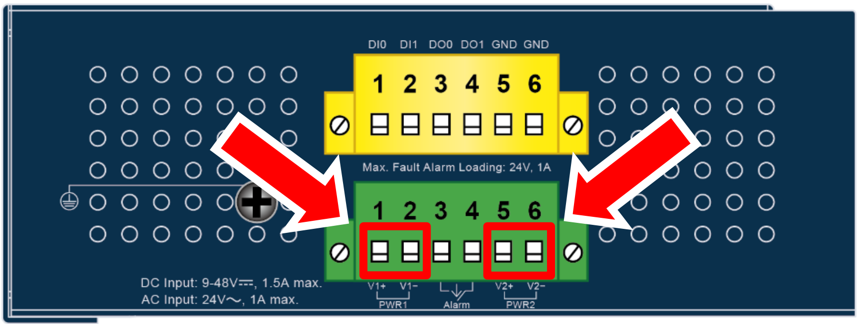


Figure 2-1-6: Industrial Managed TSN Device Upper Panel

2. Tighten the wire-clamp screws for preventing the wires from loosening.

1 2 3 4 5 6

DC 1 DC 2

\+ - + -

Figure 2-1-7: 6-pin Terminal Block Power Wiring Input for **Industrial Managed TSN Device**

1. The wire gauge for the terminal block should be in the range from **12 to 24** AWG.
2. Please check the AWG Ampere specification before connecting PLANET **Industrial Managed TSN Device**.

2.1.6 Wiring the Fault Alarm Contact

The fault alarm contacts are in the middle (3 & 4) of the terminal block connector as the picture shows below. Inserting the wires, the **Industrial Managed TSN Device** will detect the fault status of the power failure, or port link failure (available for managed model). The following illustration shows an application example for wiring the fault alarm contacts

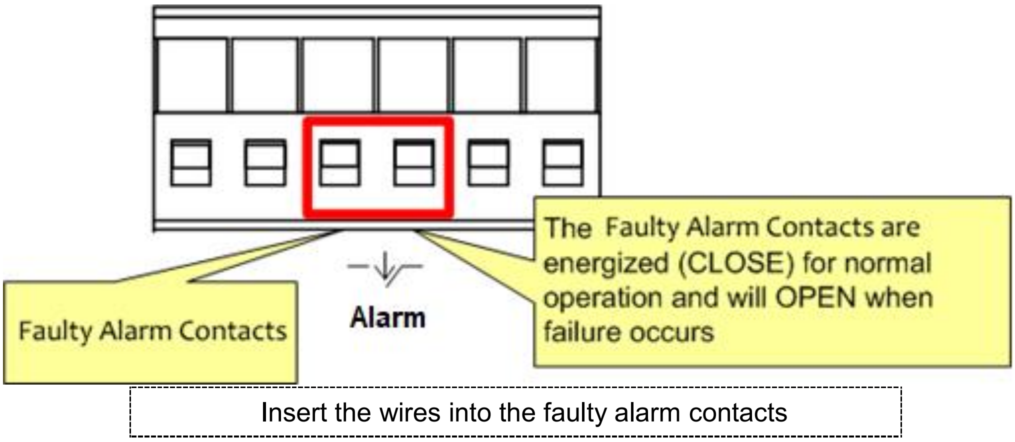


Figure 2-1-8: Fault Alarm Contact for **Industrial Managed TSN Device**

1. The wire gauge for the terminal block should be in the range of 12 ~ 24 AWG.
2. When performing any of the procedures like inserting the wires or tighten the wire-clamp screws, make sure the power is OFF to prevent from getting an electric shock.

2.1.7 Grounding the Device

Users **MUST** complete grounding wired with the device; otherwise, a sudden lightning could cause fatal damage to the device.

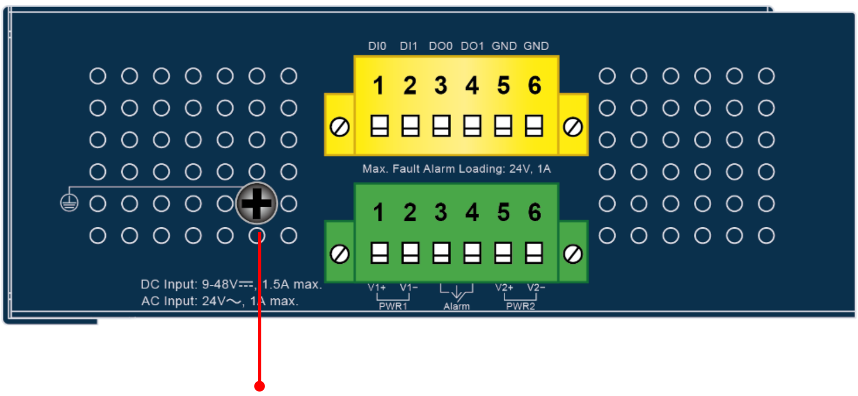


Figure 2-1-9: Wiring the DI and DO of **Industrial Managed TSN Device**

2.2 Installing the Industrial Managed TSN Device

This section describes how to install your **Industrial Managed TSN Device** and make connections to the **Industrial Managed TSN Device**. Please read the following topics and perform the procedures in the order being presented. To install your **Industrial Managed TSN Device** on a desktop or shelf, simply complete the following steps.

In this paragraph, we will describe how to install the **Industrial Managed TSN Device** and the installation points attended to it.

2.2.1 Installation Steps

1. **Unpack the Industrial Managed TSN Device.**
2. **Check if the DIN-rail bracket is screwed on the Industrial Managed TSN Device or not**. If the DIN-rail bracket is not screwed on the **Industrial Managed TSN Device**, refer to **DIN-rail Mounting** section for DIN-rail installation. If users want to wall-mount the **Industrial Managed TSN Device**, refer to the **Wall Mount Plate Mounting** section for wall-mount plate installation**.**
3. **To hang the Industrial Managed TSN Device on the DIN-rail track or wall.**
4. **Power on the Industrial Managed TSN Device**. Please refer to the **Wiring the Power Inputs** section for knowing the information about how to wire the power. The power LED on the **Industrial Managed TSN Device** will light up. Please refer to the **LED Indicators** section for indication of LED lights**.**
5. **Prepare the twisted-pair, straight-through Category 5 cable for Ethernet connection.**
6. **Insert one side of RJ45 cable (category 5) into the Industrial Managed TSN Device Ethernet port** (RJ45 port) while the other side to the network device's Ethernet port (RJ45 port), e.g., switch PC or server. The UTP port (RJ45) LED on the **Industrial Managed TSN Device** will light up when the cable is connected with the network device. Please refer to the **LED Indicators** section for LED light indication**.**

Note	
	Make sure that the connected network devices support MDI/MDI-X. If it does not support, use the crossover Category 5 cable.

7. **When all connections are set and all LED lights show normal, the installation is completed.**

2.2.2 DIN-rail Mounting

This section describes how to install the **Industrial Managed TSN Device**. There are two methods to install the **I Industrial Managed TSN Device** -- DIN-rail mounting and wall-mount plate mounting. Please read the following topics and perform the procedures in the order being presented.

Note

Follow all the DIN-rail installation steps as shown in the example.

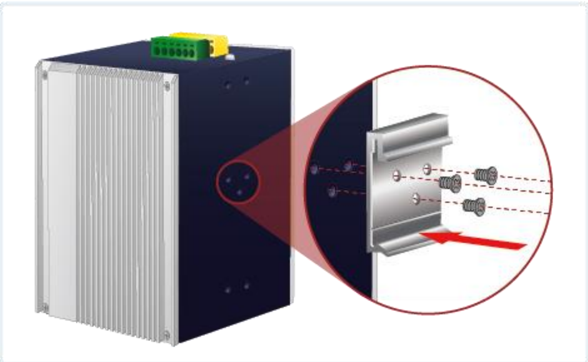
Step 1: Screw the DIN-rail bracket on the **Industrial Managed TSN Device**.

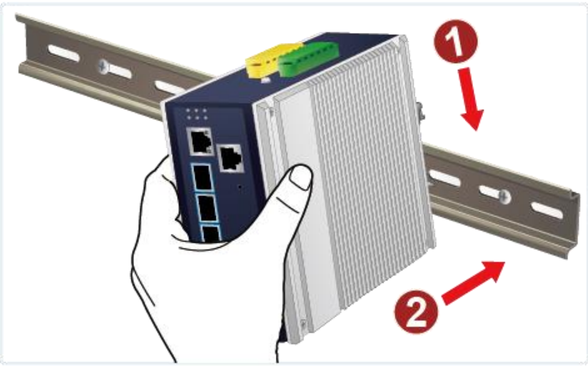
Step 2: Lightly slide the DIN-rail bracket into the track.

Step 3: Check whether the DIN-rail bracket is tightly on the track.

Please refer to the following procedures to remove the **Industrial Managed TSN Device** from the track.

Step 4: Lightly remove the unit from the track.





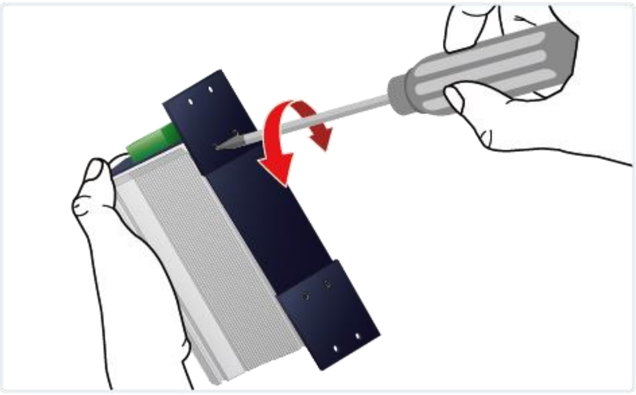
2.2.3 Wall-mount Plate Mounting

To install the **Industrial Managed TSN Device** on the wall, please follow the instructions below.

Note	**Follow all the DIN-rail installation steps as shown in the example.**

Step 1: Remove the DIN-rail bracket from the **Industrial Managed TSN Device**. Use the screwdriver to loosen the screws to remove the bracket.

Step 2: Place the wall-mount plate on the rear panel of the **Industrial Managed TSN Device**.



Step 3: Use the screwdriver to screw the wall-mount plate on the **Industrial Managed TSN Device.**

Step 4: Use the hook holes at the corners of the wall mount plate to hang the **Industrial Managed TSN Device** on the wall.

Step 5: To remove the wall-mount plate, reverse the steps above.

2.3 Cabling

- **10/100/1GBASE-T and 1G/2.5GBASE-SX/LX**

All 10/100/1GBASE-T ports come with auto-negotiation capability. Users only need to plug a working network device into one of the 10/100/1GBASE-T ports, and then turn on the **Industrial Managed TSN Device**. The port will automatically run after negotiating with the connected device. The **Industrial Managed TSN Device** has SFP interfaces that support 1G/2.5Gbps dual speed mode (Optional multi-mode/single-mode 1G/2.5GBASE-SX/LX SFP module)

- **Cabling**

Each 10/100/1GBASE-T port uses RJ45 sockets -- similar to phone jacks -- for connection of unshielded twisted-pair cable (UTP). (see table below).

The 1G/2.5GBASE-SX/LX SFP slot is used as LC connector with optional SFP module. Please see table below and know more about the cable specifications.

Port Type	Cable Type	Connector
10BASE-T	Cat 3, 4, 5, 2-pair	RJ45
100BASE-TX	Cat.5 UTP, 2-pair	RJ45
1GBASE-T	Cat.5/5e/6 UTP, 2-pair	RJ45
1GBASE-SX/LX	50/125µm or 62.5 / 125µm multi-mode 9/125µm single-mode	LC (multi/single mode)
2.5GBASE-SX/LX	50/125µm or 62.5 / 125µm multi-mode 9/125µm single-mode	LC (multi/single mode)

Any Ethernet devices like hubs/PCs can be connected to the **Industrial Managed TSN Device** by using straight-through wires. The 10M/100M/1G/2.5Gbps ports are auto-MDI/MDI-X, which can be used on straight-through or crossover cable.

2.3.1 Installing the SFP Transceiver (TSN-5225-4T2S/TSN-900-2T2S only)

The sections describe how to insert an SFP transceiver into an SFP slot. The SFP transceivers are hot-pluggable and hot-swappable. You can plug in and out the transceiver to/from any SFP port without having to power down the **Industrial Managed TSN Device** as Figure 2-3-1 appears.

Note	**Follow all the SFP installation steps as shown in the example.**

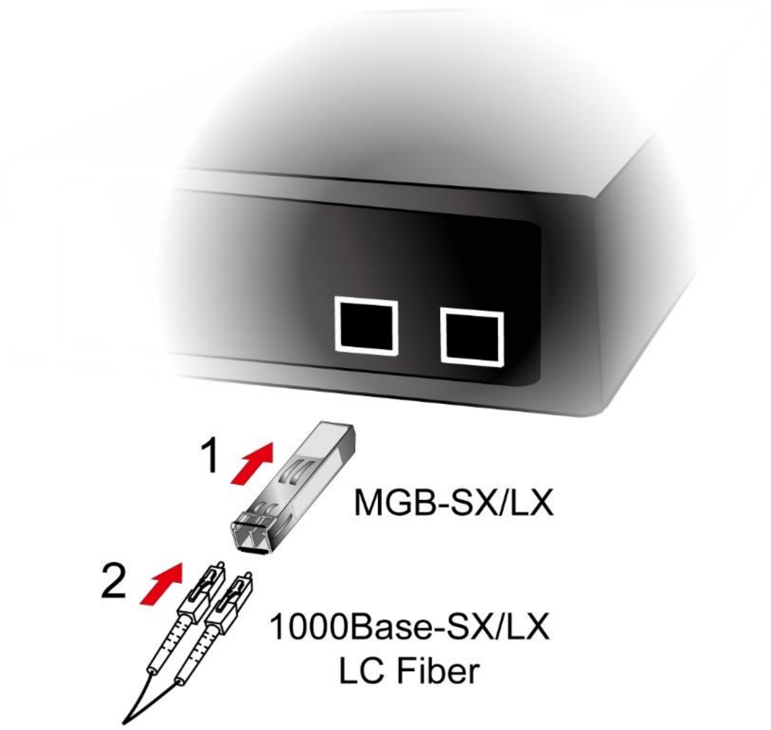


Figure 2-3-1: Plug in the SFP/SFP+ Transceiver

Approved PLANET SFP Transceivers

PLANET **Industrial Managed TSN Device** supports both single mode and multi-mode SFP transceivers. The following list of approved PLANET SFP transceivers is correct at the time of publication:

Gigabit Ethernet Transceiver (1000BASE-X SFP)

Model	Speed (Mbps)	Connector Interface	Fiber Mode	Distance	Wavelength (nm)	Operating Temp.
MGB-TSX	1000	LC	Multi Mode	550m	850nm	-40 ~ 85 degrees C
MGB-TLX	1000	LC	Single Mode	20km	1310nm	-40 ~ 85 degrees C
MGB-TL40	1000	LC	Single Mode	40km	1310nm	-40 ~ 85 degrees C
MGB-TL40	1000	LC	Single Mode	80km	1550nm	-40 ~ 85 degrees C

Gigabit Ethernet Transceiver (1000BASE-BX, Single Fiber Bi-directional SFP)

Model	Speed (Mbps)	Connector Interface	Fiber Mode	Distance	Wavelength (TX/RX)	Operating Temp.
MGB-TLA10	1000	WDM(LC)	Single Mode	10km	1310nm/1550nm	-40 ~ 85 degrees C
MGB-TLB10	1000	WDM(LC)	Single Mode	10km	1550nm/1310nm	-40 ~ 85 degrees C
MGB-TLA20	1000	WDM(LC)	Single Mode	20km	1310nm/1550nm	-40 ~ 85 degrees C
MGB-TLB20	1000	WDM(LC)	Single Mode	20km	1550nm/1310nm	-40 ~ 85 degrees C
MGB-TLA40	1000	WDM(LC)	Single Mode	40km	1310nm/1550nm	-40 ~ 85 degrees C
MGB-TLB40	1000	WDM(LC)	Single Mode	40km	1550nm/1310nm	-40 ~ 85 degrees C
MGB-TLA60	1000	WDM(LC)	Single Mode	60km	1310nm/1550nm	-40 ~ 85 degrees C
MGB-TLB60	1000	WDM(LC)	Single Mode	60km	1550nm/1310nm	-40 ~ 85 degrees C

2.5Gigabit Ethernet Transceiver (2500BASE-X SFP)

Model	Speed (Mbps)	Connector Interface	Fiber Mode	Distance	Wavelength (nm)	Operating Temp.
MGB-2GTSR	2488	LC	Multi Mode	300m	850nm	-40~85 degrees C
MGB-2GTLR2	2488	LC	Single Mode	2km	1310nm	-40~85 degrees C
MGB-2GTLR20	2488	LC	Single Mode	20km	1310nm	-40~85 degrees C
MGB-2GTLA20	2488	LC	Single Mode	20km	TX: 1310nm RX: 1550nm	-40~85 degrees C
MGB-2GTLB20	2488	LC	Single Mode	20km	TX: 1550nm RX:1310nm	-40~85 degrees C

Note

1. It is recommended to use PLANET SFP on the **Industrial Managed TSN Device**. If you insert an SFP transceiver that is not supported, the **Industrial Managed TSN Device** will not recognize it.
2. Please choose the SFP transceiver which can be operated at the temperature range of -40~85 degrees C if the **Industrial Managed TSN Device** is working in a -40~75 degrees C temperature environment.

1. Before we connect the **Industrial Managed TSN Device** to the other network device, we have to make sure both sides of the SFP transceivers are with the same media type, for example: 1000BASE-SX to 1000BASE-SX, 1000BASE-LX to 1000BASE-LX.
2. Check whether the fiber-optic cable type matches with the SFP transceiver requirement.
   - To connect to 1000BASE-SX SFP transceiver, please use the multi-mode fiber cable with one side being the male duplex LC connector type.
   - To connect to 1000BASE-LX SFP transceiver, please use the single-mode fiber cable with one side being the male duplex LC connector type.

- **Connect the fiber cable**

1. Insert the duplex LC connector into the SFP transceiver.
2. Connect the other end of the cable to a device with SFP transceiver installed.
3. Check the LNK/ACT LED of the SFP slot on the front of the Managed Switch. Ensure that the SFP transceiver is operating correctly.
4. Check the Link mode of the SFP port if the link fails. To function with some fiber-NICs or Media Converters, user has to set the port Link mode to **"1000M FDX"**.

2.3.2 Removing the SFP Transceiver

1. Make sure there is no network activity by consulting or checking with the network administrator. Or through the management interface of the switch/converter (if available) to disable the port in advance.
2. Remove the fiber optic cable gently.
3. Turn the lever of the SFP transceiver to a horizontal position.
4. Pull out the module gently through the lever.

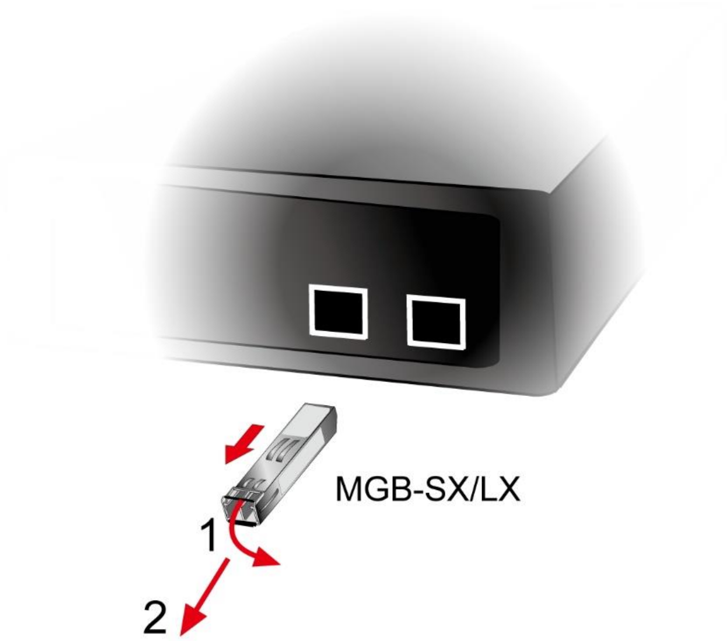


Figure 2-3-2: Pull out the SFP Transceiver Module

Note

Never pull out the module without pulling the lever or the push bolts on the module. Directly pulling out the module with force could damage the module and SFP module slot of the device.

3. SWITCH MANAGEMENT

This chapter explains the methods that you can use to configure management access to the **Industrial Managed TSN Device**. It describes the types of management applications and the communication and management protocols that deliver data between your management device (workstation or personal computer) and the system. It also contains information about port connection options.

This chapter covers the following topics:

- Requirements
- Management Access Overview
- Remote Telnet Access
- Web Management Access
- SNMP Access
- Standards, Protocols, and Related Reading

3.1 Requirements

- **Workstations** running Windows 7/8/10/11, macOS 10.12 or later, Linux Kernel 2.6.18 or later, or other modern operating systems that are compatible with TCP/IP Protocols.
- Workstations are installed with Ethernet NIC (Network Interface Card).
- **Serial Port Connection** (Terminal)
  - The above Workstations come with **COM Port** (DB9) or USB-to-RS232 converter.
  - The above Workstations have been installed with **terminal emulator**, such as putty or Tera Term.
  - **Serial cable** -- One end is attached to the RS232 serial port, while the other end to the **console port** of the Industrial Managed TSN Device.
- **Ethernet Port Connection**
  - **Network cables** -- Use standard network (UTP) cables with RJ45 connectors.
  - The above PC is installed with **Web browser**.

Note

It is recommended to use Google Chromeor above to access **Industrial Managed TSN Device**.

3.2 Management Access Overview

The **Industrial Managed TSN Device** gives you the flexibility to access and manage it using any or all of the following methods:

- Remote Telnet Interface
- **Web browser** Interface
- An external **SNMP-based network management application**

The remote Telnet and Web browser interfaces are embedded in the **Industrial Managed TSN Device** software and are available for immediate use. Each of these management methods has their own advantages. Table 3-2-1 compares the three management methods.

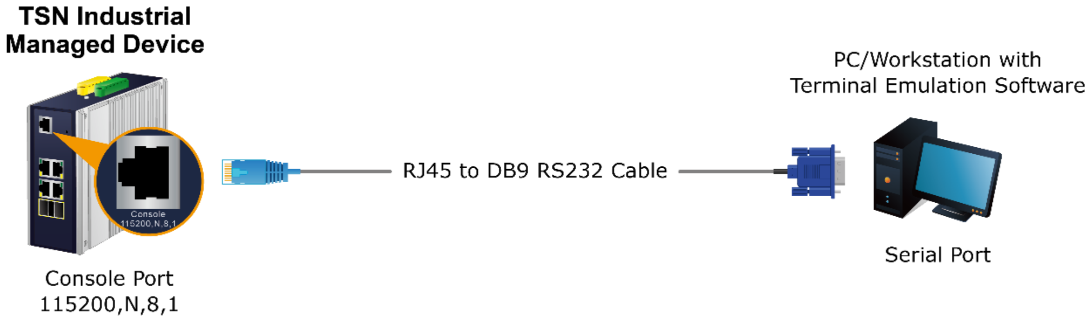
Method	Advantages	Disadvantages
Console	• No IP address or subnet needed • Text-based • Telnet functionality and HyperTerminal built into Windows 7/8/10/11 operating systems • ProComm Plus, putty, Tera term • Secure	• Must be near the switch or use dial-up connection • Not convenient for remote users • Modem connection may prove to be unreliable or slow
Remote Telnet	• Text-based • Telnet functionality built into Windows XP/2003, Vista, Windows 7/8/10/11 operating systems • Can be accessed from any location	• Security can be compromised (hackers need only know the IP address)
Web Browser	• Ideal for configuring the switch remotely • Compatible with all popular browsers • Can be accessed from any location • Most visually appealing	• Security can be compromised (hackers need only know the IP address and subnet mask) • May encounter lag times on poor connections
SNMP Agent	• Communicates with switch functions at the MIB level • Based on open standards	• Requires SNMP manager software • Least visually appealing of all three methods • Some settings require calculations • Security can be compromised (hackers need only know the community name)

Table 3-2-1: Management Methods Comparison

3.3 CLI Mode Management

There are two ways for CLI mode management, one is remote telnet and the other operated from console port. Remote telnet is an IP-based protocol and console port is for user to operate the Industrial Managed TSN Device locally only; however, their operations are the same.

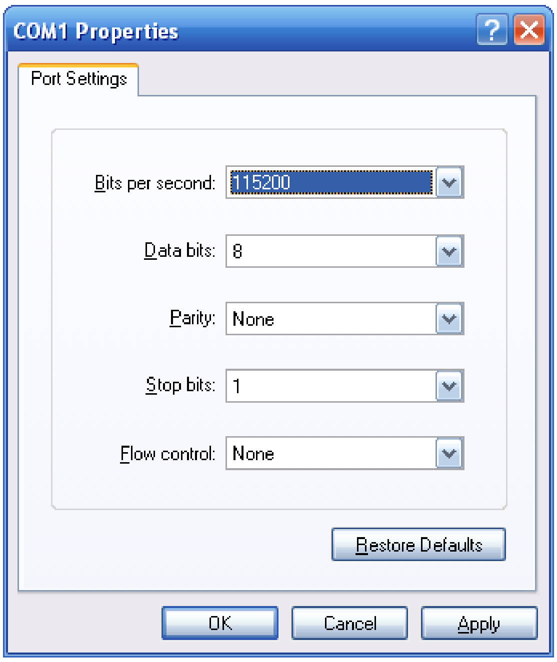
The command line user interface is for performing system administration, such as displaying statistics or changing option settings. When this method is used, you can access the **Industrial Managed TSN Device** remote telnet interface from personal computer or workstation in the same Ethernet environment as long as you know the current IP address of the **Industrial Managed TSN Device**.



Direct Access

Direct access to the administration console is achieved by directly connecting a terminal or a PC equipped with a terminal-emulation program (such as HyperTerminal, ProComm Plus, putty, Tera term) to the Managed Switch console (serial) port. When using this management method, a **straight DB9 RS-232 cable** is required to connect the switch to the PC. After making this connection, configure the terminal-emulation program to use the following parameters:
The default parameters are:

- **Baud: 115200**
- **Parity: None**
- **Data bits: 8**
- **Stop bits: 1**
- **Flow control: None**



You can change these settings, if desired, after you log on. This management method is often preferred because you can remain connected and monitor the system during system reboots. Also, certain error messages are sent to the serial port, regardless of the interface through which the associated action was initiated. A Macintosh or PC attachment can use any terminal-emulation program for connecting to the terminal serial port. A workstation attachment under UNIX can use an emulator.

3.3.1 Logging on to the Console

Once the terminal has been connected to the device, power on the **Industrial Managed TSN Device** and the terminal will display "running testing procedures".

Then, the following message asks to log in user name and password. The factory default user name and password are shown as follows.

User Name: **admin**
Password: **sw + the last 6 characters of the MAC ID in lowercase** (For TSN-5225-4T2S / TSN-5225-4T)
Password: **mc + the last 6 characters of the MAC ID in lowercase** (For TSN-900-2T2S)

Find the MAC ID on your device label. The default password is "sw" or "mc" followed by the last six lowercase characters of the MAC ID.

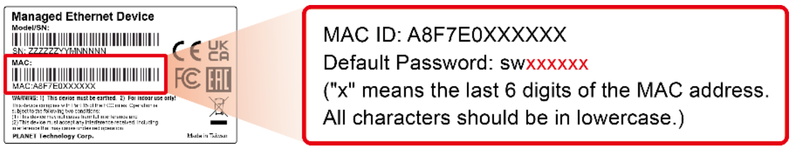


Figure 3-3-1: TSN-5225-4T MAC ID Label

Enter the default username and password, then set a new password according to the rule-based prompt and confirm it. Upon success, press any key to return to the login prompt. Log in with "admin" and the "new password" to access the CLI.

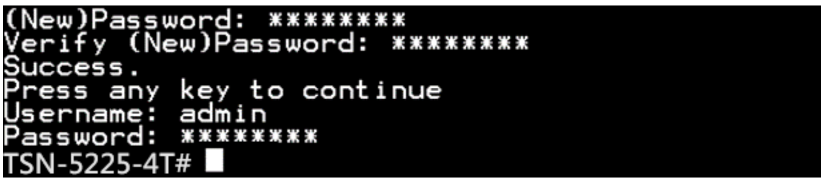


Figure 3-3-2: Create a New Password and Login Again

3.3.2 Remote Telnet

In Windows system, you may click **"Start"** and then choose **"Accessories"** and **"Command Prompt"**. Please input **"telnet 192.168.0.100"** and press **"enter'** from your keyboard. You will see the following screen appears as Figure 3-3-3 shows.

> **Note:** The following screen is based on the TSN-900-2T2S. The display of the other TSN Device is the same as that of the TSN-900-2T2S.

Figure 3-3-3: Remote Telnet Interface Main Screen of **Industrial Managed TSN Device**

3.4 Web Management

The **Industrial Managed TSN Device** offers management features that allow users to manage the **Industrial Managed TSN Device** from anywhere on the network through a standard browser such as Microsoft Google Chrome. After you set up your IP address for the **Industrial Managed TSN Device**, you can access the **Industrial Managed TSN Device**'s Web interface applications directly in your Web browser by entering the IP address of the **Industrial Managed TSN Device**.

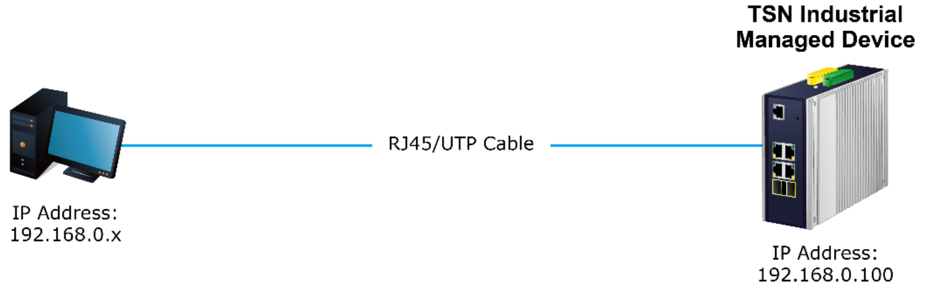


Figure 3-4-1: Web Management

You can then use your Web browser to list and manage the **Industrial Managed TSN Device** configuration parameters from one central location; the Web Management requires **Microsoft Google Chrome** or later.

Figure 3-4-1: Web Main Screen of **Industrial Managed TSN Device**

3.5 SNMP-based Network Management

You can use an external SNMP-based application to configure and manage the **Industrial Managed TSN Device**, such as SNMP Network Manager, HP Openview Network Node Management (NNM) or What's Up Gold. This management method requires the SNMP agent on the **Industrial Managed TSN Device** and the SNMP Network Management Station to use the **same community string**. This management method, in fact, uses two community strings: the **get community** string and the **set community** string.

If the SNMP Network Management Station only knows the set community string, it can read and write to the MIBs. However, if it only knows the get community string, it can only read MIBs. The default gets and sets community strings for the **Industrial Managed TSN Device** are public.

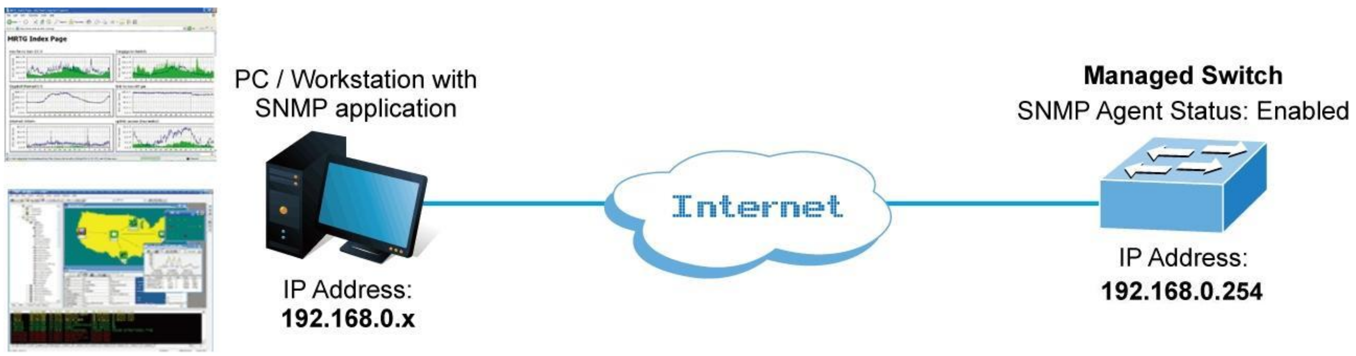


Figure 3-5-1: SNMP Management

3.6 PLANET Smart Discovery Utility

To easily list the **Industrial Managed TSN Device** in your Ethernet environment, the Planet Smart Discovery Utility from user's manual CD-ROM is an ideal solution. The following install instructions guide you to running the Planet Smart Discovery Utility.

1. Open the Planet Smart Discovery Utility in administrator PC.
2. Run this utility and the following screen appears.

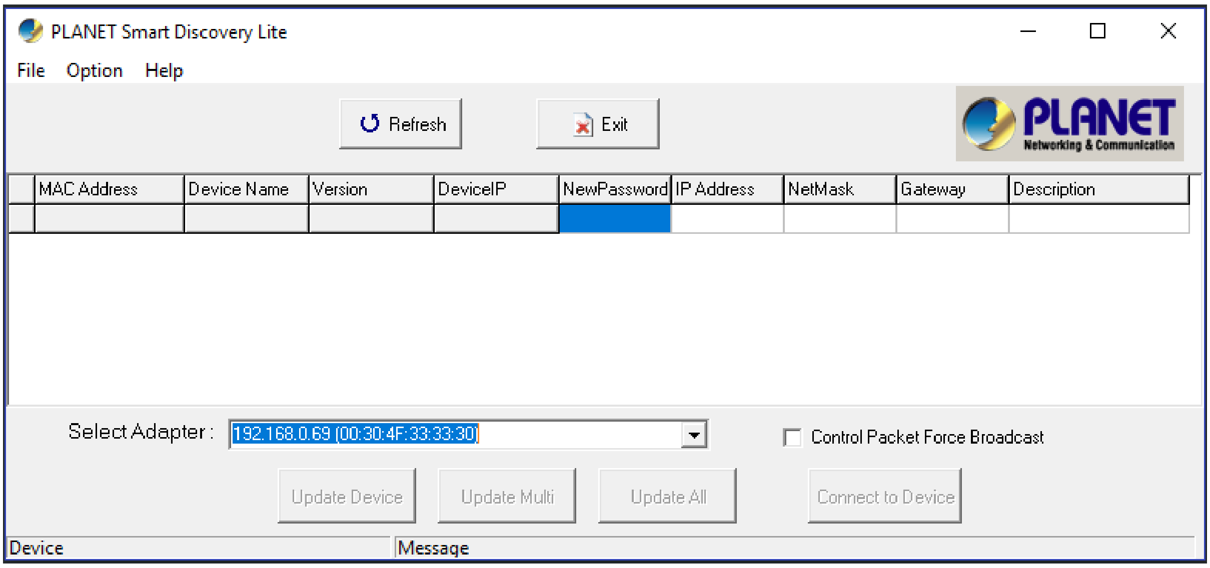


Figure 3-6-1: Planet Smart Discovery Utility Screen

Note

If there are two LAN cards or above in the same administrator PC, choose a different LAN card by using the **"Select Adapter"** tool.

3. Press the **"Refresh"** button for the currently connected devices in the discovery list as the screen is shown as follows.

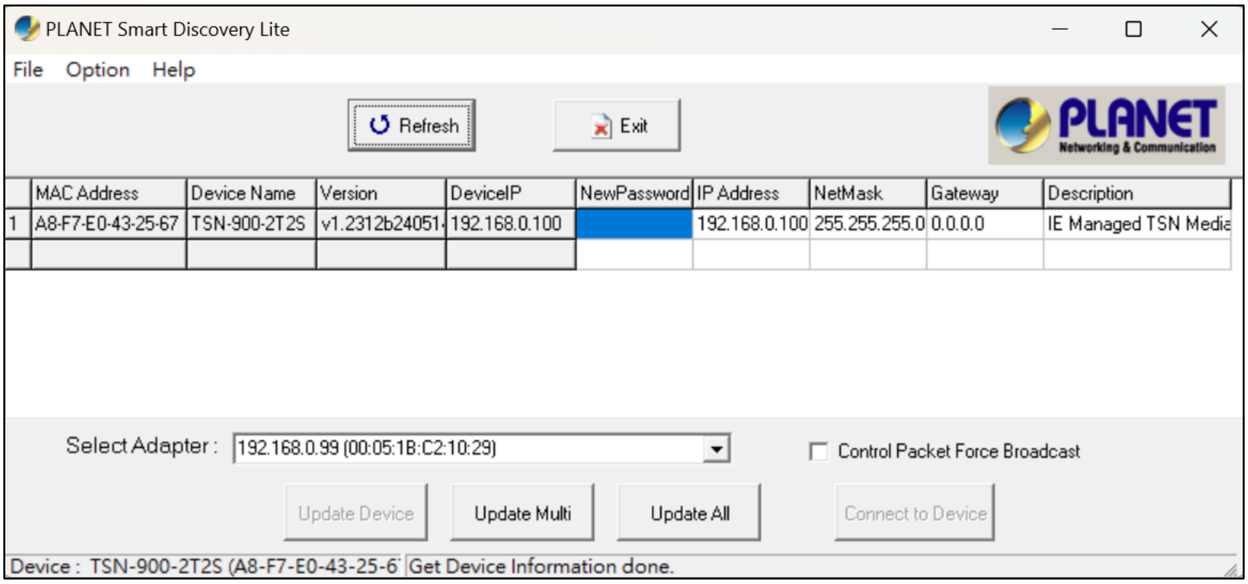


Figure 3-6-2: Planet Smart Discovery Utility Screen

1. This utility shows all the necessary information from the devices, such as MAC address, device name, firmware version and device IP subnet address. A new password, IP subnet address and description can be assigned to the devices.

2. After setup is completed, press the **"Update Device"**, **"Update Multi"** or **"Update All"** button to take effect. The functions of the 3 buttons above are shown below:
   - **Update Device**: Use the current setting on one single device.
   - **Update Multi:** Use the current setting on choose multi-devices.
   - **Update All:** Use the current setting on whole devices in the list.

   The same functions mentioned above also can be found in **"Option"** tools bar.

3. To click the **"Control Packet Force Broadcast"** function, it allows new setting value to be assigned to the Web Smart Switch under a different IP subnet address.

4. Press the **"Connect to Device"** button and then the Web login screen appears in Figure 4-2.

5. Press the **"Exit"** button to shut down Planet Smart Discovery Utility.

4. WEB CONFIGURATION

This section introduces the configuration and functions of the Web-based management.

About Web-based Management

The **Industrial Managed TSN Device** offers management features that allow users to manage the **Industrial Managed TSN Device** from anywhere on the network through a standard browser such as Microsoft Google Chrome

The Web-based Management supports Google Chrome. It is based on Java Applets with an aim to reducing network bandwidth consumption, enhancing access speed and presenting an easy viewing screen.

By default, IE7.0 or later version does not allow Java Applets to open sockets. The user has to explicitly modify the browser setting to enable Java Applets to use network ports.

The **Industrial Managed TSN Device** can be configured through an Ethernet connection, making sure the manager PC must be set to the same the IP subnet address as the **Industrial Managed TSN Device**. For example, the default IP address of the Industrial Managed TSN Device is 192.168.0.100, then the manager PC should be set to 192.168.0.x (where x is a number between 1 and 254, except 100), and the default subnet mask is 255.255.255.0.

If you have changed the default IP address of the **Industrial Managed TSN Device** to 192.168.1.1 with subnet mask 255.255.255.0 via console, then the manager PC should be set to 192.168.1.x (where x is a number between 2 and 254) to be able to do the related configuration on manager PC.

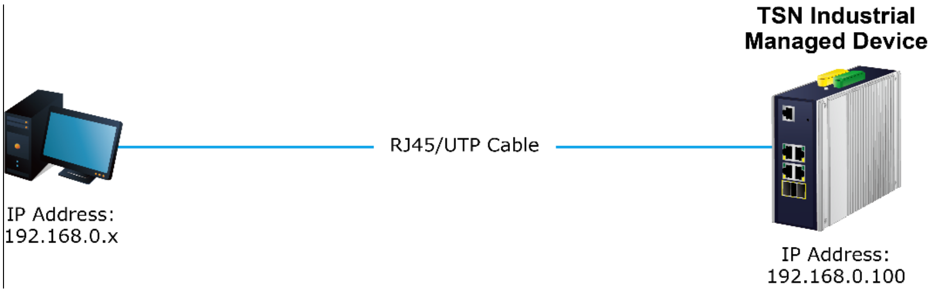


Figure 4-1: Web Management

- **Logging on to the Industrial Managed TSN Device**

1. Use Google Chrome or above Web browser. Enter the factory-default IP address to access the Web interface. The factory-default IP address is as follows:

http://192.168.0.100

2. When the following login screen appears, please enter the default username **"admin"** and password (Refer to **Section 3.3.1** to determine your initial login password.) to log in the main screen of **Industrial Managed TSN Device**. The login screen in Figure 4-2 appears.

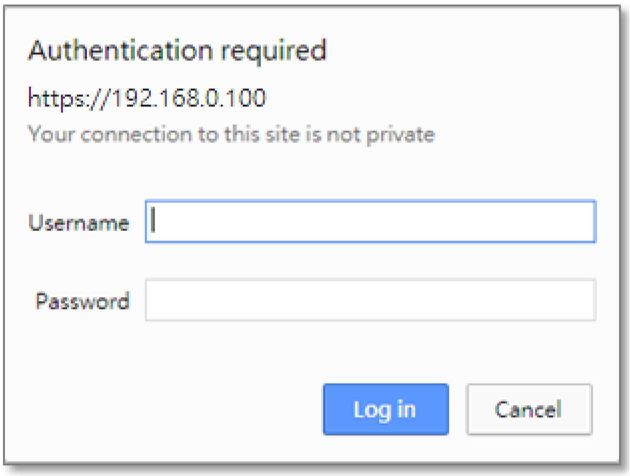


Figure 4-2: Login Screen

Default IP Address: **192.168.0.100**

Default User Name: **admin**

Default Password: **sw + the last 6 characters of the MAC ID in lowercase** (For TSN-5225-4T2S / TSN-5225-4T)

Default Password: **mc + the last 6 characters of the MAC ID in lowercase** (For TSN-900-2T2S)

Note: The following web screen is based on the TSN-900-2T2S. The display of the other TSN Device is the same as that of the TSN-900-2T2S.

After logging in, you will be prompted to change the initial password to a permanent one as Figure 4-3.

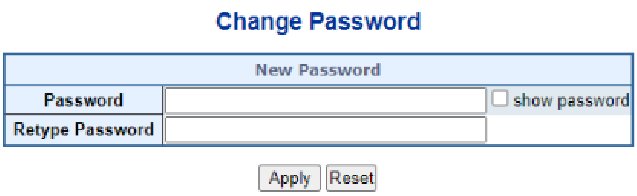


Figure 4-3: Create a New Password

Once the password change is complete, re-enter the web interface using your new password and the main screen appears as Figure 4-4 shows.

Figure 4-4: Default Main Page

Now, you can use the Web management interface to continue the switch management or manage the **Industrial Managed TSN Device** by Web interface. The Switch Menu on the left of the web page lets you access all the commands and statistics the Industrial Managed TSN Device provides.

1. It is recommended to use Google Chromeor above to access **Industrial Managed TSN Device**.
2. The changed IP address takes effect immediately after clicking on the **Save** button. From now on, you need to use the new IP address to access the Internet.

4.1 Main Web page

The **Industrial Managed TSN Device** provides a Web-based browser interface for configuring and managing it. This interface allows you to access the **Industrial Managed TSN Device** using the Web browser of your choice. This chapter describes how to use the **Industrial Managed TSN Device**'s Web browser interface to configure and manage it.

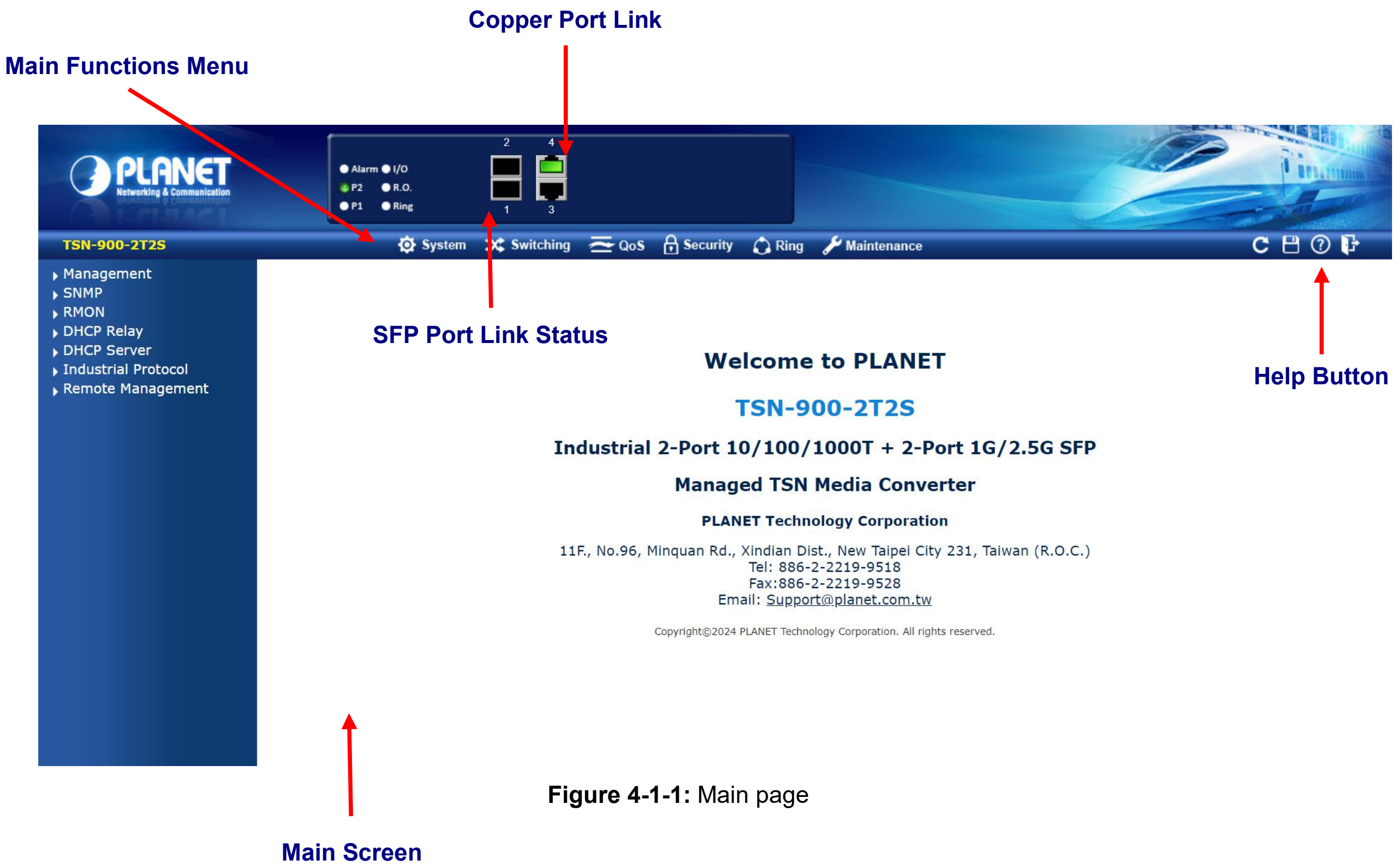


Figure 4-1-1: Main page

Panel Display

The web agent displays an image of the **Industrial Managed TSN Device**'s ports. The Mode can be set to display different information for the ports, including Link up or Link down. Clicking on the image of a port opens the **Port Statistics** page.

The port states are illustrated as follows:

State	Disabled	Down	Link
RJ45 Ports			
SFP Ports			

Main Menu

Using the onboard web agent, you can define system parameters, manage and control the **Industrial Managed TSN Device**, and all its ports, or monitor network conditions. The Main Menu always contains one or more buttons, such as **"System"**, **"Switching"**, **"Routing"**, **"QoS"**, **"Security"**, **"PoE"**, **"Ring"**, **"ONVIF"** and **"Maintenance"**

Via the Web-Management, the administrator can set up the **Industrial Managed TSN Device** by selecting the functions listed in the Main Function. The screen in Figure 4-1-2 appears.

Figure 4-1-2: Industrial Managed TSN Device Main Functions Menu

4.2 System

Use the System menu items to display and configure basic administrative details of the **Industrial Managed TSN Device**. Under the System, the following topics are provided to configure and view the system information. This section has the following items:

■ **System Information**	The **Industrial Managed TSN Device** system information is provided here.
■ **IP Configuration**	Configure the IPv4/IPv6 interface and IP routes of the **Industrial Managed TSN Device** on this page.
■ **IP Status**	This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IP routes and the neighbor cache (ARP cache) status.
■ **ARP**	The ARP is configured on this page. Set timeouts for entries in the ARP Table Configuration.
■ **Users Configuration**	This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser.
■ **Privilege Levels**	This page provides an overview of the privilege levels.
■ **NTP Configuration**	Configure NTP server on this page.
■ **Time Configuration**	Configure time parameter on this page.
■ **UPnP**	Configure UPnP on this page.
■ **DHCP Relay**	Configure DHCP Relay on this page.
■ **DHCP Relay Statistics**	This page provides statistics for DHCP relay.
■ **CPU Load**	This page displays the CPU load, using an SVG graph.
■ **System Log**	The system log information of the **Industrial Managed TSN Device** system is provided here.
■ **Detailed Log**	The detailed log information of the **Industrial Managed TSN Device** system is provided here.
■ **Remote Syslog**	Configure remote syslog on this page.
■ **SMTP Configuration**	Configure SMTP parameters on this page.
■ **Digital Input/Output**	Configure digital input and output on this page.
■ **Fault Alarm**	Configure fault alarm on this page.
■ **SNMP**	Configure SNMP parameters on this page
■ **RMON**	Configure the RMON parameters on this page
■ **DHCP server**	Configure the DHCP server on this page
■ **Industrial Protocol**	Configure the Modbus TCP Mode on this page
■ **Remote Management**	Configure the Remote NMS on this page

4.2.1 Management

4.2.1.1 System Information

The System Information page provides information for the current device information. System Information page helps a switch administrator to identify the hardware MAC address, software version and system uptime. The screen in Figure 4-2-1 appears.

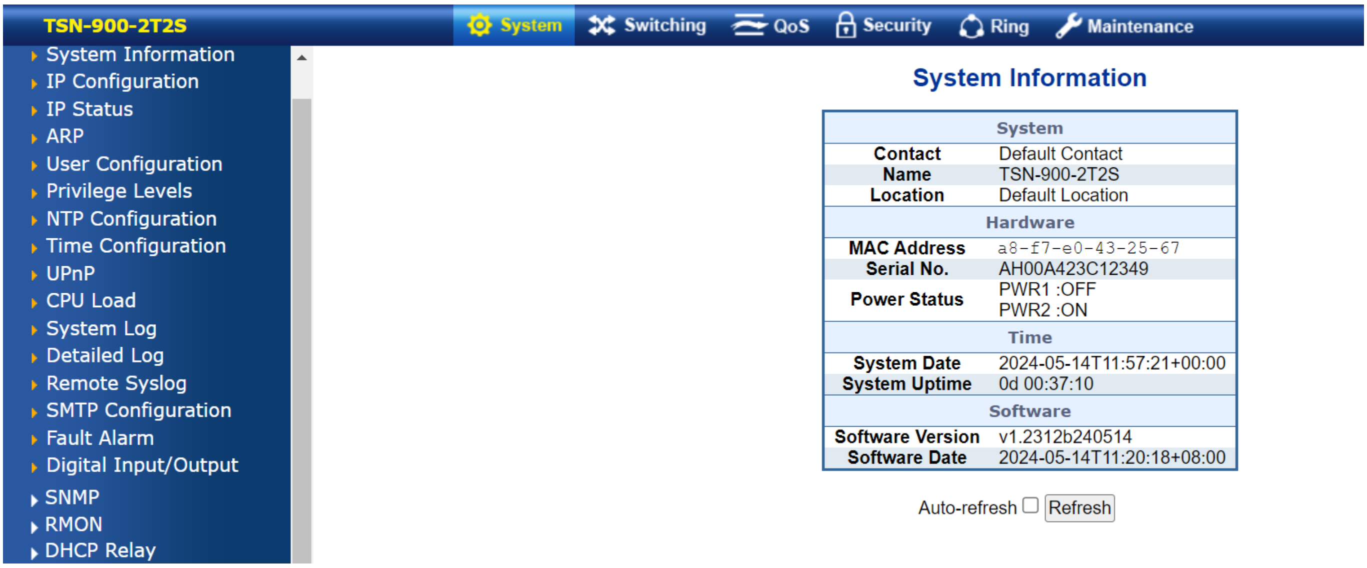


Figure 4-2-1: System Information Page Screenshot

The page includes the following fields:

Object	Description
• **Contact**	The system contact configured in SNMP | System Information | System Contact.
• **Name**	The system name configured in SNMP | System Information | System Name.
• **Location**	The system location configured in SNMP | System Information | System Location.
• **MAC Address**	The MAC Address of this **Industrial Managed TSN Device**.
• **Serial No.**	The Serial Number of this **Industrial Managed TSN Device**.
• **Power Status**	The status of power input
• **System Date**	The current (GMT) system time and date. The system time is obtained through the configured NTP Server, if any.
• **System Uptime**	The period of time the device has been operational.
• **Software Version**	The software version of the **Industrial Managed TSN Device**.
• **Software Date**	The date when the **Industrial Managed TSN Device** software was produced.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.2.1.2 IP Configuration

The IP Configuration includes the IP Configuration, IP Interface and IP Routes. The configured column is used to view or change the IP configuration. The maximum number of interfaces supported is 128 and the maximum number of routes is 128. The screen in Figure 4-2-2 appears.

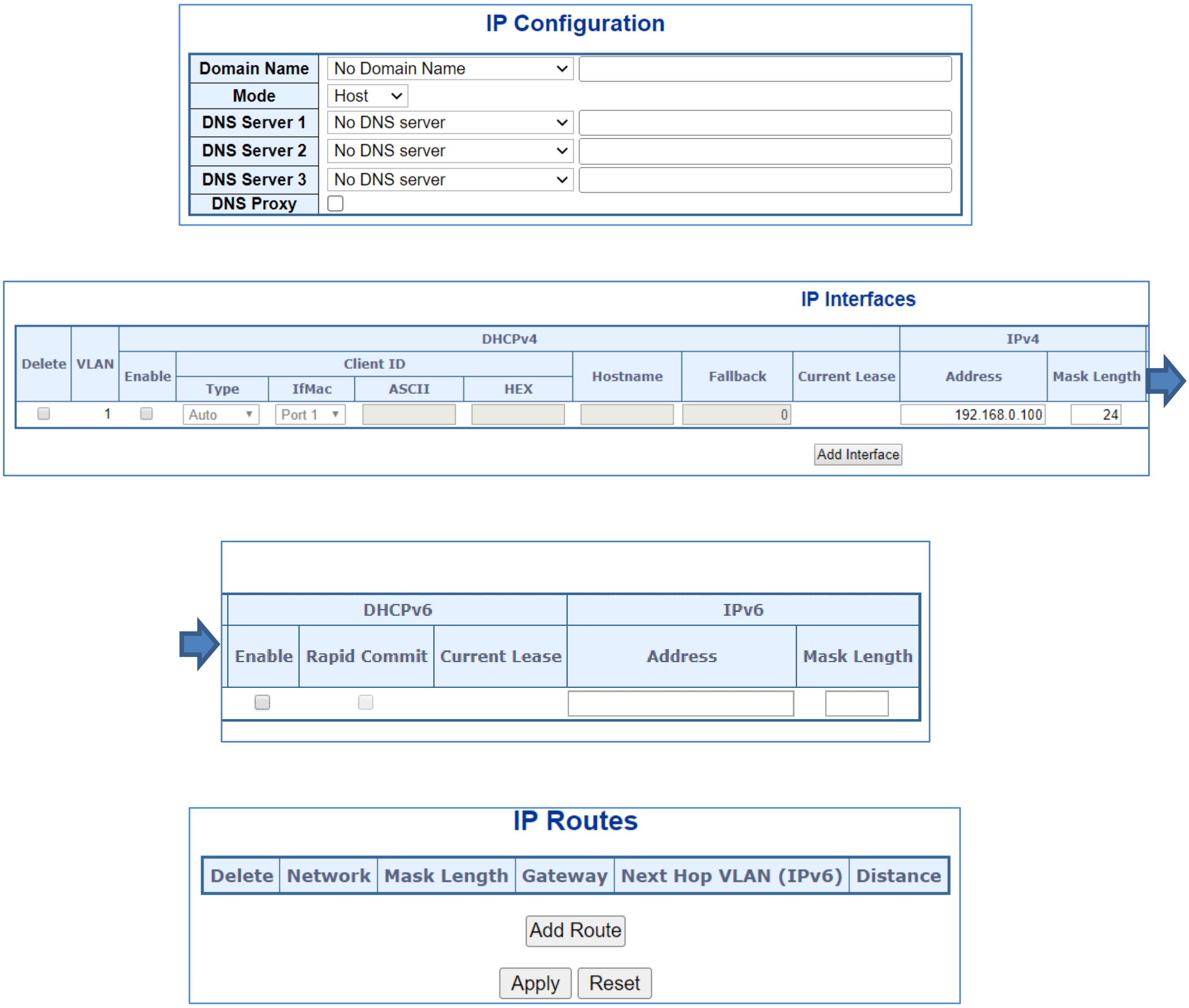


Figure 4-2-2: IP Configuration Page Screenshot

The current column is used to show the active IP configuration.

Object		Description
• **IP Configurations**	**Mode**	Configure whether the IP stack should act as a Host or a Router. In Host mode, IP traffic between interfaces will not be routed. In Router mode traffic is routed between all interfaces.
	DNS Server	This setting controls the DNS name resolution done by the switch. There are four servers available for configuration, and the index of the server presents the preference (less index has higher priority) in doing DNS name resolution. System selects the active DNS server from configuration in turn, if the preferred server does not respond in five attempts. The following modes are supported: ■ **No DNS server** No DNS server will be used. ■ **Configured IPv4** Explicitly provide the valid IPv4 unicast address of the DNS Server in dotted decimal notation. Make sure the configured DNS server could be reachable (e.g. via PING) for activating DNS service. ■ **Configured IPv6** Explicitly provide the valid IPv6 unicast (except link local) address of the DNS Server. Make sure the configured DNS server could be reachable (e.g. via PING6) for activating DNS service. ■ **From any DHCPv4 interfaces** The first DNS server offered from a DHCPv4 lease to a DHCPv4-enabled interface will be used. ■ **From this DHCPv4 interface** Specify from which DHCPv4-enabled interface a provided DNS server should be preferred. ■ **From any DHCPv6 interfaces** The first DNS server offered from a DHCPv6 lease to a DHCPv6-enabled interface will be used. ■ **From this DHCPv6 interface** Specify from which DHCPv6-enabled interface a provided DNS server should be preferred
	DNS Proxy	When DNS proxy is enabled, system will relay DNS requests to the

			currently configured DNS server, and reply as a DNS resolver to the client devices on the network.
• **IP Interface**	**Delete**		Select this option to delete an existing IP interface.
	VLAN		The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface.
	DHCPv4	**Enabled**	Enable the DHCPv4 client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCPv4 protocol. The DHCPv4 client will announce the configured System Name as hostname to provide DNS lookup.
		Fallback	The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables the fallback mechanism, such that DHCP will keep retrying until a valid lease is obtained. Legal values are 0 to 4294967295 seconds.
		Current Lease	For DHCP interfaces with an active lease, this column shows the current interface address, as provided by the DHCP server.
	IPv4	**Address**	The IPv4 address of the interface in dotted decimal notation. If DHCP is enabled, this field configures the fallback address. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.
		Mask Length	The IPv4 network mask, in number of bits (prefix length). Valid values are between 0 and 30 bits for an IPv4 address. If DHCP is enabled, this field configures the fallback address network mask. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.
	DHCPv6	**Enable**	Enable the DHCPv6 client by checking this box. If this option is enabled, the system will configure the IPv6 address of the interface using the DHCPv6 protocol.
		Rapid Commit	Enable the DHCPv6 Rapid-Commit option by checking this box. 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. This option is only manageable when DHCPv6 client is enabled.
		Current Lease	For DHCPv6 interface with an active lease, this column shows the interface address provided by the DHCPv6 server.
	IPv6	**Address**	The IPv6 address of the interface. An IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80::215:c5ff:fe03:4dc7. The symbol :: is a special syntax

			that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. System accepts the valid IPv6 unicast address only, except IPv4-Compatible address and IPv4-Mapped address. The field may be left blank if IPv6 operation on the interface is not desired.
		Mask Length	The IPv6 network mask, in number of bits (prefix length). Valid values are between 1 and 128 bits for an IPv6 address. The field may be left blank if IPv6 operation on the interface is not desired.
• **IP Routes**	**Delete**		Select this option to delete an existing IP route.
	Network		The destination IP network or host address of this route. Valid format is dotted decimal notation or a valid IPv6 notation. A default route can use the value **0.0.0.0** or IPv6 **::** notation.
	Mask Length		The destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, in order to qualify for this route. Valid values are between 0 and 32 bits respectively 128 for IPv6 routes. Only a default route will have a mask length of 0 (as it will match anything).
	Gateway		The IP address of the IP gateway. Valid format is dotted decimal notation or a valid IPv6 notation. Gateway and Network must be of the same type.
	Next Hop VLAN		The VLAN ID (VID) of the specific IPv6 interface associated with the gateway. The given VID ranges from 1 to 4095 and will be effective only when the corresponding IPv6 interface is valid. If the IPv6 gateway address is link-local, it must specify the next hop.
	Distance		The distance value of the route entry is used to provide the priority information of the routing protocols to routers. When two or more different routing protocols are involved and have the same destination, the distance value can be used to select the best path.

Buttons

Add Interface: Click to add a new IP interface. A maximum of 128 interfaces are supported.

Add Route: Click to add a new IP route. A maximum of 32 routes are supported.

Apply: Click to apply changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.2.1.3 IP Status

IP Status displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IP routes and the neighbor cache (ARP cache) status. The screen in Figure 4-2-3 appears.

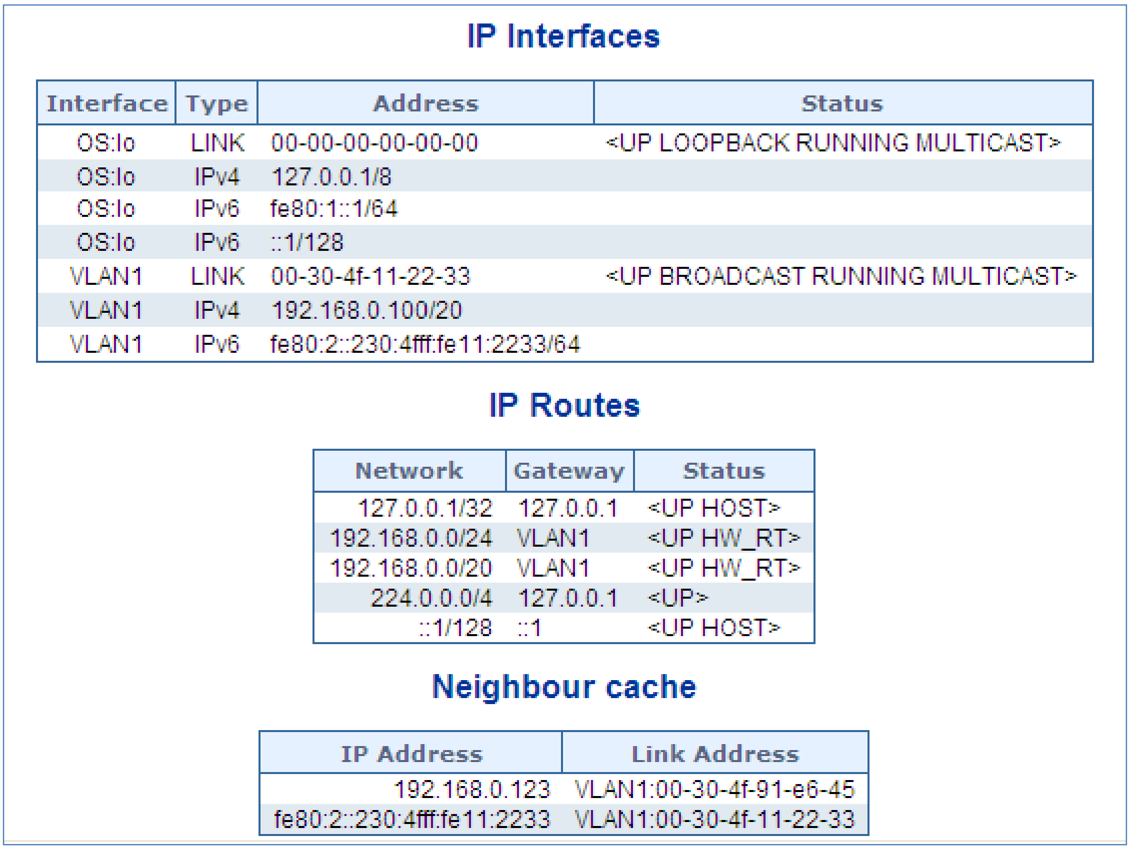


Figure 4-2-3: IP Status Page Screenshot

The page includes the following fields:

Object		Description
• **IP Interfaces**	**Interface**	The name of the interface.
	Type	The address type of the entry. This may be **LINK** or **IPv4**.
	Address	The current address of the interface (of the given type).
	Status	The status flags of the interface (and/or address).
• **IP Routes**	**Network**	The destination IP network or host address of this route.
	Gateway	The gateway address of this route.
	Status	The status flags of the route.
• **Neighbor Cache**	**IP Address**	The IP address of the entry.
	Link Address	The Link (MAC) address for which a binding to the IP address given exists.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

4.2.1.4 ARP

This page provides ARP configuration settings. press the "Apply" button to take effect, the screen in below appears.

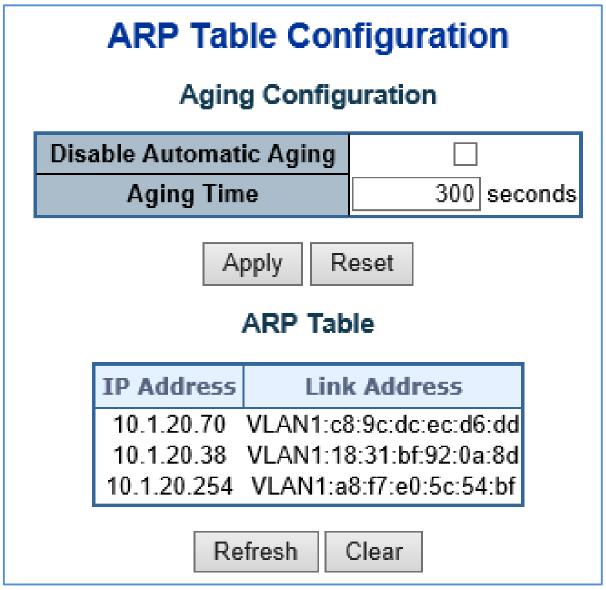


Figure 4-2-4: ARP Table Configuration Page Screenshot

The page includes the following fields:

Object		Description
• **Aging Configuration**	**Disable Automatic Aging**	Allow to click to disable the automatic aging.
	Aning Time	Allow to change the aging time settings and the available range is 10 to 1000000 seconds.
• **ARP Table**	**IP Address**	Display the IP address.
	Link Address	Display the VLAN and MAC address information.

Buttons

: Click to refresh the page.

: Clears all statistics.

4.2.1.5 Users Configuration

This page provides an overview of the current users. Currently the only way to log in as another user on the web server is to close and reopen the browser. After setup is completed, press the **"Apply"** button to take effect. Please login web interface with new user name and password; the screen in Figure 4-2-5 appears.

Figure 4-2-5 Users Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **User Name**	The name identifying the user. This is also a link to Add/Edit User.
• **Privilege Level**	The privilege level of the user. The allowed range is **0** to **15**. If the privilege level value is 15, it can access all groups, i.e. that is granted the full control of the device. But other values need to refer to each group privilege level. User's privilege should be the same or greater than the group privilege level to have the access to that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) needs user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

Buttons

: Click to add a new user.

Add / Edit User

This page configures a user – add, edit or delete user.

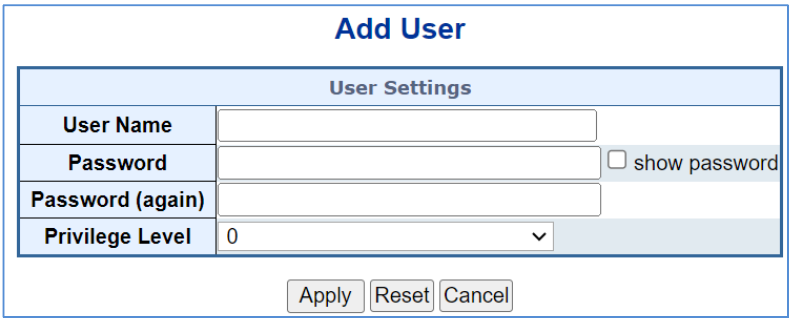


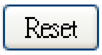
Figure 4-2-6: Add / Edit User Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Username**	A string identifying the user name that this entry should belong to. The allowed string length is **1** to **31**. The valid user name is a combination of letters, numbers and underscores.
• **Password**	The password of the user. The password must contain 8-31 characters, including upper case, lower case, numerals and other symbols. Please note, spaces (blanks) are not accepted.
• **Password (again)**	Please enter the user’s new password here again to confirm.
• **Privilege Level**	The privilege level of the user. The allowed range is **0** to **15**. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) needs user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

Buttons

: Click to apply changes.



: Click to undo any changes made locally and revert to previously saved values.

: Click to undo any changes made locally and return to the Users.

: Delete the current user. This button is not available for new configurations (Add new user).

Once the new user is added, the new user entry is shown on the Users Configuration page.

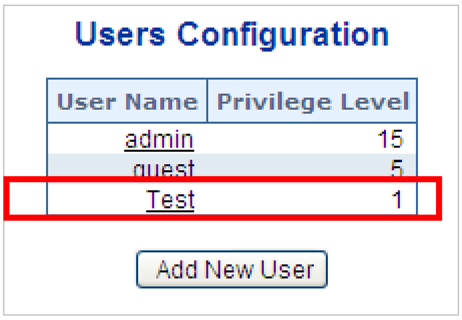


Figure 4-2-7: User Configuration Page Screenshot

If you forget the new password after changing the default password, please press the ***“Reset”*** button on the front panel of the Industrial Managed TSN Device for over 10 seconds and then release it. The current setting including VLAN will be lost and the Industrial Managed TSN Device will restore to the default mode.

4.2.1.6 Privilege Levels

This page provides an overview of the privilege levels. After setup is completed, please press the **"Apply"** button to take effect. Please log in web interface with new user name and password and the screen in Figure 4-2-8 appears.

Privilege Level Configuration

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
APS	5	10	5	10
CFM	5	10	5	10
DDMI	5	10	5	10
Debug	15	15	15	15
DHCP	5	10	5	10
DHCPv6_Client	5	10	5	10
Diagnostics	5	10	5	10
DIDO	5	10	5	10
eip	5	10	5	10
ERPS	5	10	5	10
ETH_LINK_OAM	5	10	5	10
Firmware	5	10	5	10
IP	5	10	5	10
IP8008	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10

Miscellaneous	15	15	15	15
modbus_tcp	5	10	5	10
MQTT	5	10	5	10
MRP	5	10	5	10
MVR	5	10	5	10
NTP	5	10	5	10
Ports	5	10	1	10
Private_VLANs	5	10	5	10
PTP	5	10	5	10
QoS	5	10	5	10
RMirror	5	10	5	10
Security(access)	10	10	5	10
Security(network)	5	10	5	10
sFlow	5	10	5	10
Spanning_Tree	5	10	5	10
System	5	10	1	10
UDLD	5	10	5	10
uFDMA_AIL	5	10	5	10
uFDMA_CIL	5	10	5	10
UPnP	5	10	5	10
VCL	5	10	5	10
VLAN_Translation	5	10	5	10
VLANs	5	10	5	10
Voice_VLAN	5	10	5	10
XXRP	5	10	5	10

Figure 4-2-8: Privilege Levels Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Group Name**	The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contain more than one. The following description defines these privilege level groups in details: ■ **System**: Contact, Name, Location, Timezone, Log. ■ **Security**: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection and IP source guard. ■ **IP**: Everything except 'ping'. ■ **Port**: Everything except 'VeriPHY'. ■ **Diagnostics**: 'ping' and 'VeriPHY'. ■ **Maintenance**: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance. ■ **Debug**: Only present in CLI.
• **Privilege Level**	Every privilege level group has an authorization level for the following sub groups: ■ **Configuration read-only** ■ **Configuration/execute read-write** ■ **Status/statistics read-only** ■ **Status/statistics read-write** (e.g. for clearing of statistics). User Privilege should be same or greater than the authorization Privilege level to have the access to that group.

Buttons

Apply: Click to apply changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.2.1.7 NTP Configuration

Configure NTP on this page. **NTP** is an acronym for **Network Time Protocol**, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (data grams) as transport layer. You can specify NTP Servers. The NTP Configuration screen in Figure 4-2-9 appears.

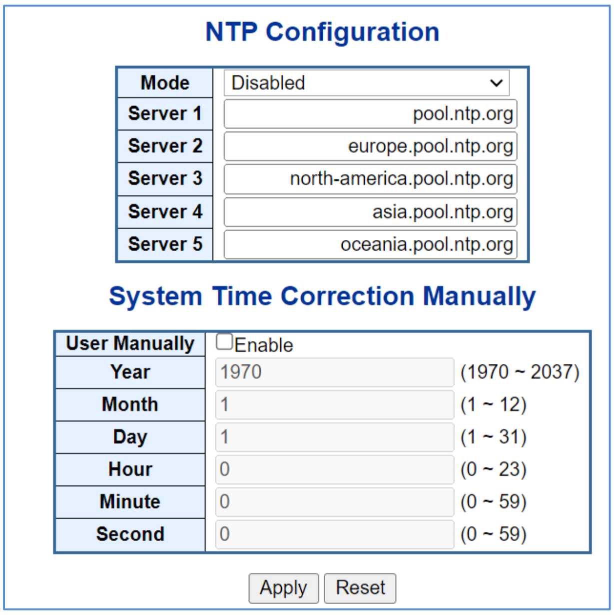


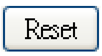
Figure 4-2-9: NTP Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	Indicates the NTP mode operation. Possible modes are: ■ **Enabled**: Enable NTP mode operation. When enabling NTP mode operation, the agent forward and transfer NTP messages between the clients and the server when they are not on the same subnet domain. ■ **Disabled**: Disable NTP mode operation.
• **Server #**	Provide the NTP IPv4 or IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros, but it can only appear once. It also uses a legal IPv4 address like '::192.1.2.34'.

Buttons

: Click to apply changes.



: Click to undo any changes made locally and revert to previously saved values.

4.2.1.8 Time Configuration

This page allows you to configure the Time Zone. Time Zone Configuration screen in Figure 4-2-10 and Figure 4-2-11 appears.

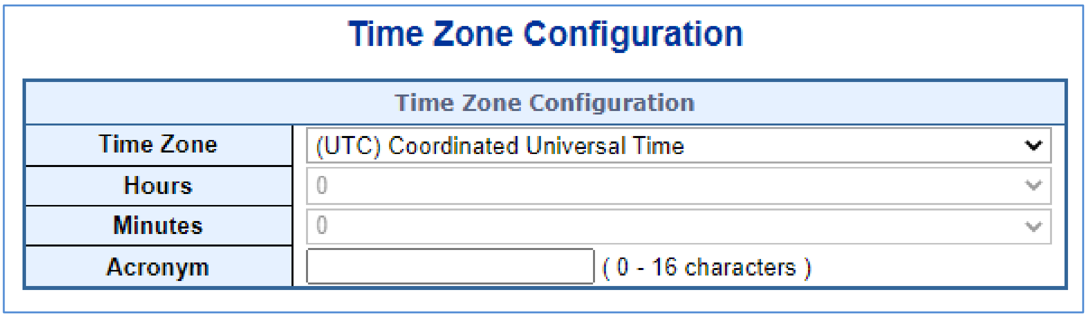


Figure 4-2-10: System Time Correction Manually Page Screenshot

The page includes the following fields:

Object	Description
• **Time Zone**	Lists various Time Zones world wide. Select appropriate Time Zone from the drop down and click Save to set. The 'Manual Setting' options is used for the specific time zone which is excluded from the options list.
• **Hours**	Number of hours offset from UTC. The field only available when time zone manual setting
• **Minutes**	Number of minutes offset from UTC. The field only available when time zone manual setting
• **Acronym**	User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. (Range : Up to 16 characters) Notice the string '' is a special syntax that is reserved for null input

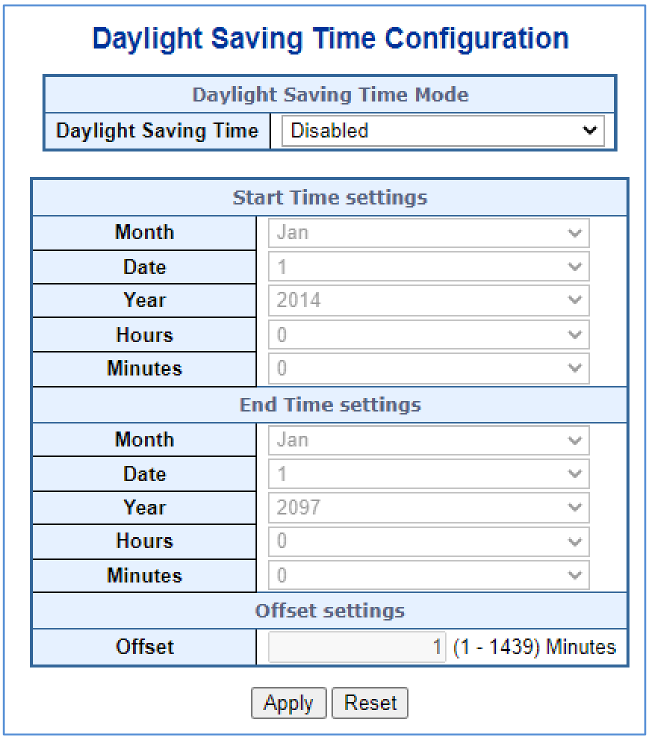


Figure 4-2-11: System Time Correction Manually Page Screenshot

Daylight Saving Time Configuration

The page includes the following fields:

Object	Description
• **Daylight Saving Time Configuration**	• **Daylight Saving Time** - This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select 'Disable' to disable the Daylight Saving Time configuration. Select 'Recurring' and configure the Daylight Saving Time duration to repeat the configuration every year. Select 'Non-Recurring' and configure the Daylight Saving Time duration for single time configuration. (Default : Disabled)
Recurring Configurations	
• **Start time settings**	• **Week** - Select the starting week number. • **Day** - Select the starting day. • **Month** - Select the starting month. • **Hours** - Select the starting hour. • **Minutes** - Select the starting minute.
• **End time settings**	• **Week** - Select the ending week number. • **Day** - Select the ending day. • **Month** - Select the ending month. • **Hours** - Select the ending hour. • **Minutes** - Select the ending minute.
• **Offset settings**	• **Offset** - Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1439)
Non Recurring Configurations	
• **Start time settings**	• **Month** - Select the starting month. • **Date** - Select the starting date. • **Year** - Select the starting year. • **Hours** - Select the starting hour. • **Minutes** - Select the starting minute.
• **End time settings**	• **Month** - Select the ending month. • **Date** - Select the ending date. • **Year** - Select the ending year. • **Hours** - Select the ending hour. • **Minutes** - Select the ending minute.
• **Offset settings**	• **Offset** - Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1439)

Buttons

Apply : Click to apply changes.

Reset : Click to undo any changes made locally and revert to previously saved values.

4.2.1.9 UPnP

Configure UPnP on this page. UPnP is an acronym for **Universal Plug and Play**. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components. The UPnP Configuration screen in Figure 4-2-12 appears.

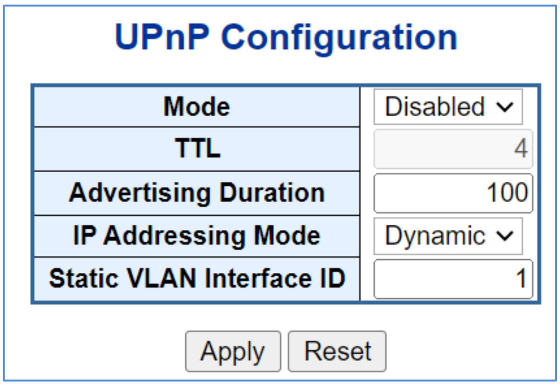
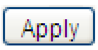


Figure 4-2-12: UPnP Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	Indicates the UPnP operation mode. Possible modes are: ■ **Enabled**: Enable UPnP mode operation. ■ **Disabled**: Disable UPnP mode operation. When the mode is enabled, two ACEs are added automatically to trap UPnP related packets to CPU. The ACEs are automatically removed when the mode is disabled.
• **TTL**	The TTL value is used by UPnP to send SSDP advertisement messages. Read only now.
• **Advertising Duration**	The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive a SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it will think that the switch no longer exists. Due to the unreliable nature of UDP, in the standard it is recommended that such refreshing of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are in the range 100 to 86400.
• **IP Addressing Mode**	IP addressing mode provides two ways to determine IP address assignment: **Dynamic**: Default selection for UPnP. UPnP module helps users choosing the IP address of the switch device. It finds the first available system IP address. **Static**: User specifies the IP interface VLAN for choosing the IP address of the switch device.
• **Static VLAN Interface ID**	The index of the specific IP VLAN interface. It will only be applied when IP Addressing Mode is static. Valid configurable values ranges from 1 to 4095. Default value is 1.

Buttons



: Click to apply changes

: Click to undo any changes made locally and revert to previously saved values.

4.2.1.10 CPU Load

This page displays the CPU load, using an SVG graph. The load is measured as average over the last 100ms, 1 sec and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well. In order to display the SVG graph, your browser must support the SVG format. Consult the SVG Wiki for more information on browser support. Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plugin installed to support SVG. The CPU Load screen in Figure 4-2-13 appears.

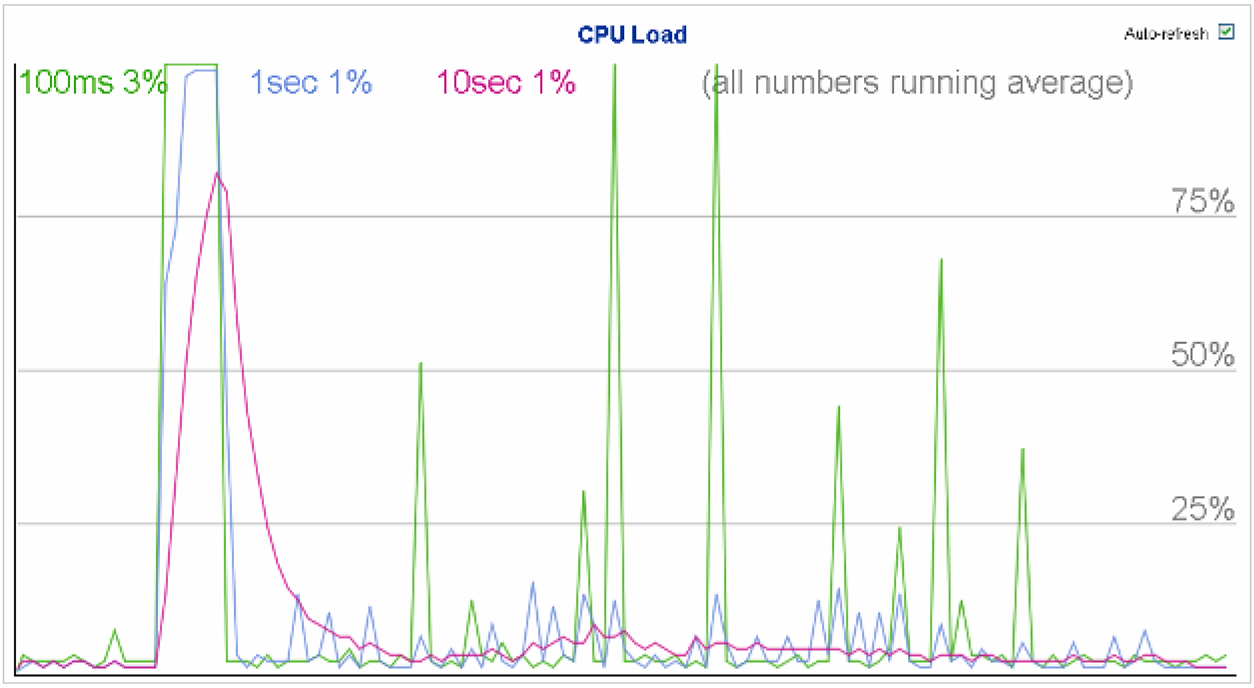


Figure 4-2-13: CPU Load Page Screenshot

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Note

If your browser cannot display anything on this page, please download Adobe SVG tool and install it in your computer.

4.2.1.11 System Log

The Managed Switch system log information is provided here. The System Log screen in Figure 4-2-14 appears.

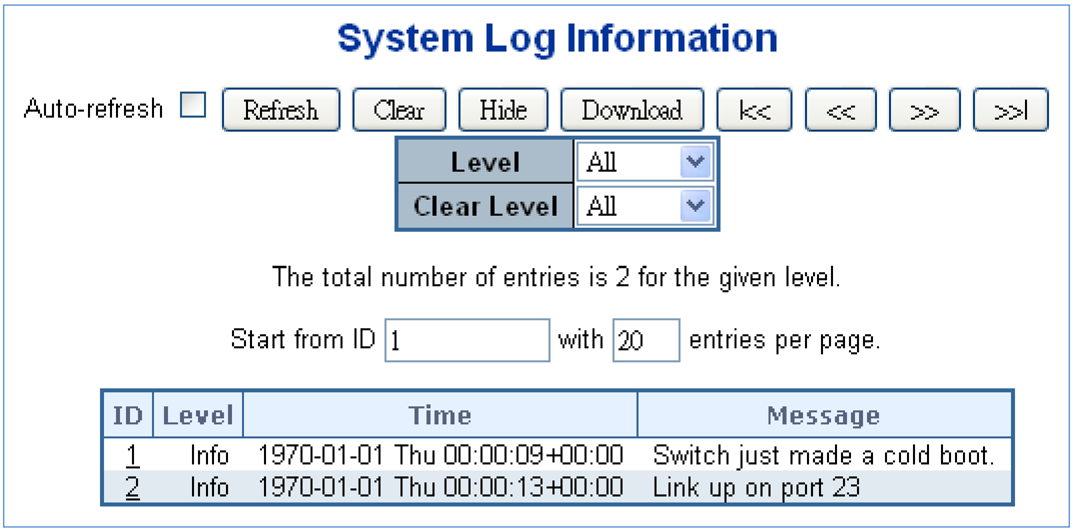


Figure 4-2-14: System Log Page Screenshot

The page includes the following fields:

Object	Description
• **ID**	The ID (>= 1) of the system log entry.
• **Level**	The level of the system log entry. The following level types are supported: ■ **Info**: Information level of the system log. ■ **Warning**: Warning level of the system log. ■ **Error**: Error level of the system log. ■ **All**: All levels.
• **Clear Level**	To clear the system log entry level. The following level types are supported: ■ **Info**: Information level of the system log. ■ **Warning**: Warning level of the system log. ■ **Error**: Error level of the system log. ■ **All**: All levels.
• **Time**	The time of the system log entry.
• **Message**	The message of the system log entry.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Updates the system log entries, starting from the current entry ID.

Clear: Flushes the selected log entries.

Hide: Hides the selected log entries.

Download: Downloads the selected log entries.

|<<: Updates the system log entries, starting from the first available entry ID.

<<: Updates the system log entries, ending at the last entry currently displayed.

>>: Updates the system log entries, starting from the last entry currently displayed.

>>|: Updates the system log entries, ending at the last available entry ID.

4.2.1.12 Detailed Log

The Managed Switch system detailed log information is provided here. The Detailed Log screen in Figure 4-2-15 appears.

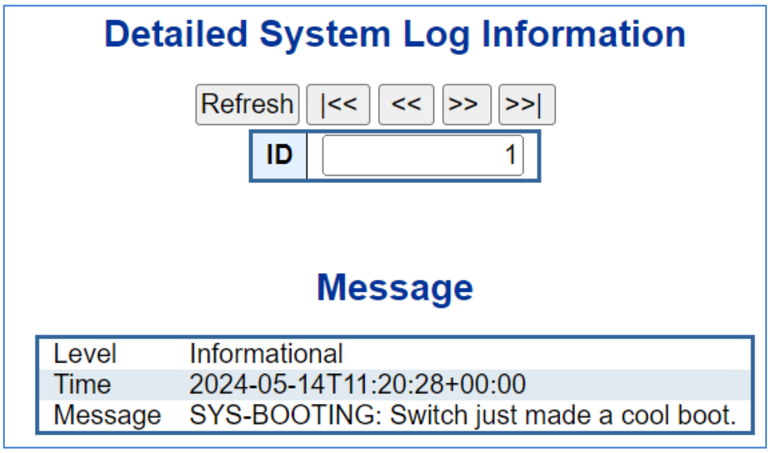


Figure 4-2-15: Detailed Log Page Screenshot

The page includes the following fields:

Object	Description
• **Level**	The severity level of the system log entry.
• **ID**	The ID (>= 1) of the system log entry.
• **Message**	The message of the system log entry.

Buttons

Refresh: Updates the system log entry to the current entry ID.

|<<: Updates the system log entry to the first available entry ID.

<<: Updates the system log entry to the previous available entry ID.

>>: Updates the system log entry to the next available entry ID.

>>|: Updates the system log entry to the last available entry ID.

Print: Print the system log entry to the current entry ID.

4.2.1.13 Remote Syslog

Configure remote syslog on this page. The Remote Syslog screen in Figure 4-2-16 appears.

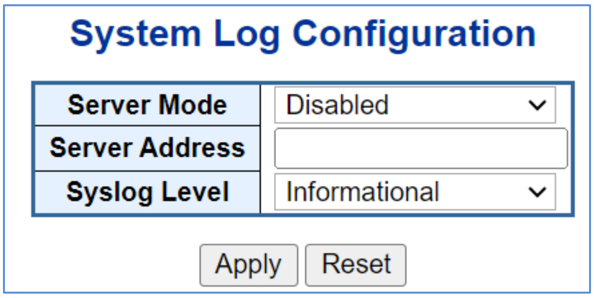


Figure 4-2-16: Remote Syslog Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist. Possible modes are: ■ **Enabled**: Enable remote syslog mode operation. ■ **Disabled**: Disable remote syslog mode operation.
• **Syslog Server IP**	Indicates the IPv4 host address of syslog server. If the switch provides DNS feature, it also can be a host name.
• **Syslog Level**	Indicates what kind of message will send to syslog server. Possible modes are: ■ **Info**: Send information, warnings and errors. ■ **Warning**: Send warnings and errors. ■ **Error**: Send errors.

Buttons

: Click to apply changes

: Click to undo any changes made locally and revert to previously saved values.

4.2.1.14 SMTP Configuration

This page facilitates an SMTP Configuration on the switch. The SMTP Configure screen in Figure 4-2-17 appears.

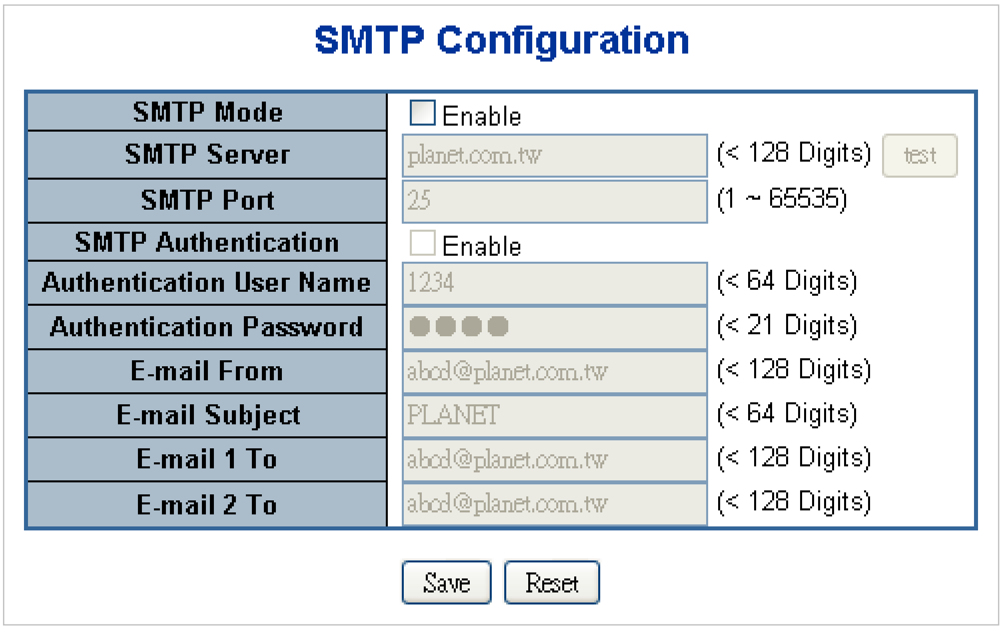


Figure 4-2-17: SMTP Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **SMTP Mode**	Controls whether SMTP is enabled on this switch.
• **SMTP Server**	Type the SMTP server name or the IP address of the SMTP server.
• **SMTP Port**	Set port number of SMTP service.
• **SMTP Authentication**	Controls whether SMTP authentication is enabled if authentication is required when an e-mail is sent.
• **Authentication User Name**	Type the user name for the SMTP server if Authentication is Enabled.
• **Authentication Password**	Type the password for the SMTP server if Authentication is Enabled.
• **E-mail From**	Type the sender's e-mail address. This address is used for reply e-mails.
• **E-mail Subject**	Type the subject/title of the e-mail.
• **E-mail 1 To**	Type the receiver's e-mail address.
• **E-mail 2 To**	

Buttons

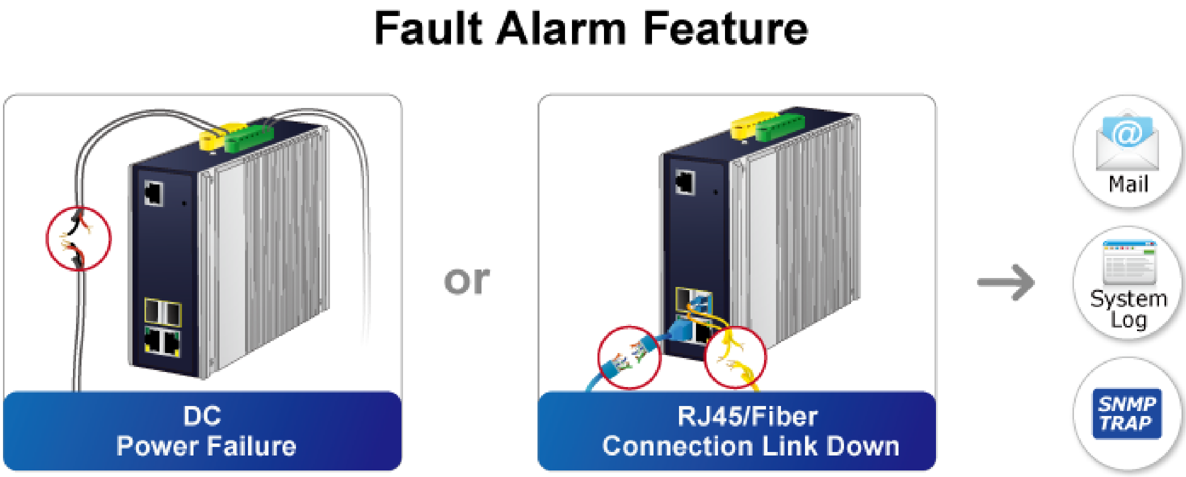
: Send a test mail to mail server to check whether this account is available or not.

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

4.2.1.15 Fault Alarm

The Industrial Managed TSN Device supports a Fault Alarm feature which can alert the users when there is something wrong with the switches. With this ideal feature, the users would not have to waste time finding where the problem is. It will help to save time and human resource.



The Fault Alarm screen in Figure 4-2-18 appears.

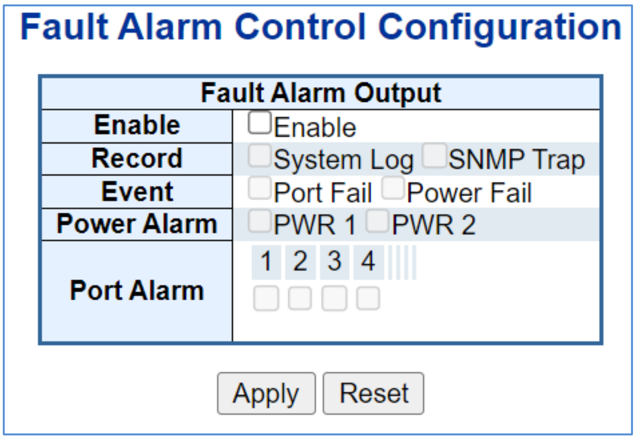


Figure 4-2-18: Fault Alarm Control Configuration page Screenshot

The page includes the following fields:

Object	Description
• **Enable**	Controls whether Fault Alarm is enabled on this switch.
• **Record**	Controls whether Record is sending System log or SNMP Trap or both.
• **Action**	Controls whether Port Fail or Power Fail or both for fault detecting.
• **Power Alarm**	Controls whether AC, DC1 or DC2 or both for fault detecting.
• **Port Alarm**	Controls which Ports or all for fault detecting.

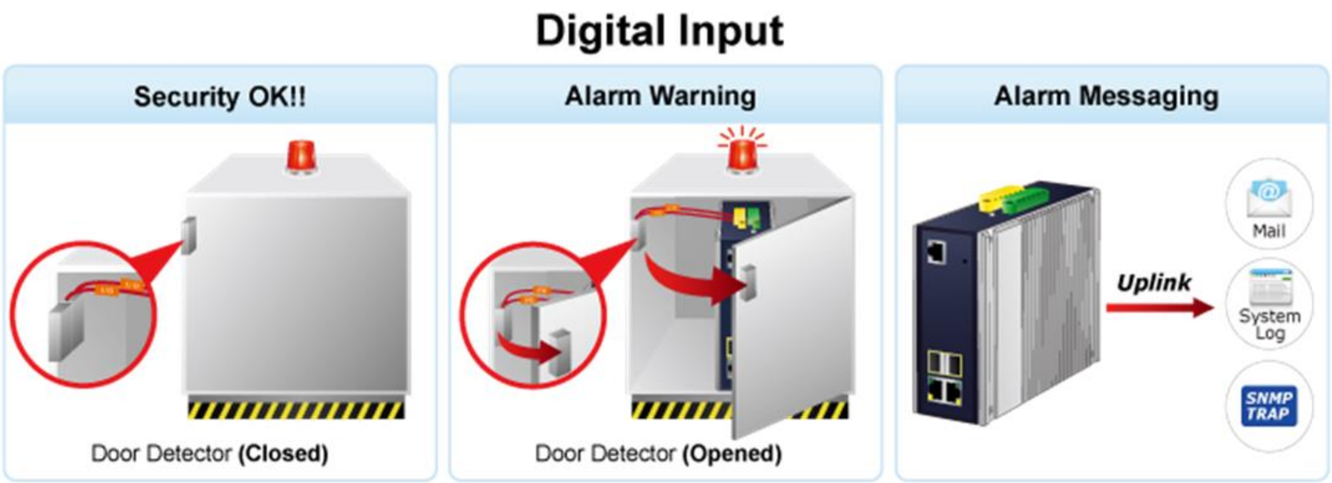
Buttons

Apply : Click to apply changes

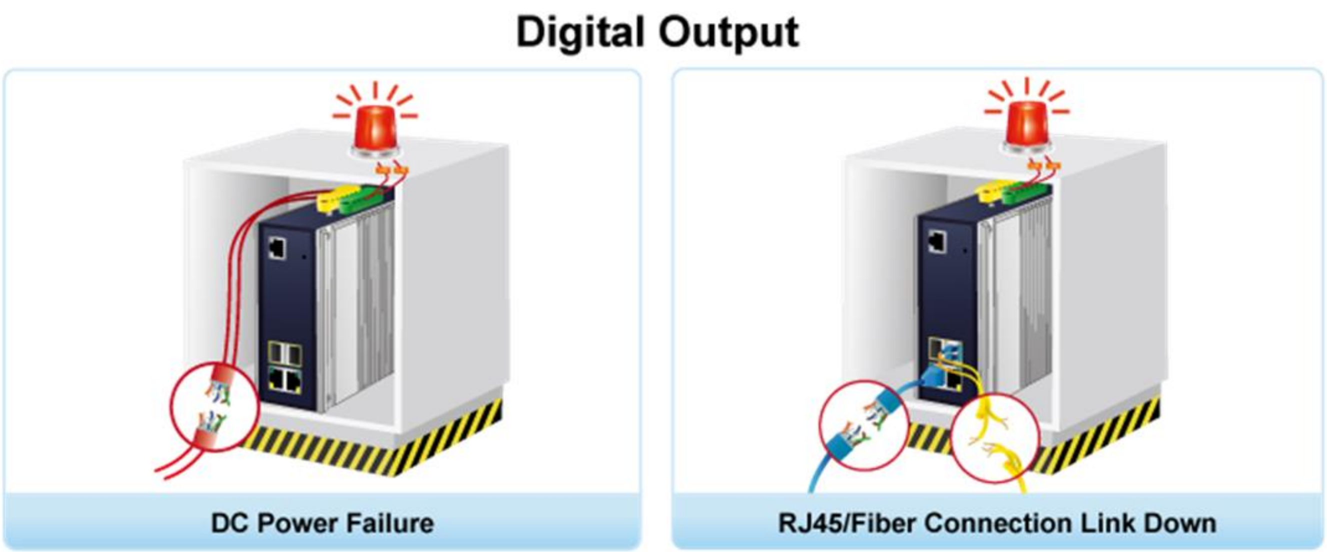
Reset : Click to undo any changes made locally and revert to previously saved values.

4.2.1.16 Digital Input/Output

Digital Input allows user to log external device (such as industrial cooler) dead or alive or something else. System will log a user customized message into system log and syslog, and issue SNMP trap or issue an alarm E-mail.



Digital Output allows user to monitor the switch port and power, and let system issue a high or low signal to an external device (such as alarm) when the monitor port or power has failed.



The Configuration screen in Figure 4-2-19 and Figure 4-2-20 appears.

Digital Input/Output Control Configuration

Digital Input 0		Digital Input 1	
Enable	Enable	Enable	Enable
DI Condition	High to Low	DI Condition	High to Low
Event Description	Customize DI0 Message.	Event Description	Customize DI1 Message.
Action	System Log SNMP Trap	Action	System Log SNMP Trap

Figure 4-2-19 Digital Input Control Configuration page Screenshot

The page includes the following fields:

Object	Description
• **Enable**	Check the Enable checkbox to enable Digital Input function. Uncheck the Enable checkbox to disable Digital Input function.
• **DI Condition**	**As Digital Input:** Allows user to select High to Low or Low to High. This means a signal received by system is from High to Low or From Low to High. It will trigger an action that logs a customize message or issue the message from the switch.
• **Event Description**	Allows user to set a customized message for Digital Input function alarming.
• **Action**	**As Digital Input:** Allows user to record alarm message to **System log**, **syslog** or issues out via **SNMP Trap** or **SMTP**. As default SNMP Trap and SMTP are disabled, please enable them first if you want to issue alarm message via them.

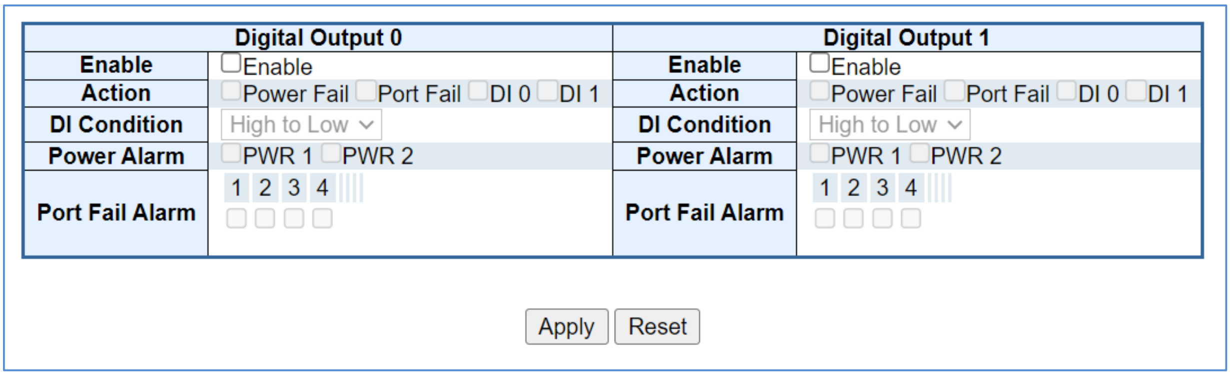


Figure 4-2-20 Digital Output Control Configuration page Screenshot

The page includes the following fields:

Object	Description
• **Enable**	Check the Enable checkbox to enable Digital Output function. Uncheck the Enable checkbox to disable Output function.
• **Event**	**As Digital Output:** Allows user to monitor an alarm from **port failure**, **power failure**, **Digital Input 0 (DI 0)** and **Digital Input 1(DI 1)** which means if Digital Output has detected these events, then Digital Output would be triggered according to the setting of Condition.
• **DI Condition**	**As Digital Output:** Allows user to select High to Low or Low to High. This means that when the switch is power-failed or port-failed, then system will issue a High or Low signal to an external device such as an alarm.

• **Power Alarm**	Allows user to choose which power module that needs to be monitored.
• **Port Alarm**	Allows user to choose which port that needs to be monitored.

Buttons

Apply: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

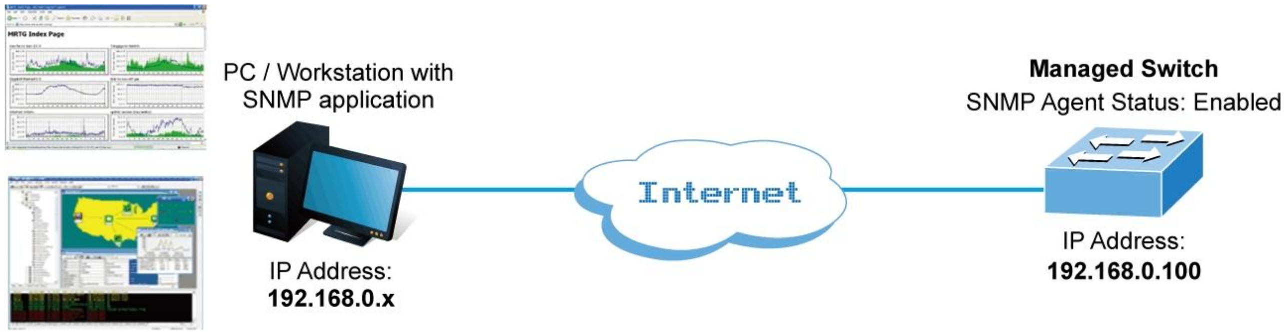
4.2.2 SNMP

4.2.2.1 SNMP Overview

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

An SNMP-managed network consists of three key components: Network management stations (NMSs), SNMP agents, Management information base (MIB) and network-management protocol:

- **Network management stations (NMSs):** Sometimes called consoles, these devices execute management applications that monitor and control network elements. Physically, NMSs are usually engineering workstation-caliber computers with fast CPUs, megapixel color displays, substantial memory, and abundant disk space. At least one NMS must be present in each managed environment.
- **Agents:** Agents are software modules that reside in network elements. They collect and store management information such as the number of error packets received by a network element.
- **Management information base (MIB):** A MIB is a collection of managed objects residing in a virtual information store. Collections of related managed objects are defined in specific MIB modules.
- **Network-management protocol:** A management protocol is used to convey management information between agents and NMSs. SNMP is the Internet community's de facto standard management protocol.



SNMP Operations

SNMP itself is a simple request/response protocol. NMSs can send multiple requests without receiving a response.

- **Get --** Allows the NMS to retrieve an object instance from the agent.
- **Set --** Allows the NMS to set values for object instances within an agent.
- **Trap --** Used by the agent to asynchronously inform the NMS of some event. The SNMPv2 trap message is designed to replace the SNMPv1 trap message.

SNMP community

An SNMP community is the group that devices and management stations running SNMP belong to. It helps define where information is sent. The community name is used to identify the group. An SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management stations that do not belong to one of its communities. SNMP default communities are:

- **Write** = private
- **Read** = public

Use the SNMP Menu to display or configure the **Industrial Managed TSN Device** 's SNMP function. This section has the following items:

■	**System Configuration**	Configure SNMP on this page.
■	**Trap Configuration**	Configure SNMP trap on this page.
■	**System Information**	The system information is provided here.
■	**SNMPv3 Communities**	Configure SNMPv3 communities table on this page.
■	**SNMPv3 Users**	Configure SNMPv3 users table on this page.
■	**SNMPv3 Groups**	Configure SNMPv3 groups table on this page.
■	**SNMPv3 Views**	Configure SNMPv3 views table on this page.
■	**SNMPv3 Access**	Configure SNMPv3 accesses table on this page.

4.2.2.2 System Configuration

Configure SNMP on this page. The SNMP System Configuration screen in Figure 4-2-21 appears.

Figure 4-2-21: SNMP System Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	Indicates the SNMP mode operation. Possible modes are: ■ **Enabled**: Enable SNMP mode operation. ■ **Disabled**: Disable SNMP mode operation.
• **Engine ID**	Indicates the SNMPv3 engine ID. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.

Buttons

: Click to apply changes

: Click to undo any changes made locally and revert to previously saved values.

4.2.2.3 System Information

The switch system information is provided here. The SNMP System Information screen in Figure 4-2-22 appears.

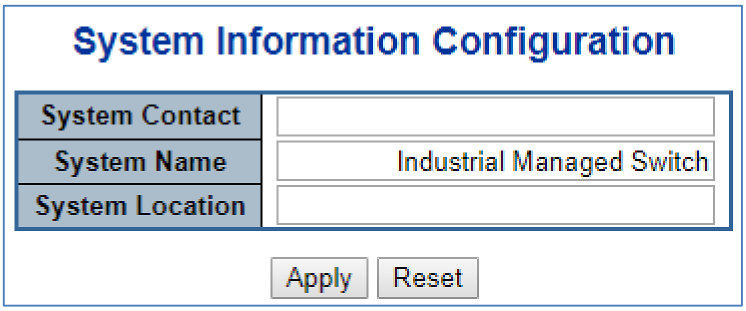


Figure 4-2-22: System Information Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **System Contact**	The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
• **System Name**	An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.
• **System Location**	The physical location of this node(e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

4.2.2.4 SNMP Trap Configuration

Configure SNMP trap on this page. The SNMP Trap Configuration screen in Figure 4-2-23 appears.

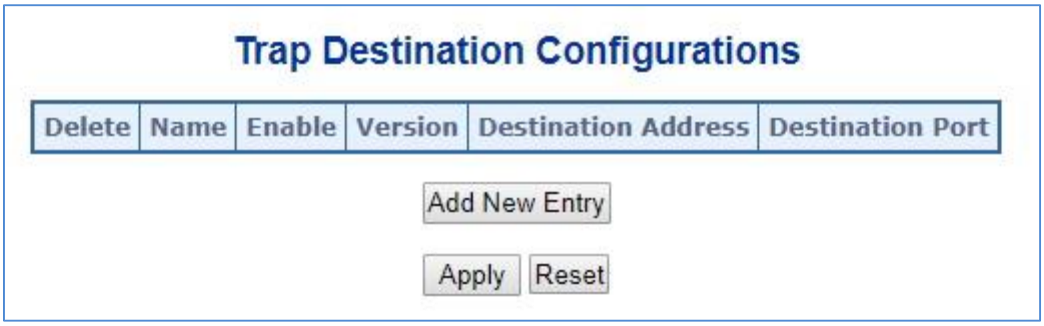


Figure 4-2-23: SNMP Trap Destination Configuration Page Screenshot

Click '**Add New Entry**" and then the SNMP Trap Configuration page in Figure 4-2-24 appears.

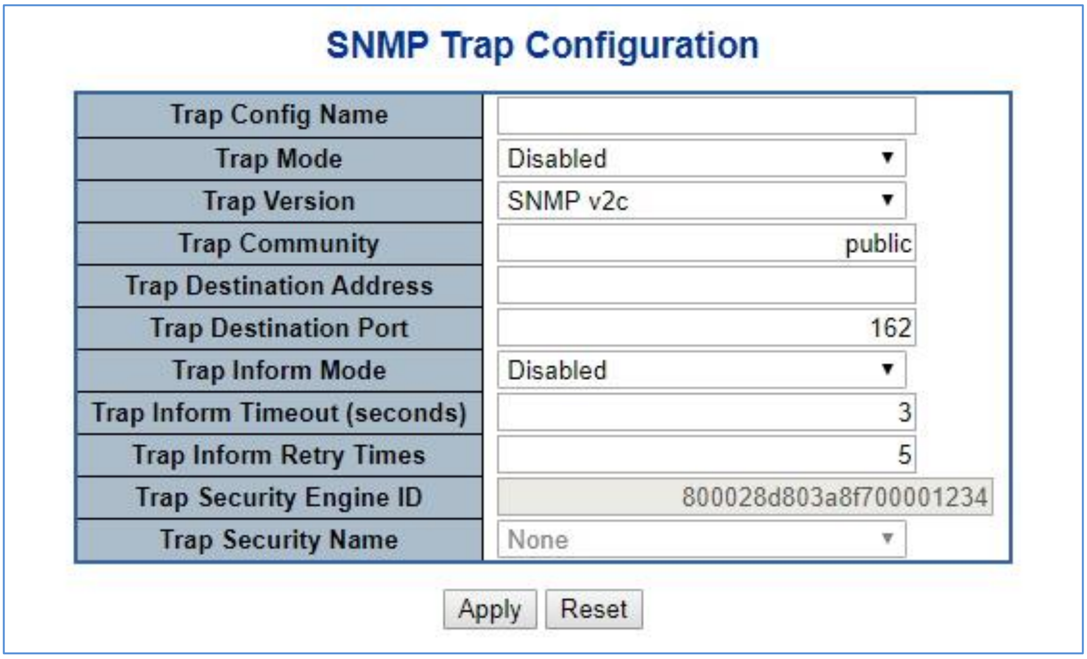


Figure 4-2-24: SNMP Trap Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Trap Config**	Indicates which trap Configuration's name for configuring. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 33 to 126.
• **Trap Mode**	Indicates the SNMP trap mode operation. Possible modes are: ■ **Enabled**: Enable SNMP trap mode operation. ■ **Disabled**: Disable SNMP trap mode operation.
• **Trap Version**	Indicates the SNMP trap supported version. Possible versions are: ■ **SNMP v1**: Set SNMP trap supported version 1. ■ **SNMP v2c**: Set SNMP trap supported version 2c.

	■ **SNMP v3**: Set SNMP trap supported version 3.
• **Trap Community**	Indicates the community access string when send SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.
• **Trap Destination Address**	Indicates the SNMP trap destination address.
• **Trap Destination Port**	Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.
• **Trap Inform Mode**	Indicates the SNMP trap inform mode operation. Possible modes are: ■ **Enabled**: Enable SNMP trap authentication failure. ■ **Disabled**: Disable SNMP trap authentication failure.
• **Trap Inform Timeout (seconds)**	Indicates the SNMP trap inform timeout. The allowed range is **0** to **2147**.
• **Trap Inform Retry Times**	Indicates the SNMP trap inform retry times. The allowed range is **0** to **255**.
• **Trap Probe Security Engine ID**	Indicates the SNMPv3 trap probe security engine ID mode of operation. Possible values are: ■ **Enabled**: Enable SNMP trap probe security engine ID mode of operation. ■ **Disabled**: Disable SNMP trap probe security engine ID mode of operation.
• **Trap Security Engine ID**	Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.
• **Trap Security Name**	Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.
• **System**	Enable/disable that the Interface group's traps. Possible traps are: ■ **Warm Start**: Enable/disable Warm Start trap. ■ **Cold Start**: Enable/disable Cold Start trap.
• **Interface**	Indicates that the Interface group's traps. Possible traps are: ■ **Link Up**: Enable/disable Link up trap. ■ **Link Down**: Enable/disable Link down trap. ■ **LLDP**: Enable/disable LLDP trap.
• **AAA**	Indicates that the AAA group's traps. Possible traps are: **Authentication Fail** : Enable/disable SNMP trap authentication failure trap.
• **Switch**	Indicates that the Switch group's traps. Possible traps are: ■ **STP**: Enable/disable STP trap. ■ **RMON**: Enable/disable RMON trap.

4.2.2.5 SNMP Trap Source Configuration

This page provides SNMP trap source configurations. A trap is sent for the given trap source if at least one filter with filter type included matches the filter, and no filters with filter type excluded matches.

Figure 4-2-25: SNMP Trap Source Configuration Page Screenshot

Click "**Add New Entry**" to add a new entry. The maximum entry count is 32.

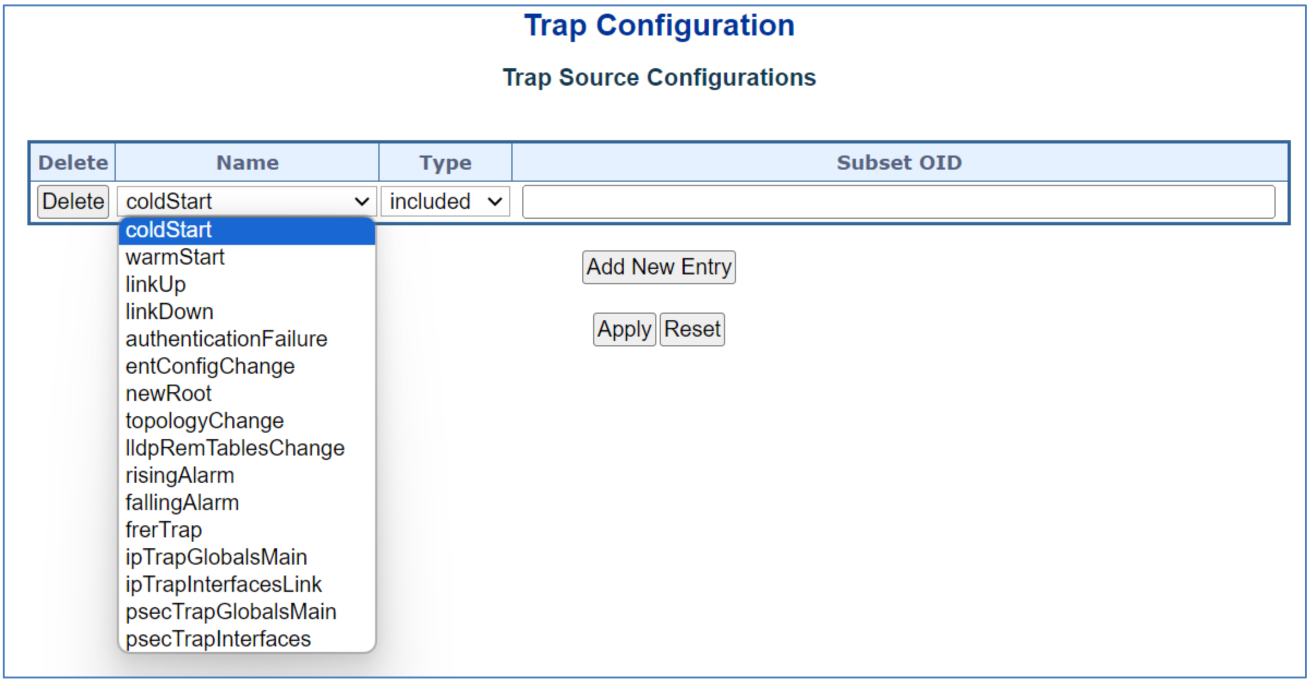


Figure 4-2-26: SNMP Trap Source Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Name**	Indicates the name for the entry.
• **Type**	The filter type for the entry. Possible types are: ■ **included**: An optional flag to indicate a trap is sent for the given trap source is matched. ■ **excluded**: An optional flag to indicate a trap is not sent for the given trap source is matched.
• **Subset OID**	The subset OID for the entry. The value should depend on the what kind of trap name. For example, the ifIdex is the subset OID of linkUp and linkDown. A valid subset OID is one or more digital number(0-4294967295) or asterisk(*) which are separated by dots(.). The first character must not begin with asterisk(*) and the maximum of OID count must not exceed 128.

Buttons

Add New Entry: Click to add a new community entry. The maximum entry count is 32

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.2.2.6 SNMPv3 Communities

Configure SNMPv3 communities table on this page. The entry index key is Community. The SNMPv3 Communities screen in Figure 4-2-27 appears.

Figure 4-2-27: SNMPv3 Communities Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Community Name**	Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string.
• **Community Secret**	Indicates the community secret (access string) to permit access using SNMPv1 and SNMPv2c to the SNMP agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
• **Source IP**	Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.
• **Source Mask**	Indicates the SNMP access source address mask.

Buttons

Add New Entry: Click to add a new community entry.

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.2.2.7 SNMPv3 Users

Configure SNMPv3 users table on this page. The entry index keys are Engine ID and User Name. The SNMPv3 Users screen in Figure 4-2-28 appears.

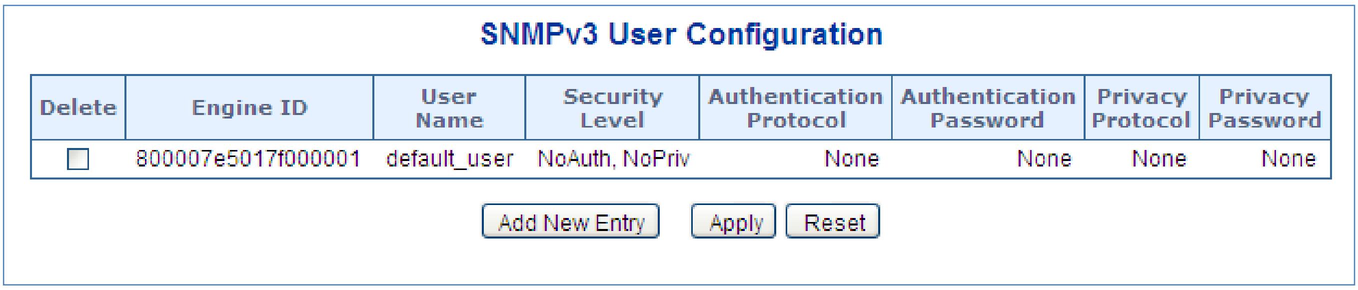


Figure 4-2-28: SNMPv3 Users Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Engine ID**	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the **User-based Security Model (USM)** for message security and the **View-based Access Control Model (VACM)** for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user.
• **User Name**	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
• **Security Level**	Indicates the security model that this entry should belong to. Possible security models are: ■ **NoAuth, NoPriv**: None authentication and none privacy. ■ **Auth, NoPriv**: Authentication and none privacy. ■ **Auth, Priv**: Authentication and privacy. The value of security level cannot be modified if entry already exist. That means must first ensure that the value is set correctly.

• **Authentication Protocol**	Indicates the authentication protocol that this entry should belong to. Possible authentication protocol are: ■ **None**: None authentication protocol. ■ **MD5**: An optional flag to indicate that this user using MD5 authentication protocol. ■ **SHA**: An optional flag to indicate that this user using SHA authentication protocol. The value of security level cannot be modified if entry already exist. That means must first ensure that the value is set correctly.
• **Authentication Password**	A string identifying the authentication pass phrase. For **MD5** authentication protocol, the allowed string length is 8 to 32. For **SHA** authentication protocol, the allowed string length is 8 to 40. The allowed content is the ASCII characters from 33 to 126.
• **Privacy Protocol**	Indicates the privacy protocol that this entry should belong to. Possible privacy protocol are: ■ **None**: None privacy protocol. ■ **DES**: An optional flag to indicate that this user using DES authentication protocol. ■ **AES**: An optional flag to indicate that this user uses AES authentication protocol.
• **Privacy Password**	A string identifying the privacy pass phrase. The allowed string length is 8 to 32, and the allowed content is the ASCII characters from 33 to 126.

Buttons

Add New Entry: Click to add a new user entry.

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.2.2.8 SNMPv3 Groups

Configure SNMPv3 groups table on this page. The entry index keys are Security Model and Security Name. The SNMPv3 Groups screen in Figure 4-2-29 appears.

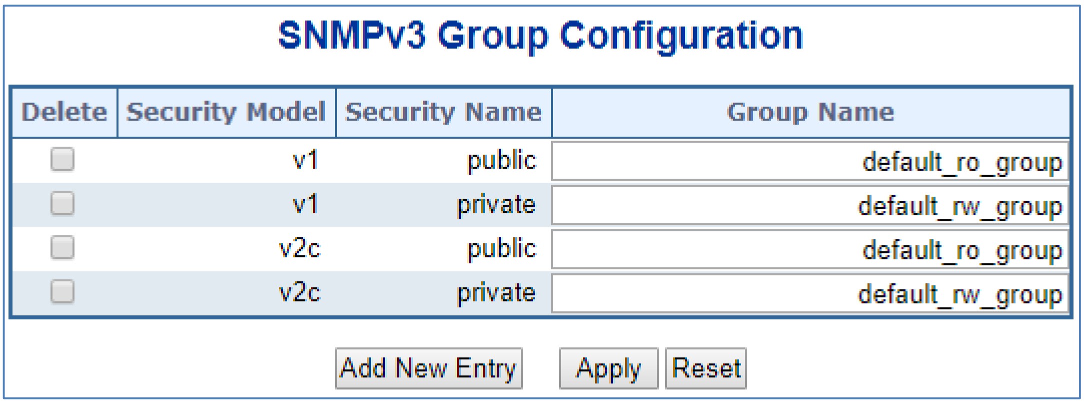


Figure 4-2-29: SNMPv3 Groups Configuration Page Screenshot

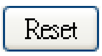
The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Security Model**	Indicates the security model that this entry should belong to. Possible security models are: ■ **v1**: Reserved for SNMPv1. ■ **v2c**: Reserved for SNMPv2c. ■ **usm**: User-based Security Model (USM).
• **Security Name**	A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
• **Group Name**	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.

Buttons

: Click to add a new group entry.

: Click to apply changes



: Click to undo any changes made locally and revert to previously saved values.

4.2.2.9 SNMPv3 Views

Configure SNMPv3 views table on this page. The entry index keys are View Name and OID Subtree. The SNMPv3 Views screen in Figure 4-2-30 appears.

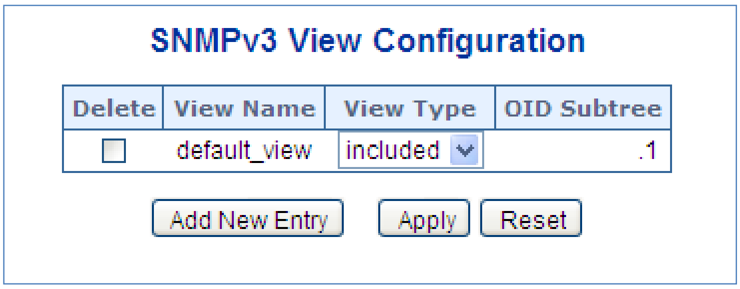


Figure 4-2-30: SNMPv3 Views Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **View Name**	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
• **View Type**	Indicates the view type that this entry should belong to. Possible view type are: ■ **included**: An optional flag to indicate that this view subtree should be included. ■ **excluded**: An optional flag to indicate that this view subtree should be excluded. In general, if a view entry's view type is 'excluded', it should be exist another view entry which view type is 'included' and it's OID subtree overstep the 'excluded' view entry.
• **OID Subtree**	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).

Buttons

Add New Entry: Click to add a new view entry.

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.2.2.10 SNMPv3 Access

Configure SNMPv3 accesses table on this page. The entry index keys are Group Name, Security Model and Security Level.

The SNMPv3 Access screen in Figure 4-2-31 appears.

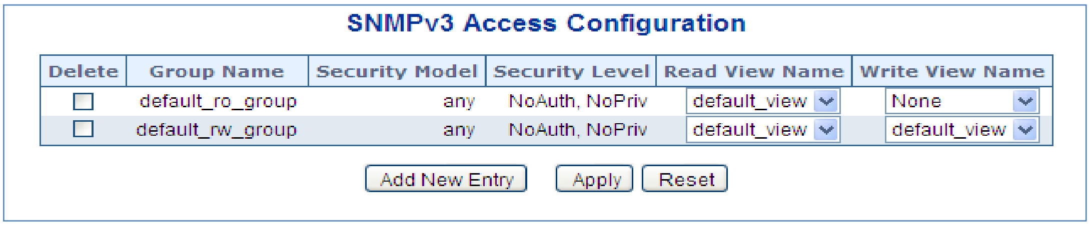


Figure 4-2-31: SNMPv3 Accesses Configuration Page Screenshot

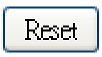
The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Group Name**	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
• **Security Model**	Indicates the security model that this entry should belong to. Possible security models are: ■ **any**: Accepted any security model (v1|v2c|usm). ■ **v1**: Reserved for SNMPv1. ■ **v2c**: Reserved for SNMPv2c. ■ **usm**: User-based Security Model (USM)
• **Security Level**	Indicates the security model that this entry should belong to. Possible security models are: ■ **NoAuth, NoPriv**: None authentication and none privacy. ■ **Auth, NoPriv**: Authentication and none privacy. ■ **Auth, Priv**: Authentication and privacy.
• **Read View Name**	The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
• **Write View Name**	The name of the MIB view defining the MIB objects for which this request may potentially SET new values. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.

Buttons

: Click to add a new access entry.

: Click to apply changes



: Click to undo any changes made locally and revert to previously saved values.

4.2.3 RMON

RMON is the most important expansion of the standard SNMP. RMON is a set of MIB definitions, used to define standard network monitor functions and interfaces, enabling the communication between SNMP management terminals and remote monitors. RMON provides a highly efficient method to monitor actions inside the subnets.

MID of RMON consists of 10 groups. The switch supports the most frequently used groups 1, 2, 3 and 9:

- **Statistics:** Maintain basic usage and error statistics for each subnet monitored by the agent.
- **History:** Record periodical statistic samples available from statistics.
- **Alarm:** Allow management console users to set any count or integer for sample intervals and alert thresholds for RMON agent records.
- **Event:** A list of all events generated by RMON agent.

Alarm depends on the implementation of Event. Statistics and History display some current or history subnet statistics. Alarm and Event provide a method to monitor any integer data change in the network, and provide some alerts upon abnormal events (sending Trap or record in logs).

4.2.3.1 RMON Alarm Configuration

Configure RMON Alarm table on this page. The entry index key is **ID**.; screen in Figure 4-2-32 appears.

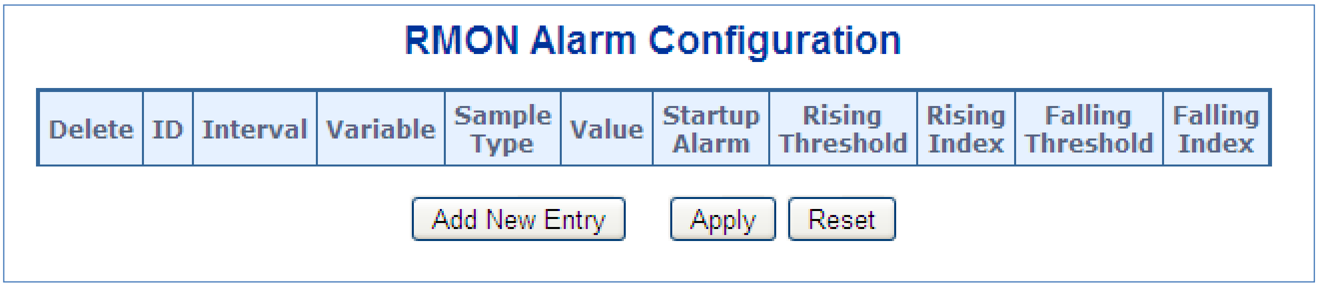


Figure 4-2-32: RMON Alarm Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **ID**	Indicates the index of the entry. The range is from 1 to 65535.
• **Interval**	Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2^31-1.
• **Variable**	Indicates the particular variable to be sampled; the possible variables are: ■ **InOctets**: The total number of octets received on the interface, including framing characters. ■ **InUcastPkts**: The number of uni-cast packets delivered to a higher-layer protocol.

	■ **InNUcastPkts**: The number of broadcast and multi-cast packets delivered to a higher-layer protocol. ■ **InDiscards**: The number of inbound packets that are discarded even the packets are normal. ■ **InErrors**: The number of inbound packets that contains errors preventing them from being deliverable to a higher-layer protocol. ■ **InUnknownProtos**: the number of the inbound packets that is discarded because of the unknown or un-support protocol. ■ **OutOctets**: The number of octets transmitted out of the interface, including framing characters. ■ **OutUcastPkts**: The number of uni-cast packets that requests to transmit. ■ **OutNUcastPkts**: The number of broadcast and multi-cast packets that requests to transmit. ■ **OutDiscards**: The number of outbound packets that is discarded even the packets are normal. ■ **OutErrors**: The number of outbound packets that could not be transmitted because of errors. ■ **OutQLen**: The length of the output packet queue (in packets).
• **Sample Type**	The method of sampling the selected variable and calculating the value to be compared against the thresholds; possible sample types are: ■ **Absolute**: Get the sample directly. ■ **Delta**: Calculate the difference between samples (default).
• **Value**	The value of the statistic during the last sampling period.
• **Startup Alarm**	The method of sampling the selected variable and calculating the value to be compared against the thresholds; possible sample types are: ■ **Rising**Trigger alarm when the first value is larger than the rising threshold. ■ **Falling**Trigger alarm when the first value is less than the falling threshold. ■ **RisingOrFalling**Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).
• **Rising Threshold**	Rising threshold value (-2147483648-2147483647).
• **Rising Index**	Rising event index (1-65535).
• **Falling Threshold**	Falling threshold value (-2147483648-2147483647)
• **Falling Index**	Falling event index (1-65535).

Buttons

Add New Entry : Click to add a new community entry.

Apply : Click to apply changes

Reset : Click to undo any changes made locally and revert to previously saved values.

4.2.3.2 RMON Alarm Status

This page provides an overview of RMON Alarm entries. Each page shows up to 99 entries from the Alarm table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Alarm table. The first displayed will be the one with the lowest ID found in the Alarm table; screen in Figure 4-2-33 appears.

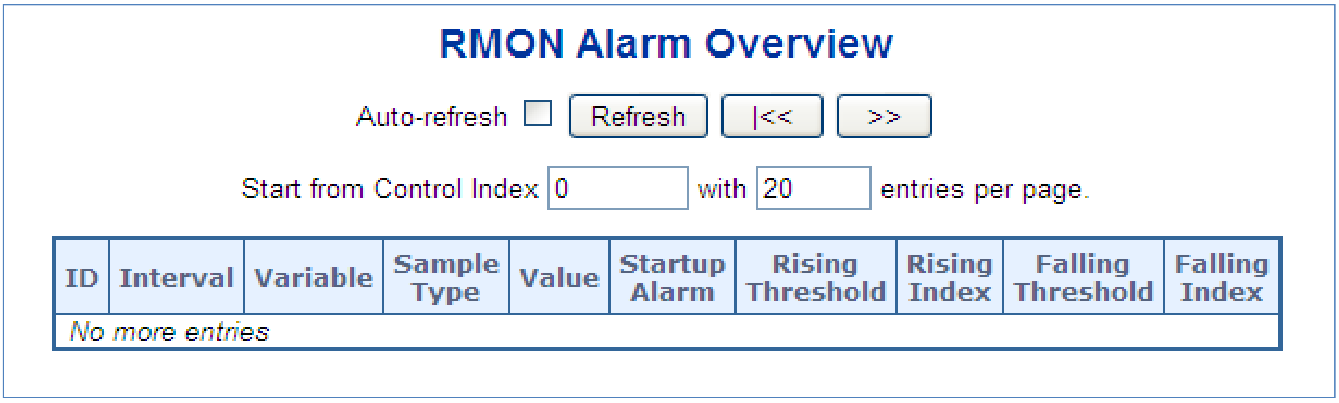


Figure 4-2-33: RMON Alarm Overview Page Screenshot

The page includes the following fields:

Object	Description
• **ID**	Indicates the index of Alarm control entry.
• **Interval**	Indicates the interval in seconds for sampling and comparing the rising and falling threshold.
• **Variable**	Indicates the particular variable to be sampled.
• **Sample Type**	The method of sampling the selected variable and calculating the value to be compared against the thresholds.
• **Value**	The value of the statistic during the last sampling period.
• **Startup Alarm**	The alarm that may be sent when this entry is first set to valid.
• **Rising Threshold**	Rising threshold value
• **Rising Index**	Rising event index
• **Falling Threshold**	Falling threshold value
• **Falling Index**	Falling event index

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

|<<: Updates the table, starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID.

>>: Updates the table, starting with the entry after the last entry currently displayed.

4.2.3.3 RMON Event Configuration

Configure RMON Event table on this page. The entry index key is **ID**; screen in Figure 4-2-34 appears.

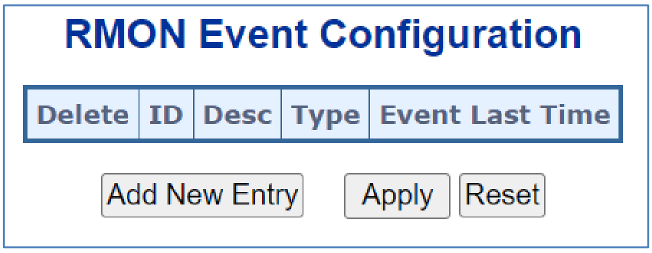


Figure 4-2-34 RMON Event Configuration Page Screenshot

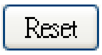
The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **ID**	Indicates the index of the entry. The range is from 1 to 65535.
• **Desc**	Indicates this event, the string length is from 0 to 127, default is a null string.
• **Type**	Indicates the notification of the event; the possible types are: ■ **none**: The total number of octets received on the interface, including framing characters. ■ **log**: The number of uni-cast packets delivered to a higher-layer protocol. ■ **snmptrap**: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol. ■ **logandtrap**: The number of inbound packets that are discarded even the packets are normal.
• **Event Last Time**	Indicates the value of sysUpTime at the time this event entry last generated an event.

Buttons

: Click to add a new community entry.

: Click to apply changes



: Click to undo any changes made locally and revert to previously saved values.

4.2.3.4 RMON Event Status

This page provides an overview of RMON Event table entries. Each page shows up to 99 entries from the Event table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Event table. The first displayed will be the one with the lowest Event Index and Log Index found in the Event table; screen in Figure 4-2-35 appears.

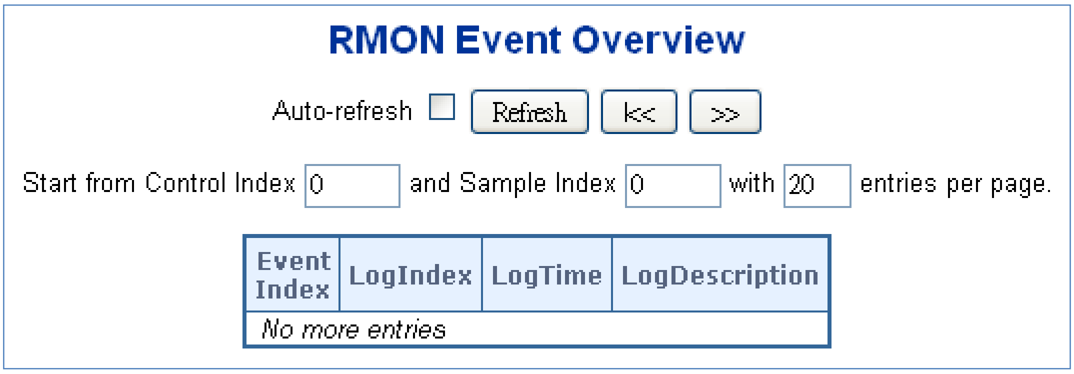


Figure 4-2-35: RMON Event Overview Page Screenshot

The page includes the following fields:

Object	Description
• **Event Index**	Indicates the index of the event entry.
• **Log Index**	Indicates the index of the log entry.
• **Logtime**	Indicates Event log time.
• **Log Description**	Indicates the Event description.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

|<<: Updates the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID.

>>: Updates the table, starting with the entry after the last entry currently displayed.

>>: Updates the table, starting with the entry after the last entry currently displayed.

4.2.3.5 RMON History Configuration

Configure RMON History table on this page. The entry index key is **ID**; screen in Figure 4-2-36 appears.

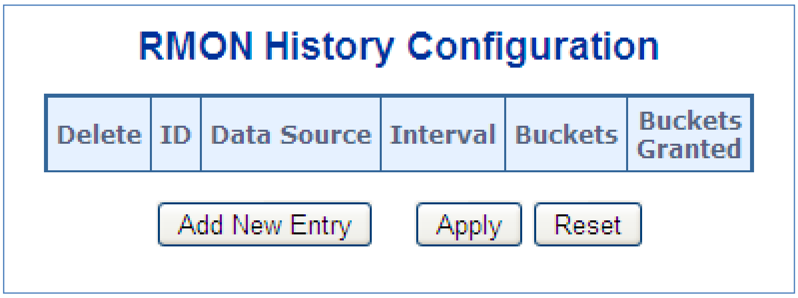


Figure 4-2-36: RMON History Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **ID**	Indicates the index of the entry. The range is from 1 to 65535.
• **Data Source**	Indicates the port ID which wants to be monitored.
• **Interval**	Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.
• **Buckets**	Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600, default value is 50.
• **Buckets Granted**	The number of data will be saved in the RMON.

Buttons

Add New Entry: Click to add a new community entry.

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.2.3.6 RMON Statistics Configuration

Configure RMON Statistics table on this page. The entry index key is **ID**; screen in Figure 4-2-37 appears.

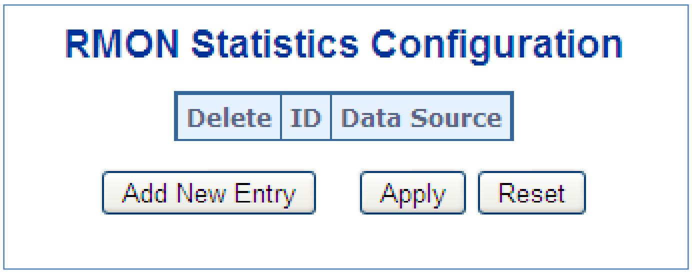


Figure 4-2-37: RMON Statistics Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **ID**	Indicates the index of the entry. The range is from 1 to 65535.
• **Data Source**	Indicates the port ID which wants to be monitored.

Buttons

Add New Entry: Click to add a new community entry.

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.2.3.7 RMON Statistics Status

This page provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Statistics table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table; screen in Figure 4-2-38 appears.

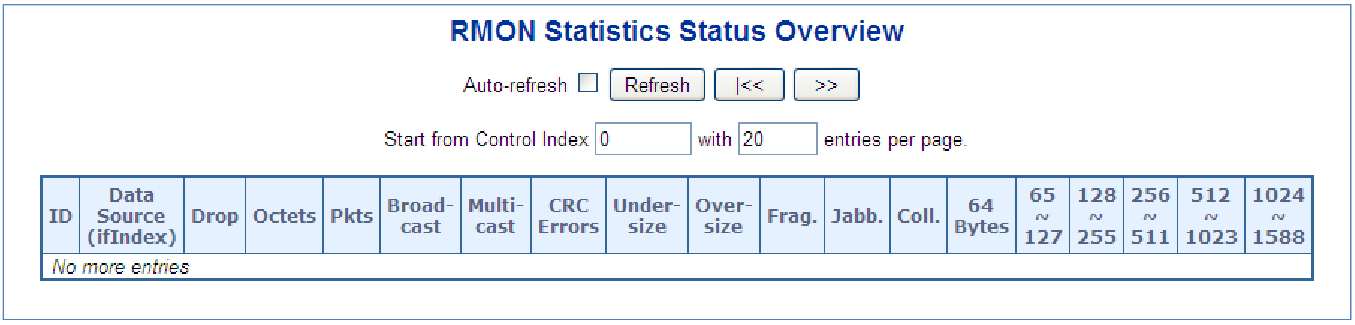


Figure 4-2-38: RMON Statistics Status Overview Page Screenshot

The page includes the following fields:

Object	Description
• **ID**	Indicates the index of Statistics entry.
• **Data Source (ifIndex)**	The port ID which wants to be monitored.
• **Drop**	The total number of events in which packets were dropped by the probe due to lack of resources.
• **Octets**	The total number of octets of data (including those in bad packets) received on the network.
• **Pkts**	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
• **Broadcast**	The total number of good packets received that were directed to the broadcast address.
• **Multicast**	The total number of good packets received that were directed to a multicast address.
• **CRC Errors**	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets.
• **Undersize**	The total number of packets received that were less than 64 octets.
• **Oversize**	The total number of packets received that were longer than 1518 octets.
• **Frag.**	The number of frames whose size is less than 64 octets received with invalid CRC.
• **Jabb.**	The number of frames whose size is larger than 64 octets received with invalid CRC.
• **Coll.**	The best estimate of the total number of collisions in this Ethernet segment.

• **64 Bytes**	The total number of packets (including bad packets) received that were 64 octets in length.
• **65~127**	The total number of packets (including bad packets) received that were between 65 to 127 octets in length.
• **128~255**	The total number of packets (including bad packets) received that were between 128 to 255 octets in length.
• **256~511**	The total number of packets (including bad packets) received that were between 256 to 511 octets in length.
• **512~1023**	The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.
• **1024~1518**	The total number of packets (including bad packets) received that were between 1024 to 1518 octets in length.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

|<<: Updates the table, starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID.

>>: Updates the table, starting with the entry after the last entry currently displayed.

4.2.4 DHCP Relay

4.2.4.1 DHCPv4 Relay

A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain. It stores the incoming interface IP address in the GIADDR field of the DHCP packet. The DHCP server can use the value of GIADDR field to determine the assigned subnet. For such condition, please make sure the switch configuration of VLAN interface IP address and PVID(Port VLAN ID) correctly. This page configures **DHCP Relay** to enable/disable DHCP Relay Mode, screen in Figure 4-2-39 appears.

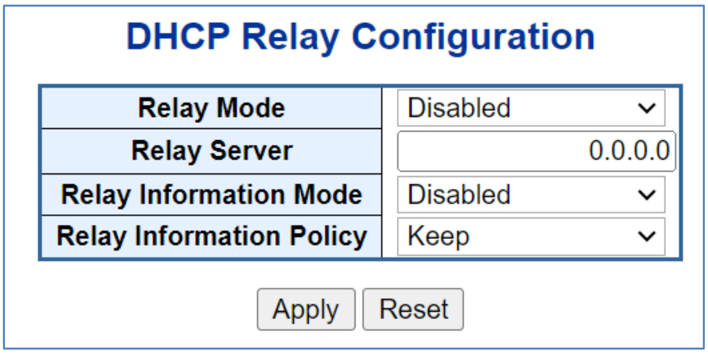


Figure 4-2-39: DHCP server mode Page Screenshot

The page includes the following fields:

Object	Description
• **Relay Mode**	Indicates the DHCP relay mode operation. Possible modes are: **Enabled**: Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations. **Disabled**: Disable DHCP relay mode operation.
• **Relay Server**	Indicates the DHCP relay server IP address.
• **Relay Information Mode**	Indicates the DHCP relay information mode option operation. The option 82 circuit ID format as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID(in standalone device it always equal 0, in stackable device it means switch ID), and the last two characters are the port number. For example, "00030108" means the DHCP message receive form VLAN ID 3, switch ID 1, port No 8. And the option 82 remote ID value is equal the switch MAC address. Possible modes are: **Enabled**: Enable DHCP relay information mode operation. When DHCP relay

	information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled. **Disabled**: Disable DHCP relay information mode operation.
• **Relay Information Policy**	Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if the agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' policy is invalid when relay information mode is disabled. Possible policies are: **Replace**: Replace the original relay information when a DHCP message that already contains it is received. **Keep**: Keep the original relay information when a DHCP message that already contains it is received. **Drop**: Drop the package when a DHCP message that already contains relay information is received.

Buttons

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.2.4.2 DHCPv4 Relay Statistics

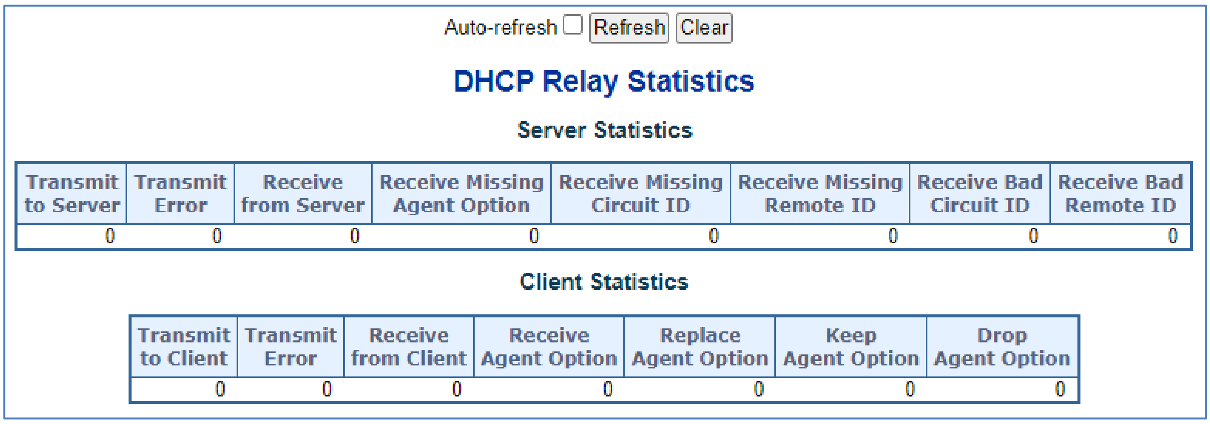


Figure 4-2-40: DHCPv4 Relay Statistics

The first part of this page provides statistics for the DHCP server.

Object	Description
• **Transmit to Server**	The number of packets that are relayed from client to server.
• **Transmit Error**	The number of packets that resulted in errors while being sent to clients.
• **Receive from Server**	The number of packets received from server.
• **Receive Missing Agent Option**	The number of packets received without agent information options.
• **Receive Missing Circuit ID**	The number of packets received with the Circuit ID option missing.
• **Recevie Missing Remote ID**	The number of packets received with the Remote ID option missing.
• **Receive Bad Circuit ID**	The number of packets whose Circuit ID option did not match known circuit ID.
• **Receive Bad Remote ID**	The number of packets whose Remote ID option did not match known Remote ID.

The second part of this page provides statistics for the Client.

Object	Description
• **Transmit to Client**	The number of relayed packets from server to client.
• **Transmit Error**	The number of packets that resulted in error while being sent to servers.
• **Receive from Client**	The number of received packets from server.
• **Receive Agent Option**	The number of received packets with relay agent information option.
• **Replace Agent Option**	The number of packets which were replaced with relay agent information option.
• **Keep Agent Option**	The number of packets whose relay agent information was retained.
• **Drop Agent Option**	The number of packets that were dropped which were received with relay agent information.

Bottons:

Refresh: Click to refresh the page immediately.

Clear: Clear all statistics.

4.2.4.3 DHCPv6 Relay

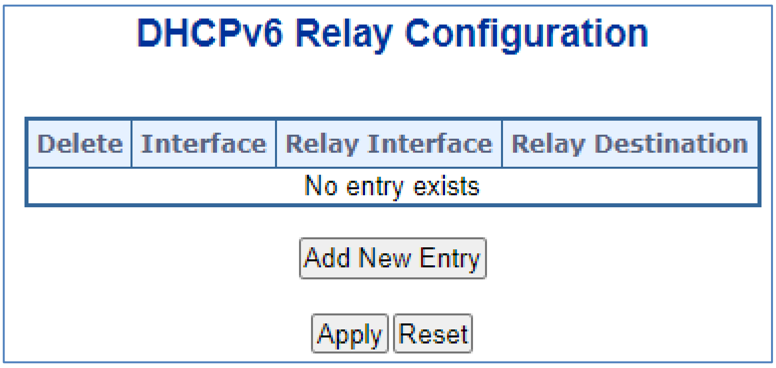


Figure 4-2-41: DHCPv6 Relay Configuration

This table is used to configure DHCPv6_Relay for a specific VLAN.

Object	Description
• **Interface**	Interface identification.
• **Relay Interface**	Interface identification. The id of the interface used for relaying.
• **Relay Destination**	An Ipv6 address represented as human readable test as specified in RFC5952. The IPv6 address of the DHCPv6 server that requests shall be relayed to. The default value 'ff05::1:3' mans 'any DHCP server'.

Bottons:

Add New Entry : Click to add new entry.

Apply: Click to apply changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.2.4.4 DHCPv6 Relay Statistics

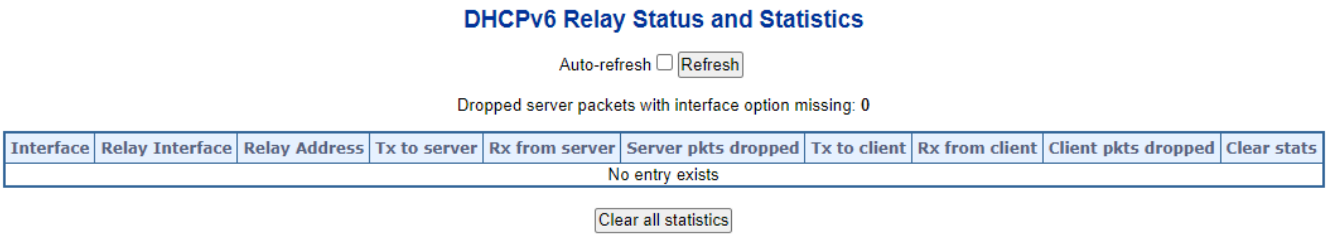


Figure 4-2-42: DHCPv6 Relay Statistics

The table below shows the current , configured relay agents and their statistics.

Object	Description
• **Interface**	Interface identification. The id of the interface that receives client requests.
• **Relay Interface**	Interface identification. The id of the interface used for relaying.
• **Relay Address**	An Ipv6 address represented as human readable test as specified in RFC5952. The IPv6 address that requests shall be relayed to. The default value 'ff05::1:3' means 'any DHCPv6 server'.
• **Tx to Server**	Integer number. Number of packets relayed to server.
• **Rx from Server**	Integer number. Number of packets received from server.
• **Server Pkts Dropped**	Integer number. Number of packets from server that relay agent drops.
• **Tx to Client**	Integer number. Number of packets sent to client.
• **Rx from client**	Integer number. Number of packets received from client.
• **Client pkts dropped**	Integer number. Number of packets from client that relay agent drops.
• **Clear Stats**	Resets all statistics counters of relevant entry to zero.

Bottons:

Refresh : Resets all statistics counters to zero.

Clear all statistics : Click to refresh the page immediately.

4.2.5 DHCP server

4.2.5.1 Mode

This page configures **global mode** and **VLAN mode** to enable/disable DHCP server per system and per VLAN.

Configure DHCP server mode on this page. The entry index key is **ID**.; screen in Figure 4-2-43 appears.

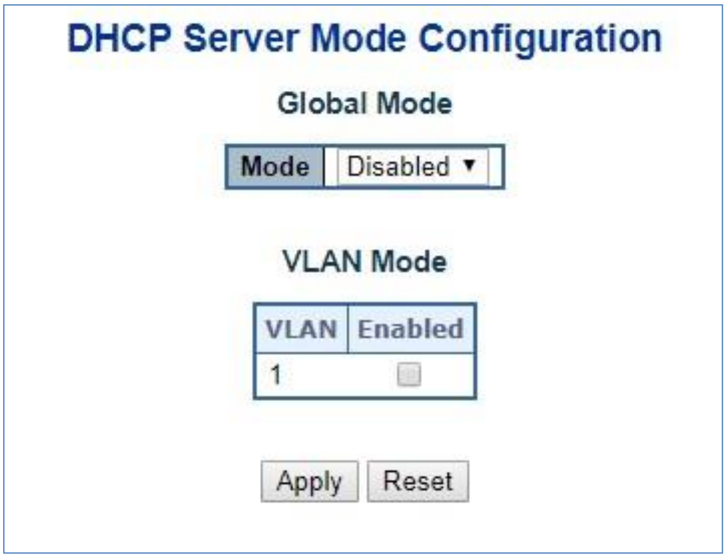


Figure 4-2-43: DHCP server mode Page Screenshot

The page includes the following fields:

Global Mode

Configure operation mode to enable/disable DHCP server per system.

Object	Description
• **Mode**	Configure the operation mode per system. Possible modes are: **Enabled**: Enable DHCP server per system. **Disabled**: Disable DHCP server pre system.

VLAN Mode

Configure operation mode to enable/disable DHCP server per VLAN.

Object	Description
• **VLAN Range**	Indicate the VLAN range in which DHCP server is enabled or disabled. The first VLAN ID must be smaller than or equal to the second VLAN ID. BUT, if the VLAN range contains only 1 VLAN ID, then you can just input it into either one of the first and second VLAN ID or both. On the other hand, if you want to disable existed VLAN range, then you can follow the steps. 1. press "**Add VLANRange**" to add a new VLAN range. 2. input the VLAN range that you want to disable. 3. choose Mode to be **Disabled**. 4. press "**Apply**" to apply the change. Then, you will see the disabled VLAN range is removed from the DHCP Server mode configuration page.
• **Mode**	■ Indicate the operation mode per VLAN. Possible modes are: **Enabled**: Enable DHCP server per VLAN. **Disabled**: Disable DHCP server pre VLAN.

Buttons

Add VLAN Range: Click to add a new VLAN range.

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.2.5.2 Excluded IP

Configure excluded IP addresses. DHCP server will not allocate these excluded IP addresses to DHCP client.; screen in Figure 4-2-44 appears.

Figure 4-2-44: DHCP server excluded Page Screenshot

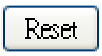
The page includes the following fields:

Object	Description
• **IP range**	Define the IP range to be excluded IP addresses. The first excluded IP must be smaller than or equal to the second excluded IP. BUT, if the IP range contains only 1 excluded IP, then you can just input it to either one of the first and second excluded IP or both.

Buttons

: Click to add a new excluded IP range.

: Click to apply changes



: Click to undo any changes made locally and revert to previously saved values.

4.2.5.3 Pool

This page manages DHCP pools. According to the DHCP pool, DHCP server will allocate IP address and deliver configuration parameters to DHCP client. screen in Figure 4-2-45 appears.

Figure 4-2-45: DHCP server pool Page Screenshot

The page includes the following fields:

Object	Description
• **Name**	Configure the pool name that accepts all printable characters, except white space. If you want to configure the detail settings, you can click the pool name to go into the configuration page.
• **Type**	Display which type of the pool is. **Network**: the pool defines a pool of IP addresses to service more than one DHCP client. **Host**: the pool services for a specific DHCP client identified by client identifier or hardware address.
• **IP**	Display network number of the DHCP address pool. If "-" is displayed, it means not defined
• **Subnet Mask**	Display subnet mask of the DHCP address pool. If "-" is displayed, it means not defined.
• **Lease Time**	Display lease time of the pool.

Buttons

Add New Pool: Click to add a new excluded IP range.

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.2.5.4 Statistics

This page displays the database counters and the number of DHCP messages sent and received by DHCP server.. screen in Figure 4-2-46 appears.

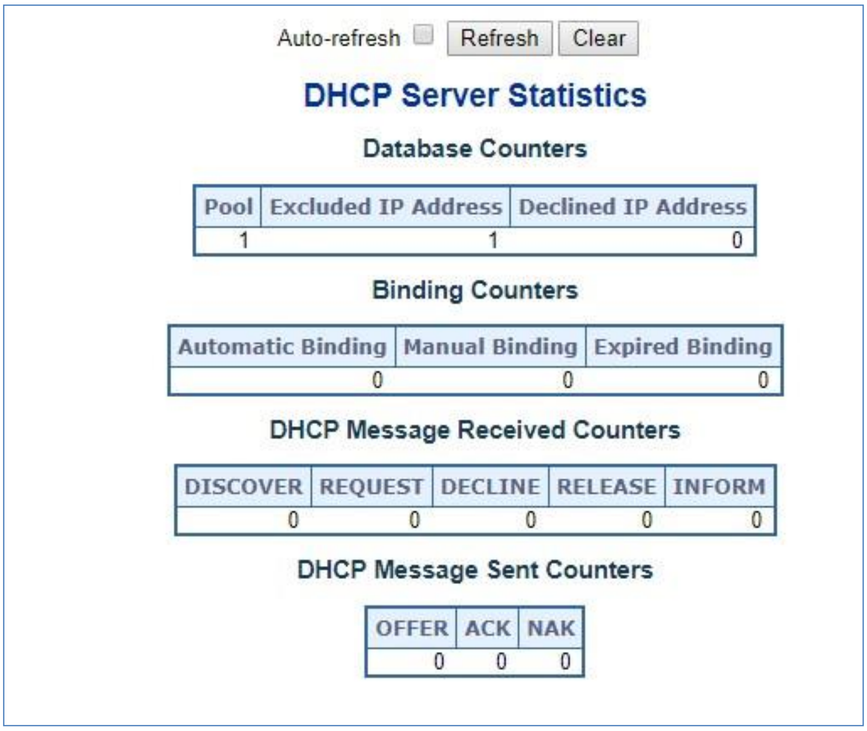


Figure 4-2-46: DHCP server Statistics Page Screenshot

The page includes the following fields:

Database Counters

Object	Description
• **Pool**	Number of pools
• **Excluded IP Address**	Number of excluded IP address ranges
• **Declined IP Address**	Number of declined IP addresses.

Binding Counters

Object	Description
• **Automatic Binding**	Number of bindings with network-type pools
• **Manual Binding**	Number of bindings that administrator assigns an IP address to a client. That is, the pool is of host type.
• **Expired Binding**	Number of bindings that their lease time expired or they are cleared from Automatic/Manual type bindings.

DHCP message Received Counters

Object	Description
• **Discover**	Number of DHCP DISCOVER messages received.
• **Request**	Number of DHCP REQUEST messages received.
• **Decline**	Number of DHCP DECLINE messages received.
• **Release**	Number of DHCP RELEASE messages received.
• **Inform**	Number of DHCP INFORM messages received.

DHCP message Sent Counters

Object	Description
• **Offer**	Number of DHCP OFFER messages sent.
• **ACK**	Number of DHCP ACK messages sent.
• **NAK**	Number of DHCP NAK messages sent.

Buttons

Auto-refresh ☐ seconds. : Check this box to refresh the page automatically.

Apply : Click to apply changes

Reset : Click to undo any changes made locally and revert to previously saved values

4.2.5.5 Binding

This page displays bindings generated for DHCP clients. screen in Figure 4-2-47 appears.

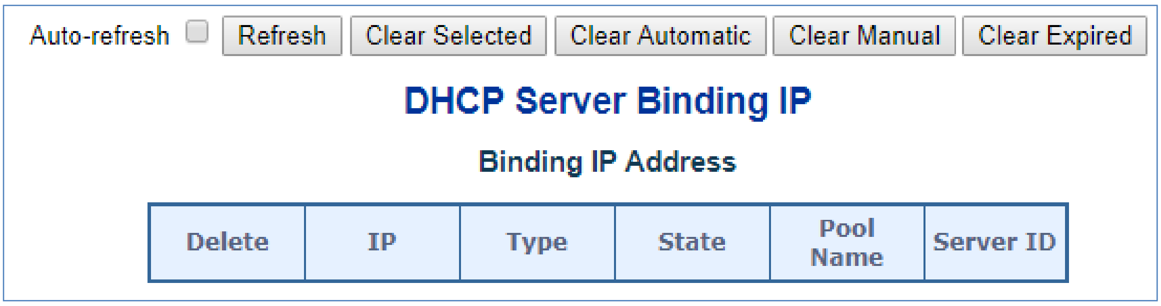


Figure 4-2-47: DHCP server Binding IP page Screenshot

The page includes the following fields:

Object	Description
• **IP**	Display IP address allocated to DHCP client.
• **Type**	Display type of binding. Possible types are Automatic, Manual, Expired.
• **State**	Display state of binding. Possible states are Committed, Allocated, Expired
• **Pool Name**	Display the pool that generates the binding.
• **Server ID**	Display server IP address to service the binding.

Buttons

Auto-refresh ☐ :: Check this box to refresh the page automatically

Refresh : Click to refresh the page immediately.

Clear Selected : Click to clear selected bindings. If the selected binding is Automatic or Manual, then it is changed to be Expired. If the selected binding is Expired, then it is freed.

Clear Automatic : Click to clear all Automatic bindings and Change them to Expired bindings.

Clear Manual : Click to clear all Manual bindings and Change them to Expired bindings.

Clear Expired : Click to clear all Expired bindings and free them.

4.2.5.6 Declined IP

This page displays declined IP addresses. screen in Figure 4-2-48 appears.

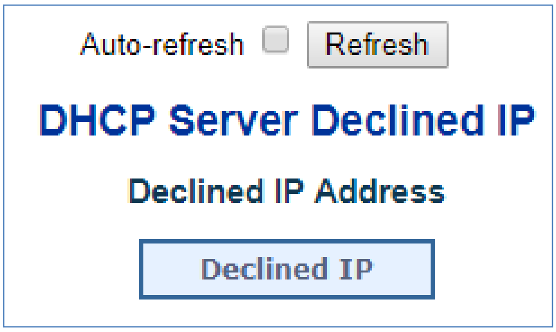


Figure 4-2-48: DHCP server Declined IP Page Screenshot

The page includes the following fields:

Object	Description
• **Delined IP**	Display List of IP addresses declined.

Buttons

Auto-refresh : Check this box to refresh the page automatically

Refresh : Click to refresh the page immediately.

4.2.6 Industrial Protocol

With the supported Modbus TCP/IP protocol, the **Industrial Managed TSN Device** can easily integrate with **SCADA** systems, **HMI** systems and other data acquisition systems in factory floors. It enable administrators to remotely monitor the industrial Ethernet switch's **operating information**, **port information** and **communication status**, thus easily achieving enhanced monitoring and maintenance of the entire factory.

4.2.6.1 Protocol Configuration

The Industrial Protocol Configuration are configured here.; screen in Figure 4-2-49 appears.

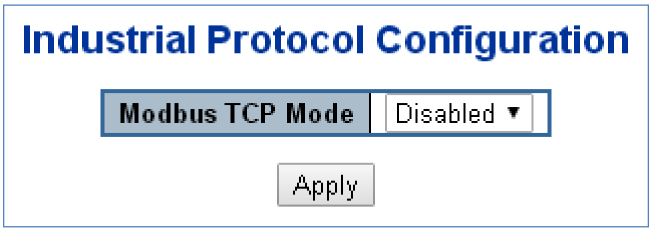


Figure 4-2-49: Protocol Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Modbus TCP Mode**	Indicates the modbus TCP mode operation. When the mode operation is enabled, the modbus TCP protocol will be activated. The modbus TCP protocol is based on TCP communication and received on TCP port 502. Possible modes are: ■ **Enabled**: Enable modbus TCP mode operation. ■ **Disabled**: Disable modbus TCP mode operation.

Buttons

: Click to apply changes

4.2.7 Remote Management

The Industrial Managed PoE+ Switch can support both NMS controller and CloudViewer Sever for remote management. PLANET's **NMS Controller** is a Network Management System can monitor all kinds of deployed network devices, such as Industrial Managed PoE+ Switches, media converters, routers, smart APs, VoIP phones, IP cameras, etc., compliant with the SNMP Protocol, ONVIF Protocol and PLANET Smart Discovery utility. The **CloudViewer** is a free networking service just for PLANET Products. This service provides simplified network monitoring and real-time network status. Working with PLANET CloudViewer app, user can easily check network status, device information, Port and PoE status from Internet. Any other services are not included.

4.2.7.1 Remote NMS Configuration

The Remote NMS Configuration screens in Figure 4-2-50 appear.

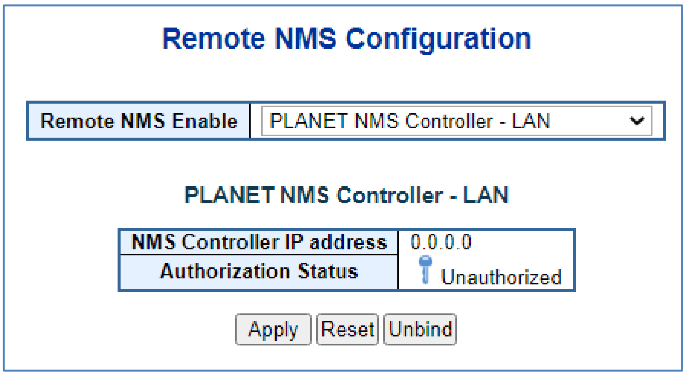


Figure 4-2-50: Remote NMS Configuration Page Screenshot

The PLANET NMS Controller – LAN Configuration screens in Figure 4-2-51 appear.

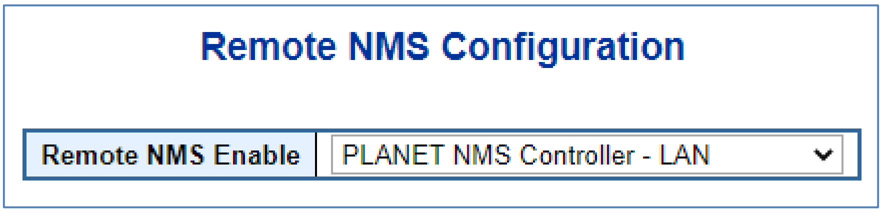


Figure 4-2-51: PLANET NMS Controller – LAN Configuration Page Screenshot

Object	Description
• **Remote NMS Enable**	Enable NMS management.
• **NMS Controller IP address**	The IP address of NMS Controller.
• **Authorization Status**	Indicate the authorization status of the switch to NMS Controller.

The CloudViewer Server – Internet screens in Figure 4-2-52 appear.

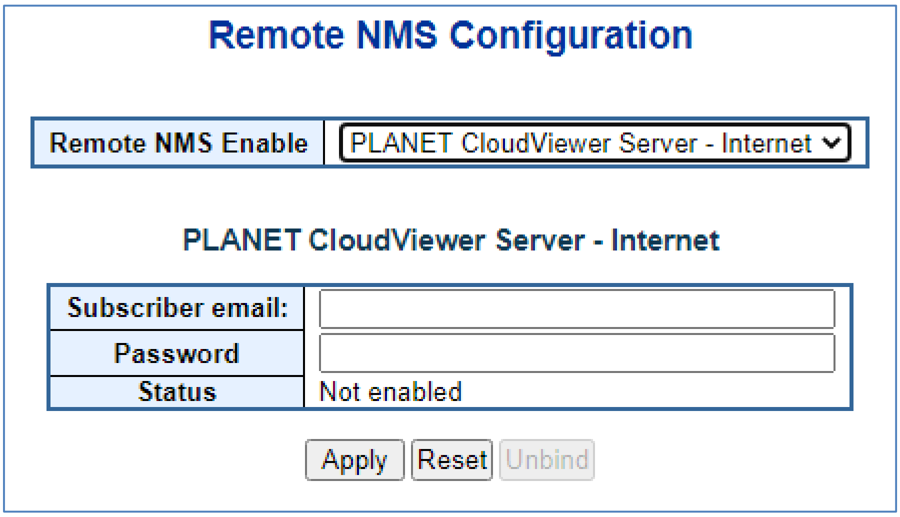
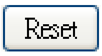


Figure 4-2-52: CloudViewer Server – Internet Configuration Page Screenshot

Object	Description
• **Remote NMS Enable**	Enable NMS management.
• **Subscriber email**	The email registered on CloudViewer Server.
• **Password**	The password of your CloudViewer account.
• **Status**	Indicate the status of connecting CloudViewer Server.

: Click to apply changes



: Click to undo any changes made locally and revert to previously saved values

4.3 Switching

4.3.1 Port Management

Use the Port Menu to display or configure the **Industrial Managed TSN Device's** ports. This section has the following items:

- **Port Configuration** — Configures port connection settings
- **Port Statistics Overview** — Lists Ethernet and RMON port statistics
- **Port Statistics Detail** — Lists Ethernet and RMON port statistics
- **SFP Module Information** — Display SFP information
- **Port Mirror** — Sets the source and target ports for mirroring

4.3.1.1 Port Configuration

This page displays current port configurations. Ports can also be configured here. The Port Configuration screen in Figure 4-3-1 appears.

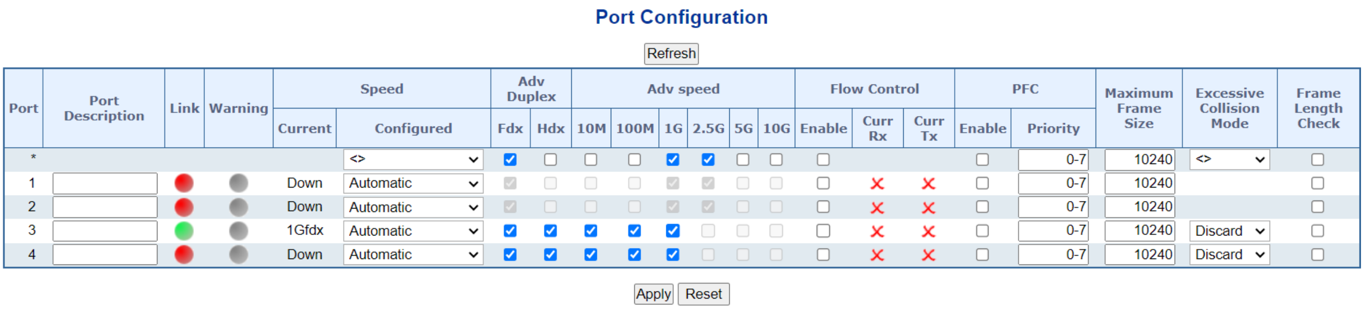


Figure 4-3-1: Port Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	This is the logical port number for this row.
• **Port Description**	Indicates the per port description.
• **Link**	The current link state is displayed graphically. Green indicates the link is up and red indicates the link is down.
• **Current Link Speed**	Provides the current link speed of the port.
• **Configured Link Speed**	Select any available link speed for the given switch port. Draw the menu bar to select the mode. ■ **Auto** - Set up Auto negotiation for copper interface. ■ **10Mbps HDX** - Force sets 10Mbps/Half-Duplex mode. ■ **10Mbps FDX** - Force sets 10Mbps/Full-Duplex mode. ■ **100Mbps HDX** - Force sets 100Mbps/Half-Duplex mode. ■ **100Mbps FDX** - Force sets 100Mbps/Full-Duplex mode.

	■ **1Gbps FDX** - Force sets 1000Mbps/Full-Duplex mode. ■ **2.5G FDX** - Forces sets 1Gbps/Full-Duplex mode. ■ **Disable** - Shut down the port manually.
• **Flow Control**	When **Auto Speed** is selected on a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. 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. Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.
• **Maximum Frame Size**	Enter the maximum frame size allowed for the switch port, including FCS. The allowed range is 1518 bytes to 10056 bytes.

Note

When setting each port to run at 100M Full-, 100M Half-, 10M Full-, and 10M Half-speed modes. The Auto-MDIX function will disable.

Buttons

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

Refresh: Click to refresh the page. Any changes made locally will be undone.

4.3.1.2 Port Statistics Overview

This page provides an overview of general traffic statistics for all switch ports. The Port Statistics Overview screen in Figure 4-3-2 appears.

Port Statistics Overview

Auto-refresh ☐ Refresh Clear

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	18586	10558	2937659	2531732	0	0	0	0	2733
4	0	0	0	0	0	0	0	0	0

Figure 4-3-2: Port Statistics Overview Page Screenshot

The displayed counters are:

Object	Description
• **Port**	The logical port for the settings contained in the same row.
• **Packets**	The number of received and transmitted packets per port.
• **Bytes**	The number of received and transmitted bytes per port.
• **Errors**	The number of frames received in error and the number of incomplete transmissions per port.
• **Drops**	The number of frames discarded due to ingress or egress congestion.
• **Filtered**	The number of received frames filtered by the forwarding process.

Buttons

Download: Download the Port Statistics Overview result in EXCEL file.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for all ports.

Print: Print the Port Statistics Overview result.

Auto-refresh ☐: Check this box to enable an automatic refresh of the page at regular intervals.

4.3.1.3 Port Statistics Details

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. The Detailed Port Statistics screen in Figure 4-3-3 appears.

Detailed Port Statistics Port 1

Port 1 Auto-refresh Refresh Clear

Receive Total		Transmit Total	
Rx Packets	2335	Tx Packets	2066
Rx Octets	431172	Tx Octets	1531131
Rx Unicast	2039	Tx Unicast	2050
Rx Multicast	48	Tx Multicast	11
Rx Broadcast	248	Tx Broadcast	5
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	1465	Tx 64 Bytes	242
Rx 65-127 Bytes	175	Tx 65-127 Bytes	53
Rx 128-255 Bytes	66	Tx 128-255 Bytes	523
Rx 256-511 Bytes	553	Tx 256-511 Bytes	203
Rx 512-1023 Bytes	76	Tx 512-1023 Bytes	284
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	761
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	2283	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	2066
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	52	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	52		

Figure 4-3-3: Detailed Port Statistics Port 1 Page Screenshot

The page includes the following fields:

Receive Total and Transmit Total

Object	Description
• **Rx and Tx Packets**	The number of received and transmitted (good and bad) packets
• **Rx and Tx Octets**	The number of received and transmitted (good and bad) bytes, including FCS, but excluding framing bits.
• **Rx and Tx Unicast**	The number of received and transmitted (good and bad) unicast packets.
• **Rx and Tx Multicast**	The number of received and transmitted (good and bad) multicast packets.
• **Rx and Tx Broadcast**	The number of received and transmitted (good and bad) broadcast packets.
• **Rx and Tx Pause**	A count of the MAC Control frames received or transmitted on this port that has an opcode indicating a PAUSE operation.

Receive and Transmit Size Counters

The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

Receive and Transmit Queue Counters

The number of received and transmitted packets per input and output queue.

Receive Error Counters

Object	Description
• **Rx Drops**	The number of frames dropped due to lack of receive buffers or egress congestion.
• **Rx CRC/Alignment**	The number of frames received with CRC or alignment errors.
• **Rx Undersize**	The number of short frames received with valid CRC.
• **Rx Oversize**	The number of long frames received with valid CRC.
• **Rx Fragments**	The number of short frames received with invalid CRC.
• **Rx Jabber**	The number of long frames received with invalid CRC.
• **Rx Filtered**	The number of received frames filtered by the forwarding process. Short frames are frames that are smaller than 64 bytes. Long frames are frames that are longer than the configured maximum frame length for this port.

1 Short frames are frames that are smaller than 64 bytes.

2 Long frames are frames that are longer than the configured maximum frame length for this port.

Transmit Error Counters

Object	Description
• **Tx Drops**	The number of frames dropped due to output buffer congestion.
• **Tx Late/Exc. Coll.**	The number of frames dropped due to excessive or late collisions.

Buttons

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for all ports.

Auto-refresh ☐: Check this box to enable an automatic refresh of the page at regular intervals.

4.3.1.4 Port Mirror

Configure port Mirroring on this page. This function provides monitoring network traffic that forwards a copy of each incoming or outgoing packet from one port of a network Switch to another port where the packet can be studied. It enables the manager to keep close track of switch performance and alter it if necessary.

- To debug network problems, selected traffic can be copied, or mirrored, to a mirror port where a frame analyzer can be attached to analyze the frame flow.
- The **Industrial Managed TSN Device** can unobtrusively mirror traffic from any port to a monitor port. You can then attach a protocol analyzer or RMON probe to this port to perform traffic analysis and verify connection integrity.

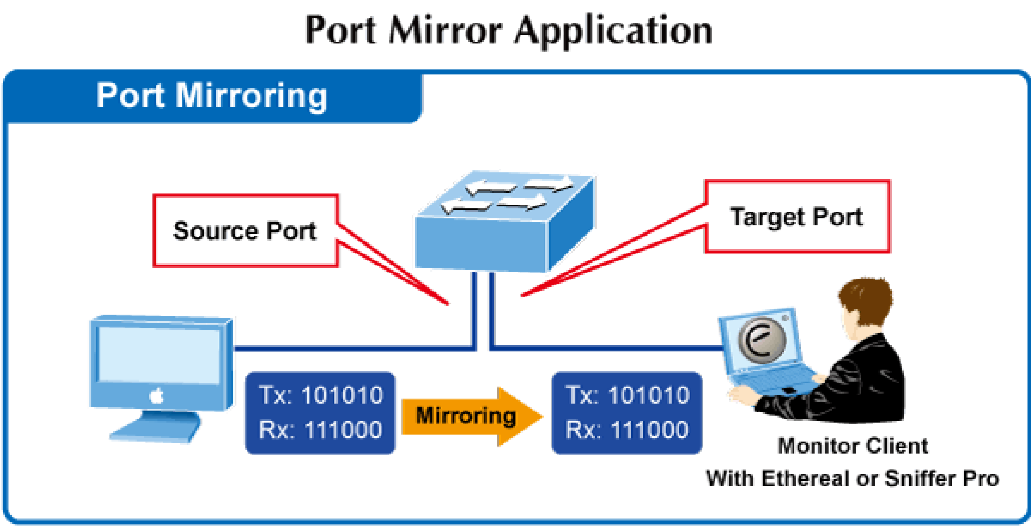


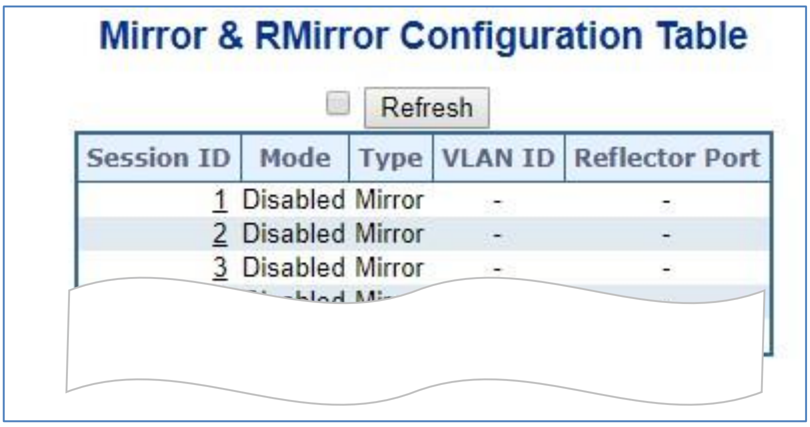
Figure 4-3-4: Port Mirror Application

The traffic to be copied to the mirror port is selected as follows:

- All frames received on a given port (also known as ingress or source mirroring).
- All frames transmitted on a given port (also known as egress or destination mirroring).

Mirror Port Configuration

The Port Mirror screen in Figure 4-3-5 appears.and click the session ID to Figure 4-3-6



Mirror & RMirror Configuration Table

Refresh

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

Figure 4-3-5: Mirror Configuration Page Screenshot

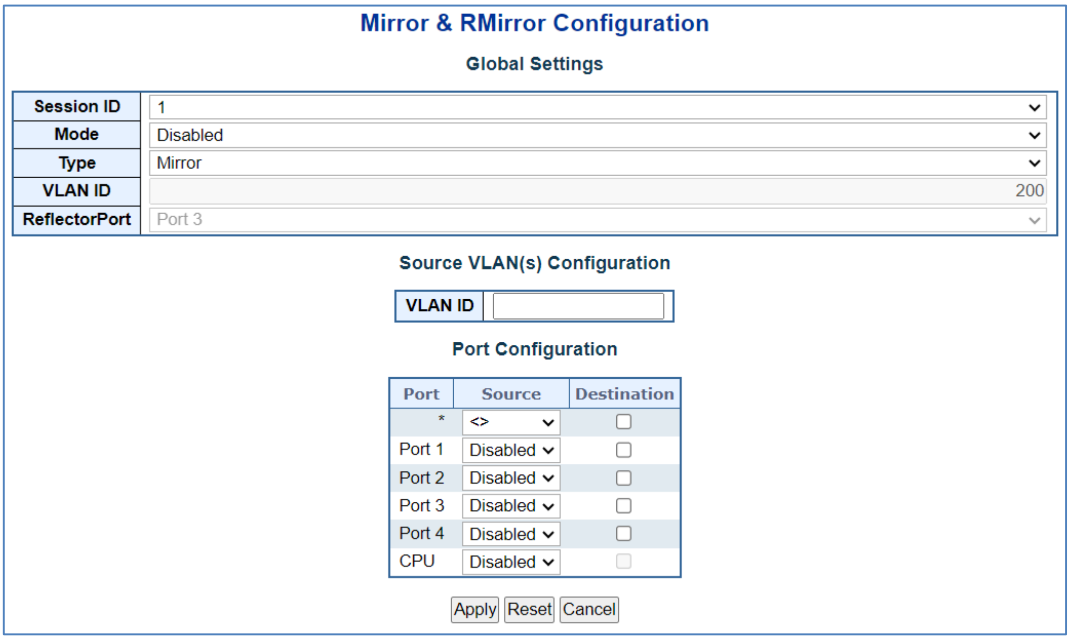


Figure 4-3-6: Mirror Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Session**	Select session id to configure.
• **Mode**	To Enabled/Disabled the mirror or Remote Mirroring function
• **Type**	**Mirror** The switch is running on mirror mode. The source port(s) and destination port are located on this switch. **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.
• **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
• **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.
• **Remote Mirroring Port Configuration**	The following table is used for port role selecting. ■ **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.

Note

For a given port, a frame is only transmitted once. It is therefore not possible to mirror Tx frames on the **mirror port**. Because of this, **mode** for the selected mirror port is limited to **Disabled** or **Rx only**.

Buttons

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.1.5 Name Map

Interface Name to Port Number Map Help

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.

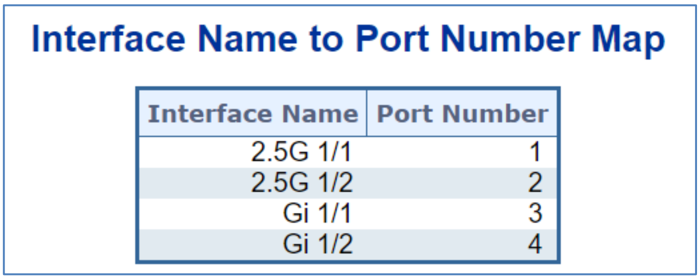


Figure 4-3-7: Name Map Page Screenshot

4.3.1.6 DDMI (TSN-5225-4T2S/TSN-900-2T2S only)

Configure DDMI on this page.

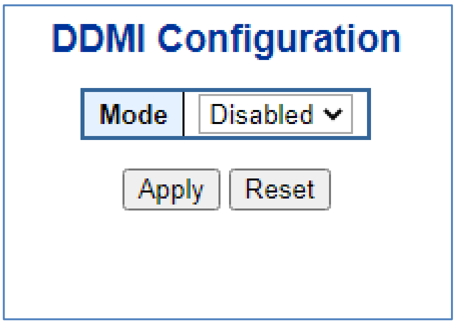


Figure 4-3-8: DDMI Page Screenshot

The displayed settings are:

Object	Description
• **Mode**	Indicates the DDMI mode operation. Possible modes are: **Enabled**: Enable DDMI mode operation. **Disabled**: Disable DDMI mode operation.

Buttons

Apply : Click to apply changes

Reset : Click to undo any changes made locally and revert to previously saved values.

4.3.1.7 DDMI Over View (TSN-5225-4T2S/TSN-900-2T2S only)

Display DDMI overview information on this page.

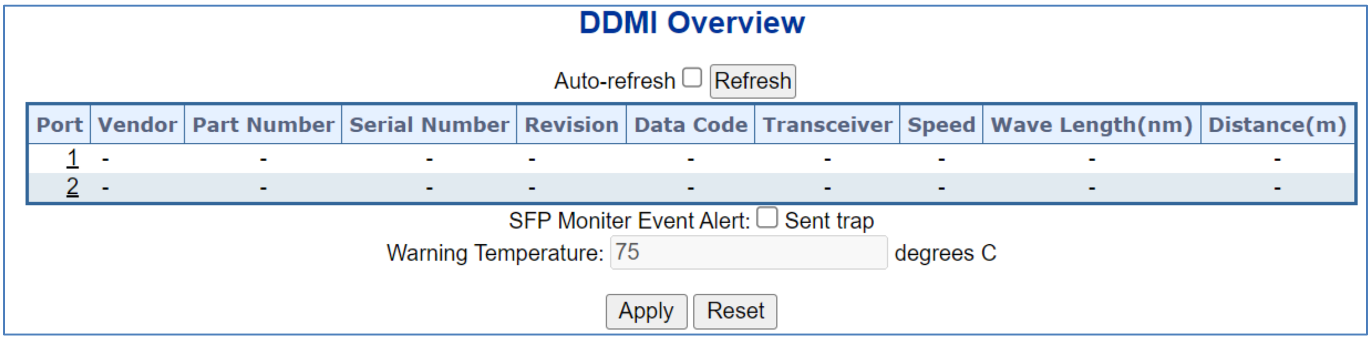


Figure 4-3-9: DDMI Overview Page Screenshot

The displayed settings are:

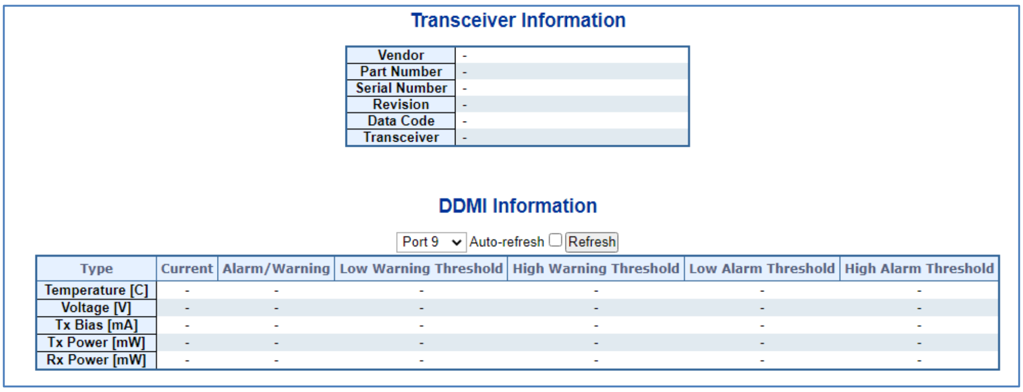
Object	Description
• **Port**	DDMI port.
• **Vendor**	Indicates Vendor name SFP vendor name.
• **Part Number**	Indicates Vendor PN Part number provided by SFP vendor.
• **Serial Number**	Indicates Vendor SN Serial number provided by vendor.
• **Revision**	Indicates Vendor rev Revision level for part number provided by vendor.
• **Data Code**	Indicates Date code Vendor's manufacturing date code.
• **Transceiver**	Indicates Transceiver compatibility.
• **speed**	Display speed data
• **Wave Length**	Display Wave Length data
• **Distance**	Display Distance data
• **SFP Event Alert Monitoring**	This option is for user to make a temperature monitoring trap that if SFP module operating temperature is over the warning limit, a system log will be issued.
• **Warning Temperature**	This option is for use to set a temperature control trap for the SFP module. When the operating temperature of the SFP module reaches the warning limit, an alarm log will be issued.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.3.1.8 DDMI Detailed (TSN-5225-4T2S/TSN-900-2T2S only)

Display DDMI detailed information on this page.



Transceiver Information

Vendor	-
Part Number	-
Serial Number	-
Revision	-
Data Code	-
Transceiver	-

DDMI Information

Port 9 Auto-refresh Refresh

Type	Current	Alarm/Warning	Low Warning Threshold	High Warning Threshold	Low Alarm Threshold	High Alarm Threshold
Temperature [C]	-	-	-	-	-	-
Voltage [V]	-	-	-	-	-	-
Tx Bias [mA]	-	-	-	-	-	-
Tx Power [mW]	-	-	-	-	-	-
Rx Power [mW]	-	-	-	-	-	-

Figure 4-3-10: DDMI Detailed Page Screenshot

The displayed settings are:

Object	Description
• **Vendor**	Indicates SFP vendor name.
• **Part Number**	Indicates part number provided by SFP vendor.
• **Serial Number**	Indicates part number provided by SFP vendor.
• **Revision**	Indicates revision level for part number provided by SFP vendor.
• **Data Code**	Indicates vendor's manufacturing date code.
• **Transceiver**	Indicates SFP transceiver compatibility.
• **DDMI Infomration**	Display DDMI infomration on this page.
• **Current**	The current value of temperature, voltage, Tx bias, Tx power, and Rx power.
• **Alarm/Warning**	Indicates whether there is an alarm or warning.
• **Low Warning Threshold**	The low warning threshold value of temperature, voltage, Tx bias, Tx power, and Rx power.
• **High Warning Threshold**	The high warning threshold value of temperature, voltage, Tx bias, Tx power, and Rx power.
• **Low Alarm Threshold**	The low alarm threshold value of temperature, voltage, Tx bias, Tx power, and Rx power.
• **High Alarm Threshold**	The high alarm threshold value of temperature, voltage, Tx bias, Tx power, and Rx power.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.3.2 Link Aggregation

Port Aggregation optimizes port usage by linking a group of ports together to form a single Link Aggregated Groups (LAGs). Port Aggregation multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy.

Each LAG is composed of ports of the same speed, set to full-duplex operations. Ports in a LAG, can be of different media types (UTP/Fiber, or different fiber types), provided they operate at the same speed.

Aggregated Links can be assigned manually (**Port Trunk**) or automatically by enabling Link Aggregation Control Protocol (**LACP**) on the relevant links.

Aggregated Links are treated by the system as a single logical port. Specifically, the Aggregated Link has similar port attributes to a non-aggregated port, including auto-negotiation, speed, Duplex setting, etc.

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.

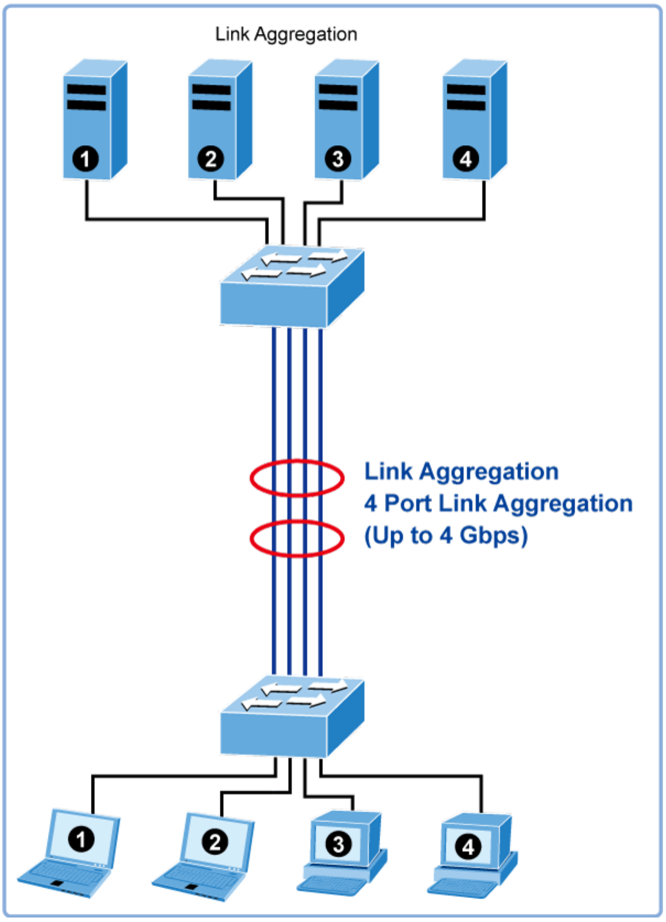


Figure 4-3-11: Link Aggregation

The **Link Aggregation Control Protocol** (**LACP**) provides a standardized means for exchanging information between Partner Systems that require high speed redundant links. Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. LACP operation requires full-duplex mode, more detail information refer to the IEEE 802.3ad standard.

Port link aggregations can be used to increase the bandwidth of a network connection or to ensure fault recovery. Link aggregation lets you group up to 4 consecutive ports into a single dedicated connection between any two the Switch or other Layer 2 switches. However, before making any physical connections between devices, use the Link aggregation Configuration menu to specify the link aggregation on the devices at both ends. When using a port link aggregation, note that:

- The ports used in a link aggregation must all be of the same media type (RJ45, 100 Mbps fiber).
- The ports that can be assigned to the same link aggregation have certain other restrictions (see below).
- Ports can only be assigned to one link aggregation.
- The ports at both ends of a connection must be configured as link aggregation ports.
- None of the ports in a link aggregation can be configured as a mirror source port or a mirror target port.
- All of the ports in a link aggregation have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- The Spanning Tree Protocol will treat all the ports in a link aggregation as a whole.
- Enable the link aggregation prior to connecting any cable between the switches to avoid creating a data loop.
- Disconnect all link aggregation port cables or disable the link aggregation ports before removing a port link aggregation to avoid creating a data loop.

It allows a maximum of 10 ports to be aggregated at the same time. The **Industrial Managed TSN Device** support Gigabit Ethernet ports (up to 5 groups). If the group is defined as a LACP static link aggregation group, then any extra ports selected are placed in a standby mode for redundancy if one of the other ports fails. If the group is defined as a local static link aggregation group, then the number of ports must be the same as the group member ports.

The aggregation code ensures that frames belonging to the same frame flow (for example, a TCP connection) are always forwarded on the same link aggregation member port. Recording of frames within a flow is therefore not possible. The aggregation code is based on the following information:

- **Source MAC**
- **Destination MAC**
- **Source and destination IPv4 address.**
- **Source and destination TCP/UDP ports for IPv4 packets**

Normally, all 5 contributions to the aggregation code should be enabled to obtain the best traffic distribution among the link aggregation member ports. Each link aggregation may consist of up to 10 member ports. Any quantity of link aggregation s may be configured for the device (only limited by the quantity of ports on the device.) To configure a proper traffic distribution, the ports within a link aggregation must use the same link speed.

4.3.2.1 Common

This page is used to configure the Aggregation hash mode and the aggregation group. The aggregation hash mode settings are global.

Hash Code Contributors

The Common Aggregation Configuration screen in Figure 4-3-12 appears.

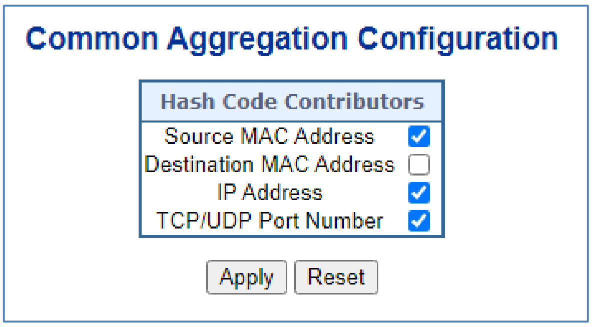


Figure 4-3-12: Common Aggregation Configuration Page Screenshot

The page includes the following fields:

Object	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.

4.3.2.2 Groups

This page is used to configure the Aggregation hash mode and the aggregation group. The aggregation hash mode settings are global.

The Aggregation Group Configuration screen in Figure 4-3-13 appears.

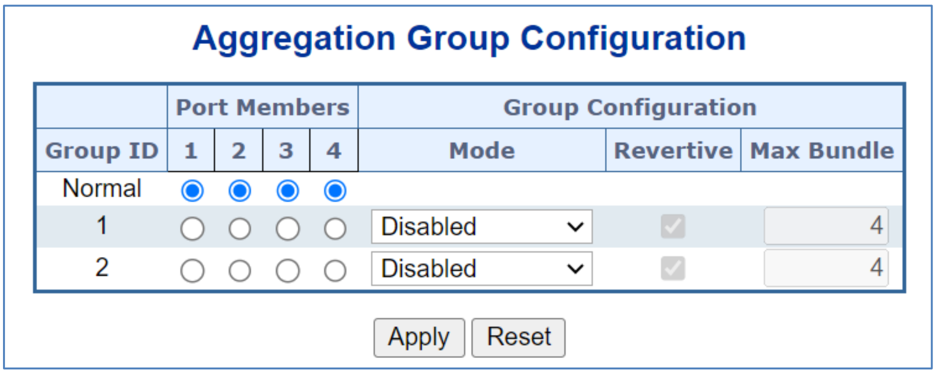


Figure 4-3-13: Aggregation Group Configuration Page Screenshot

The page includes the following fields:

.Object	Description
• **Group ID**	Indicates the 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.

Buttons

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.2.3 Aggregation Status

This page is used to see the staus of ports in Aggregation group. The Static Aggregation Status screen in Figure 4-3-14 appears.

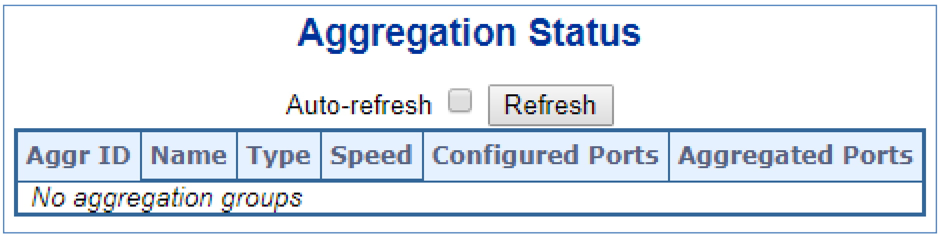


Figure 4-3-14: LACP Port Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Aggr ID**	Display the Aggregation ID associated with this aggregation instance.
• **Name**	Display the Name of the Aggregation group ID.
• **Type**	Display the type of the Aggregation group(Static or LACP).
• **Speed**	Display the Speed of the Aggregation group.
• **Configured Ports**	Display the Configured member ports of the Aggregation group.
• **Aggregated Ports**	Display the Aggregated member ports of the Aggregation group.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh : Automatic refresh occurs every 3 seconds.

4.3.2.4 LACP Configuration

Link Aggregation Control Protocol (LACP) - LACP LAG negotiate Aggregated Port links with other LACP ports located on a different device. LACP allows switches connected to each other to discover automatically whether any ports are member of the same LAG.

This page allows the user to inspect the current LACP port configurations, and possibly change them as well. The LACP Configuration screen in Figure 4-3-15 appears.

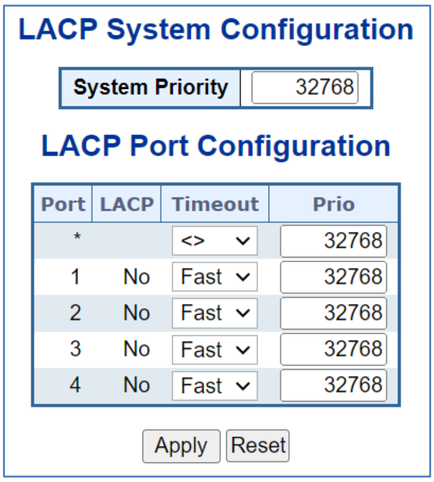


Figure 4-3-15: LACP Port Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number.
• **LACP Enabled**	Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner.
• **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.
• **Priority**	The Priority controls the priority of the port. 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.

Buttons

: Click to apply changes

: Click to undo any changes made locally and revert to previously saved values.

4.3.2.5 LACP System Status

This page provides a status overview of all LACP instances. The LACP Status Page display the current LACP aggregation Groups and LACP Port status. The LACP System Status screen in Figure 4-3-16 appears.

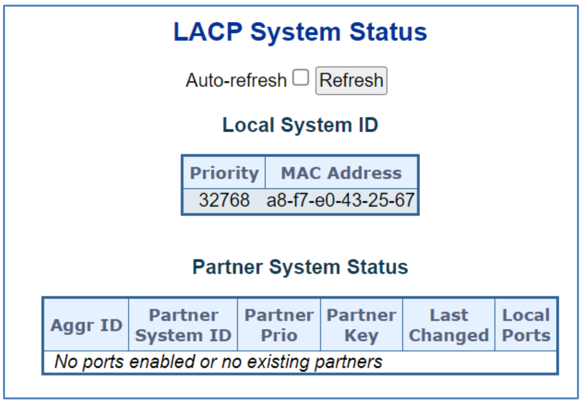


Figure 4-3-16: LACP System Status Page Screenshot

The page includes the following fields:

Object	Description
• **Aggr ID**	The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'
• **Partner System ID**	The system ID (MAC address) of the aggregation partner.
• **Partner Key**	The Key that the partner has assigned to this aggregation ID.
• **Partner Priority**	The priority of the aggregation partner.
• **Last Changed**	The time since this aggregation changed.
• **Local Ports**	Shows which ports are a part of this aggregation for this switch.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh: Automatic refresh occurs every 3 seconds.

4.3.2.6 LACP Internal Port Status

This page provides a status overview of LACP status for all ports. The LACP Internal Port Status screen in Figure 4-3-17 appears.

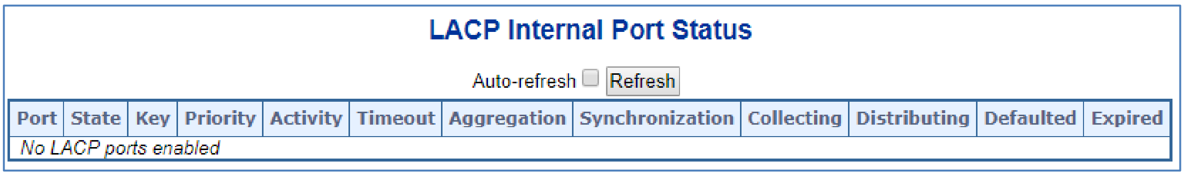


Figure 4-3-17: LACP Status Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number.
• **State**	The current port state: ● Down: The port is not active. ● Active: The port is in active state. ● Standby: The port is in standby state.
• **Key**	The key assigned to this port. Only ports with the same key can aggregate together.
• **Priority**	The priority assigned to this aggregation group.
• **Activity**	The LACP mode of the group (Active or Passive).
• **Timeout**	The timeout mode configured for the port (Fast or Slow).
• **Aggregation**	Show whether the system considers this link to be "aggregateable"; i.e., a potential candidate for aggregation.
• **Synchronization**	Show whether the system considers this link to be "IN_SYNC"; i.e., it has been allocated to the correct LAG, the group has been associated with a compatible Aggregator, and the identity of the LAG is consistent with the System ID and operational Key information transmitted.
• **Collecting**	Show if collection of incoming frames on this link is enabled.
• **Distributing**	Show if distribution of outgoing frames on this link is enabled.
• **Defaulted**	Show if the Actor's Receive machine is using Defaulted operational Partner information.
• **Expired**	Show if that the Actor's Receive machine is in the EXPIRED state.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh ☐: Automatic refresh occurs every 3 seconds.

4.3.2.7 LACP Neighbor Port Status

This page provides a status overview of LACP status for all ports. The LACP Internal Port Status screen in Figure 4-3-18 appears.

Figure 4-3-18: LACP Neighbor Port Status Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number.
• **State**	The current port state: ● Down: The port is not active. ● Active: The port is in active state. ● Standby: The port is in standby state.
• **Aggr ID**	The aggregation group ID which the port is assigned to.
• **Partner Key**	The key assigned to this port by the partner.
• **Partner Priority**	The priority assigned to this partner port .
• **Activity**	The LACP mode of the group (Active or Passive).
• **Timeout**	The timeout mode configured for the port (Fast or Slow).
• **Aggregation**	Show whether the system considers this link to be "aggregateable"; i.e., a potential candidate for aggregation.
• **Synchronization**	Show whether the system considers this link to be "IN_SYNC"; i.e., it has been allocated to the correct LAG, the group has been associated with a compatible Aggregator, and the identity of the LAG is consistent with the System ID and operational Key information transmitted.
• **Collecting**	Show if collection of incoming frames on this link is enabled.
• **Distributing**	Show if distribution of outgoing frames on this link is enabled.
• **Defaulted**	Show if the Actor's Receive machine is using Defaulted operational Partner information.
• **Expired**	Show if that the Actor's Receive machine is in the EXPIRED state.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh : Automatic refresh occurs every 3 seconds.

4.3.3 VLAN

4.3.3.1 VLAN Overview

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLAN also logically segment the network into different broadcast domains so that packets are forwarded only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

VLAN can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

A VLAN is a collection of end nodes grouped by logic instead of physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated.

Note

1. No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLAN without a network device performing a routing function between the VLANs.
2. The **Industrial Managed TSN Device** supports IEEE 802.1Q VLAN. The port untagging function can be used to remove the 802.1 tag from packet headers to maintain compatibility with devices that are tag-unaware..

Note

The **Industrial Managed TSN Device** 's default is to assign all ports to a single 802.1Q VLAN named DEFAULT_VLAN. As new VLAN is created, the member ports assigned to the new VLAN will be removed from the DEFAULT_ VLAN port member list. The DEFAULT_VLAN has a VID = 1.

This section has the following items:

■ **VLAN Port Configuration**	Enables VLAN group
■ **VLAN Membership Status**	Displays VLAN membership status
■ **VLAN Port Status**	Displays VLAN port status
■ **Private VLAN**	Creates/removes primary or community VLANs
■ **Port Isolation**	Enables/disablse port isolation on port
■ **MAC-based VLAN**	Configures the MAC-based VLAN entries
■ **MAC-based VLAN Status**	Displays MAC-based VLAN entries
■ **Protocol-based VLAN**	Configures the protocol-based VLAN entries
■ **Protocol-based VLAN Membership**	Displays the protocol-based VLAN entries

4.3.3.2 IEEE 802.1Q VLAN

In large networks, routers are used to isolate broadcast traffic for each subnet into separate domains. This **Industrial Managed TSN Device** provides a similar service at Layer 2 by using VLANs to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group, and can eliminate broadcast storms in large networks. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as videoconferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

This **Industrial Managed TSN Device** supports the following VLAN features:

- Up to 255 VLANs based on the IEEE 802.1Q standard
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging

IEEE 802.1Q Standard

IEEE 802.1Q (tagged) VLAN is implemented on the Switch. 802.1Q VLAN requires tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

VLAN allows a network to be segmented in order to reduce the size of broadcast domains. All packets entering a VLAN will only be forwarded to the stations (over IEEE 802.1Q enabled switches) that are members of that VLAN, and this includes broadcast, multicast and unicast packets from unknown sources.

VLAN can also provide a level of security to your network. IEEE 802.1Q VLAN will only deliver packets between stations that are members of the VLAN. Any port can be configured as either **tagging** or **untagging**.:

- The untagging feature of IEEE 802.1Q VLAN allows VLAN to work with legacy switches that don't recognize VLAN tags in packet headers.

- The tagging feature allows VLAN to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

Some relevant terms:

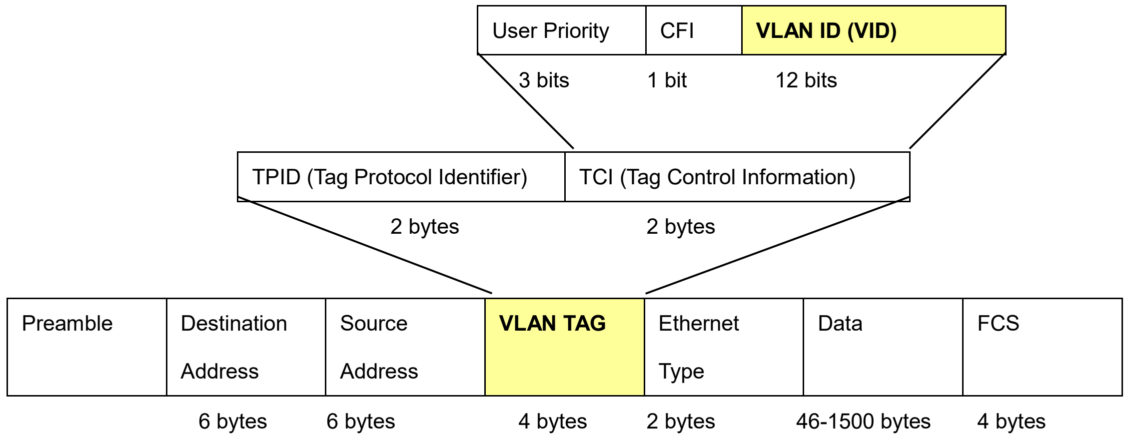
- **Tagging** - The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** - The act of stripping 802.1Q VLAN information out of the packet header.

802.1Q VLAN Tags

The figure below shows the 802.1Q VLAN tag. There are four additional octets inserted after the source MAC address. Their presence is indicated by a value of **0x8100** in the Ether Type field. When a packet's Ether Type field is equal to 0x8100, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of 3 bits of user priority, 1 bit of Canonical Format Identifier (CFI - used for encapsulating Token Ring packets so they can be carried across Ethernet backbones), and 12 bits of **VLAN ID (VID)**. The 3 bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLAN can be identified.

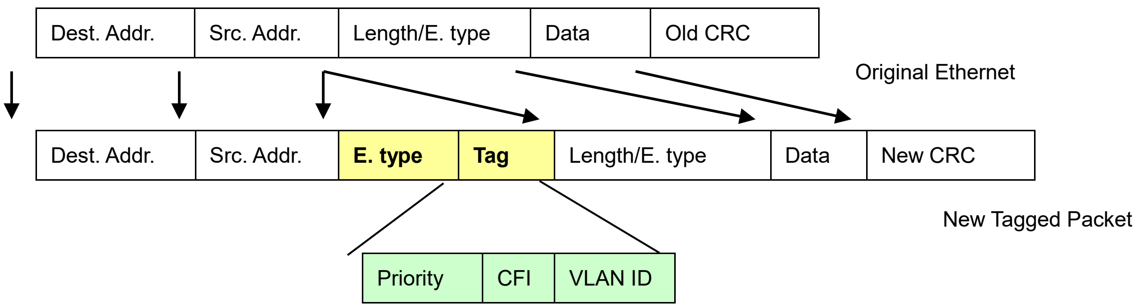
The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

802.1Q Tag



The Ether Type and VLAN ID are inserted after the MAC source address, but before the original Ether Type/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.

Adding an IEEE802.1Q Tag



Port VLAN ID

Packets that are tagged (are carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This allows 802.1Q VLAN to span network devices (and indeed, the entire network – if all network devices are 802.1Q compliant).

Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID, for use within the switch. If no VLAN are defined on the switch, all ports are then assigned to a default VLAN with a PVID equal to 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID, in so far as VLAN are concerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the PVID is not used to make packet forwarding decisions, the VID is.

Tag-aware switches must keep a table to relate PVID within the switch to VID on the network. The switch will compare the VID of a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VID are different the switch will drop the packet. Because of the existence of the PVID for untagged packets and the VID for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network.

A switch port can have only one PVID, but can have as many VID as the switch has memory in its VLAN table to store them.

Because some devices on a network may be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted – should the packet to be transmitted have a tag or not? If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

Default VLANs

The Switch initially configures one VLAN, VID = 1, called **"default."** The factory default setting assigns all ports on the Switch to the **"default"**. As new VLAN are configured in Port-based mode, their respective member ports are removed from the "default."

Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

Note	VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags should be stripped off before passing it on to any end-node host that does not support VLAN tagging.

■ VLAN Classification

When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the default VLAN ID of the receiving port). But if the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

■ Port Overlapping

Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by enabled routing on this switch.

■ Untagged VLANs

Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets.

4.3.3.3 VLAN Port Configuration

This page is used for configuring the **Industrial Managed TSN Device** port VLAN. The VLAN per Port Configuration page contains fields for managing ports that are part of a VLAN. The port default VLAN ID (PVID) is configured on the VLAN Port Configuration page. All untagged packets arriving to the device are tagged by the ports PVID.

Understanding nomenclature of the Switch

IEEE 802.1Q Tagged and Untagged

Every port on an 802.1Q compliant switch can be configured as tagged or untagged.

- **Tagged:** Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into those ports. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag can then be used by other 802.1Q compliant devices on the network to make packet-forwarding decisions.
- **Untagged:** Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the Switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

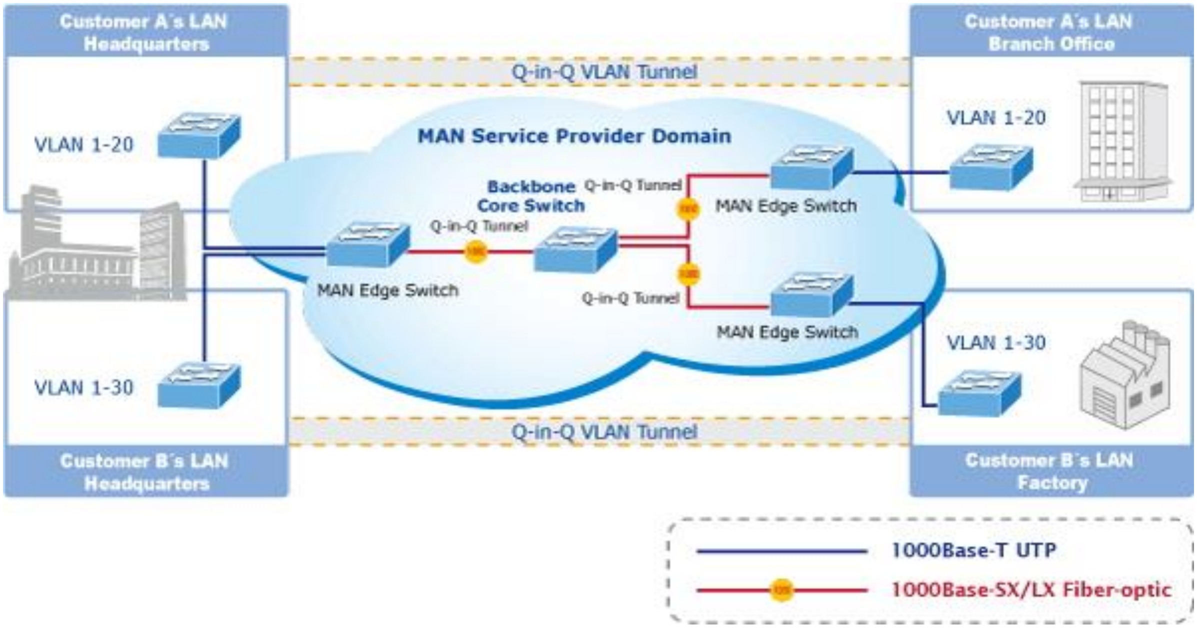
Frame Income / Frame Leave	Income Frame is **tagged**	Income Frame is **untagged**
Leave port is tagged	Frame remains tagged	Tag is inserted
Leave port is untagged	Tag is removed	Frame remain untagged

Table 4-3-1: Ingress / Egress Port with VLAN VID Tag / Untag Table

IEEE 802.1Q Tunneling (Q-in-Q)

IEEE 802.1Q Tunneling (Q-in-Q) is designed for service providers carrying traffic for multiple customers across their networks. Q-in-Q tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting **Service Provider VLAN (SPVLAN)** tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.

A service provider's customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4096.



The **Industrial Managed TSN Device** supports multiple VLAN tags and can therefore be used in MAN applications as a provider bridge, aggregating traffic from numerous independent customer LANs into the **MAN (Metro Access Network)** space. One of the purposes of the provider bridge is to recognize and use VLAN tags so that the VLANs in the MAN space can be used independent of the customers' VLANs. This is accomplished by adding a VLAN tag with a MAN-related VID for frames entering the MAN. When leaving the MAN, the tag is stripped and the original VLAN tag with the customer-related VID is again available.

This provides a tunneling mechanism to connect remote costumer VLANs through a common MAN space without interfering with the VLAN tags. All tags use EtherType **0x8100** or **0x88A8**, where 0x8100 is used for customer tags and 0x88A8 are used for service provider tags.

In cases where a given service VLAN only has two member ports on the switch, the learning can be disabled for the particular VLAN and can therefore rely on flooding as the forwarding mechanism between the two ports. This way, the MAC table requirements is reduced.

Global VLAN Configuration

The Global VLAN Configuration screen in Figure 4-3-19 appears.

Global VLAN Configuration

Allowed Access VLANs	1
Ethertype for Custom S-ports	88A8

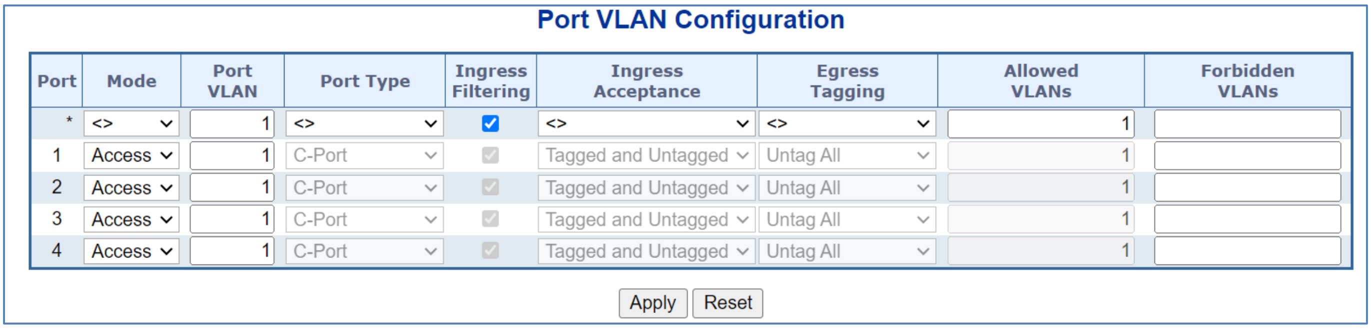
Figure 4-3-19: Global VLAN Configuration Screenshot

The page includes the following fields:

Object	Description
• **Allowed Access VLANs**	This field shows the allowed Access VLANs, it only affects ports configured as Access ports. Ports in other modes are members of all VLANs specified in the Allowed VLANs field. By default, only VLAN 1 is enabled. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: **1,10-13,200,300**. Spaces are allowed in between the delimiters.
• **Ethertype for Custom S-ports**	This field specifies the ethertype/TPID (specified in hexadecimal) 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

The VLAN Port Configuration screen in Figure 4-3-20 appears.


Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

Apply Reset

Figure 4-3-20: Port VLAN Configuration Screenshot

The page includes the following fields:

Object		Description
• **Port**		This is the logical port number for this row.
• **Mode**	**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 (Access VLAN), which by default is 1 • Accepts untagged and C-tagged frames • Discards all frames that are not classified to the Access VLAN

		• On egress all frames classified to the Access VLAN are transmitted untagged. Other (dynamically added VLANs) are transmitted tagged
	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 (1-4095) • 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**		Determines the **port's VLAN ID** (**PVID**). Allowed VLANs are in the range 1 through 4095, default being 1. ■ On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0). ■ On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN. The Port VLAN is called an "**Access VLAN**" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.
• **Port Type**		Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required. ■ **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 ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 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 an S-tag. ■ **S-Custom-Port:** On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S ports 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 the custom S-tag.
• **Ingress Filtering**	Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled. ■ If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded. ■ If ingress filtering is 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**	Hybrid ports allow for changing the type of frames that are accepted on ingress. ■ **Tagged and Untagged** Both tagged and untagged frames are accepted. ■ **Tagged Only** Only tagged frames are accepted on ingress. Untagged frames are discarded. ■ **Untagged Only** Only untagged frames are accepted on ingress. Tagged frames are discarded.
Egress Tagging	This option is only available for ports in Hybrid mode. Ports in Trunk and Hybrid mode may control the tagging of frames on egress. ■ **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.
• **Allowed VLANs**	Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. The field's syntax is identical to the syntax used in the Enabled VLANs field. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to **1-4095**. The field may be left empty, which means that the port will not become member of any VLANs.
• **Forbidden VLANs**	A port may be configured to never be member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs. The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Enabled VLANs field. By default, the field is left blank, which means that the port may become a member of all possible VLANs.

Note

The port must be a member of the same VLAN as the Port VLAN ID.

Buttons

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.3.4 VLAN Membership Status

This page provides an overview of membership status for VLAN users. The VLAN Membership Status screen in Figure 4-3-21 appears.

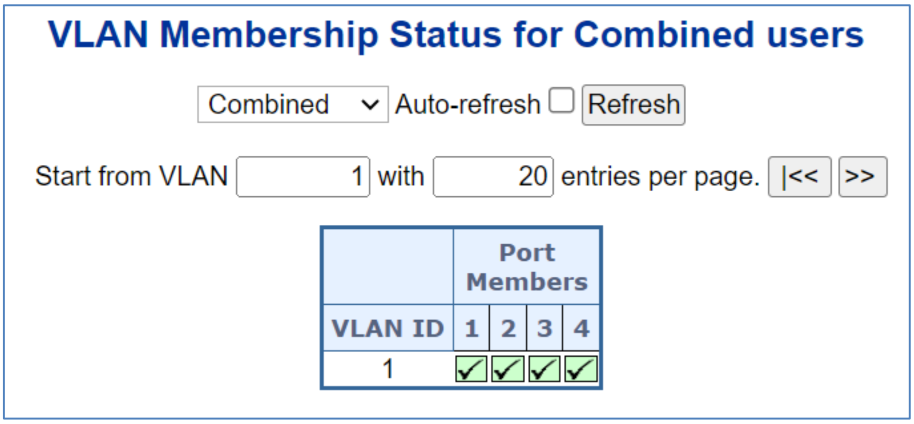


Figure 4-3-21: VLAN Membership Status for Static User Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN User**	A VLAN User is a module that uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configuration such as PVID, UVID. Currently we support following VLAN : - **Admin** : This is referred as static. - **NAS** : NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server. - **GVRP** : GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network . - **Voice VLAN** : Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones. - **MVR** : MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.
• **Port Members**	A row of check boxes for each port is displayed for each VLAN ID. If a port is included in a VLAN, an image will be displayed. If a port is included in a Forbidden port list, an image will be displayed. If a port is included in a Forbidden port list and dynamic VLAN user register VLAN on same Forbidden port, then conflict port will be displayed as conflict port.
• **VLAN Membership**	The VLAN Membership Status page shall show the current VLAN port members

	for all VLANs configured by a selected VLAN User (selection shall be allowed by a Combo Box). When ALL VLAN Users are selected, it shall show this information for all the VLAN Users, and this is by default. VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.

Buttons

Combined: Select VLAN Users from this drop down list.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

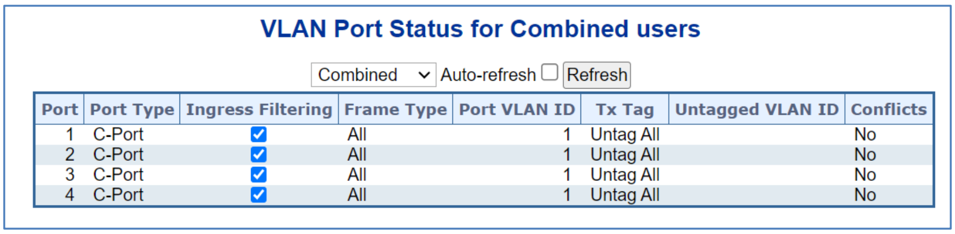
Refresh: Click to refresh the page immediately.

|<<: Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.

>>: Updates the table, starting with the entry after the last entry currently displayed.

4.3.3.5 VLAN Port Status

This page provides VLAN Port Status. The VLAN Port Status screen in Figure 4-3-22 appears.


VLAN Port Status for Combined users

Combined Auto-refresh Refresh

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	☑	All	1	Untag All		No
2	C-Port	☑	All	1	Untag All		No
3	C-Port	☑	All	1	Untag All		No
4	C-Port	☑	All	1	Untag All		No

Figure 4-3-22: VLAN Port Status for Combined users Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The logical port for the settings contained in the same row.
• **Port Type**	Show the VLAN Awareness for the port. If VLAN awareness is enabled, the tag is removed from tagged frames received on the port. VLAN tagged frames are classified to the VLAN ID in the tag. If VLAN awareness is disabled, all frames are classified to the Port VLAN ID and tags are not removed.
• **Ingress Filtering**	Show the ingress filtering for a port. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded.
• **Frame Type**	Shows whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on that port are discarded.
• **Port VLAN ID**	Shows the PVID setting for the port.
• **Tx Tag**	Shows egress filtering frame status whether tagged or untagged.
• **Untagged VLAN ID**	Shows UVID (untagged VLAN ID). Port's UVID determines the packet's behavior at the egress side.
• **Conflicts**	Shows status of Conflicts whether exists or Not. When a Volatile VLAN User requests to set VLAN membership or VLAN port configuration, the following conflicts can occur: ■ Functional Conflicts between feature. ■ Conflicts due to hardware limitation. ■ Direct conflict between user modules.

Buttons

Static: Select VLAN Users from this drop down list.

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4.3.3.6 SVL

This page allows for controlling SVL configuration on the switch.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.

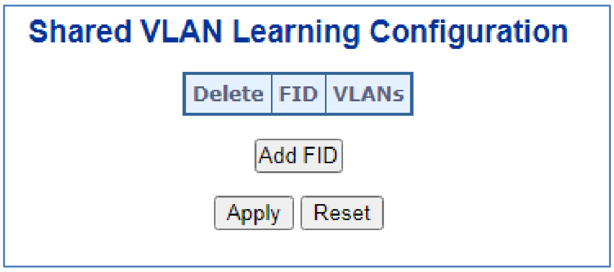
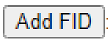


Figure 4-3-23: Shared VLAN Learning Configuration page screenshot

The page includes the following fields:

Object	Description
• **Delete**	A previously allocated FID can be deleted by the use of this button.
• **FID**	The Filter ID (FID) is the ID that VLANs get learned on in the MAC table when SVL is in effect.No two rows in the table can have the same FID and the FID must be a number between 1 and 4095.
• **VLANs**	List of VLANs mapped into FID. The syntax is as follows: Individual VLANs are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will map VLANs 1, 10, 11, 12, 13, 200, and 300: **1,10-13,200,300**. Spaces are allowed in between the delimiters. The range of valid VLANs is 1 to 4095. The same VLAN can only be a member of one FID. A message will be displayed if one VLAN is grouped into two or more FIDs. All VLANs must map to a particular FID, and by default VLAN x maps to FID x. This implies that if FID x is defined, then VLAN x is implicitly a member of FID x unless it is specified for another FID. If FID x doesn't exist, a confirmation message will be displayed, asking whether to continue adding VLAN x implicitly to FID x.

Buttons



: Add a new row to the SVL table. The FID will be pre-filled with the first unused FID.

: Click to apply changes.

: Click to undo any changes made locally and revert to previously saved values.

4.3.4 VLAN Translation

4.3.4.1 Port to Group Configuration

This page allows you to configure switch Ports to use a given VLAN Translation Mapping Group. This will enable all VLAN Translation mappings of that group (if any) on the selected switch port.

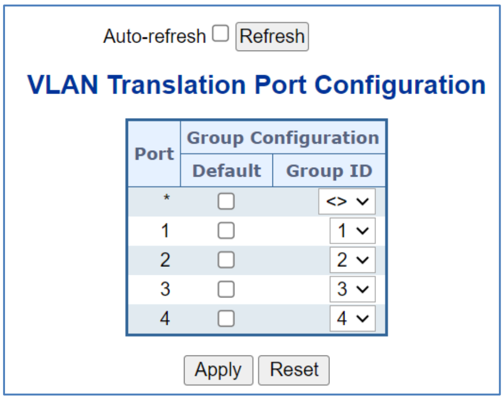


Figure 4-3-24: Shared Translation Port Configuration page screenshot

The displayed settings are:

Object	Description
• **Port**	The Port column shows the list of ports for which you can configure the VLAN Translation Mapping Group. SVL is in effect.No two rows in the table can have the same FID and the FID must be a number between 1 and 4095.
• **Default**	To set the switch port to use the default VLAN Translation Group click the checkbox and press Save.
• **Group ID**	The VLAN Translation mappings are organized into Groups, identified by the Group ID. This way a port is configured to use a number of VLAN Translation mappings easily by simply configuring it to use a given group. Then number of possible groups in a switch is equal to the number of ports present in this switch. A port can be configured to use any of the groups, but only one at any given time. Multiple ports can be configured to use the same group. A valid Group ID is an integer value from 1 to 10. Note: By default, each port is set to use the group with Group ID equal to the port number. For example, port #1 is by default set to use group with GID = 1.

Buttons

Refresh: Click to refresh the page immediately.

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.3.5 Private VLANs

4.3.5.1 Private VLAN Configuration

The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here.

Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs. The VLAN Port Status screen in Figure 4-3-25 appears.

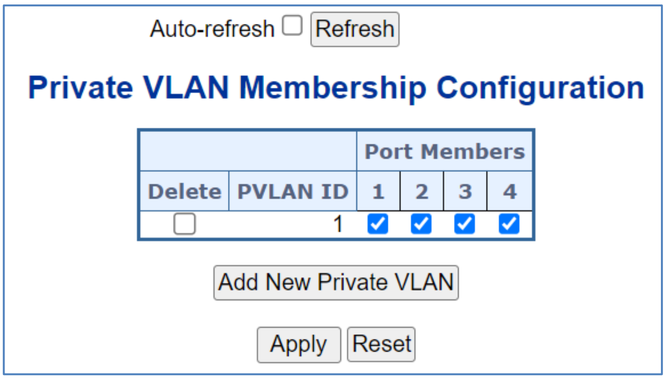


Figure 4-3-25: Private VLAN Membership Configuration page screenshot

The page includes the following fields:

Object	Description
• **Delete**	To delete a private VLAN entry, check this box. The entry will be deleted during the next save.
• **Private VLAN ID**	Indicates the ID of this particular private VLAN.
• **Port Members**	A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
• **Adding a New Private VLAN**	Click to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click "OK" to discard the incorrect entry, or click "Cancel" to return to the editing and make a correction.

	The Private VLAN is enabled when you click "Save". The button can be used to undo the addition of new Private VLANs.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Apply: Click to apply changes

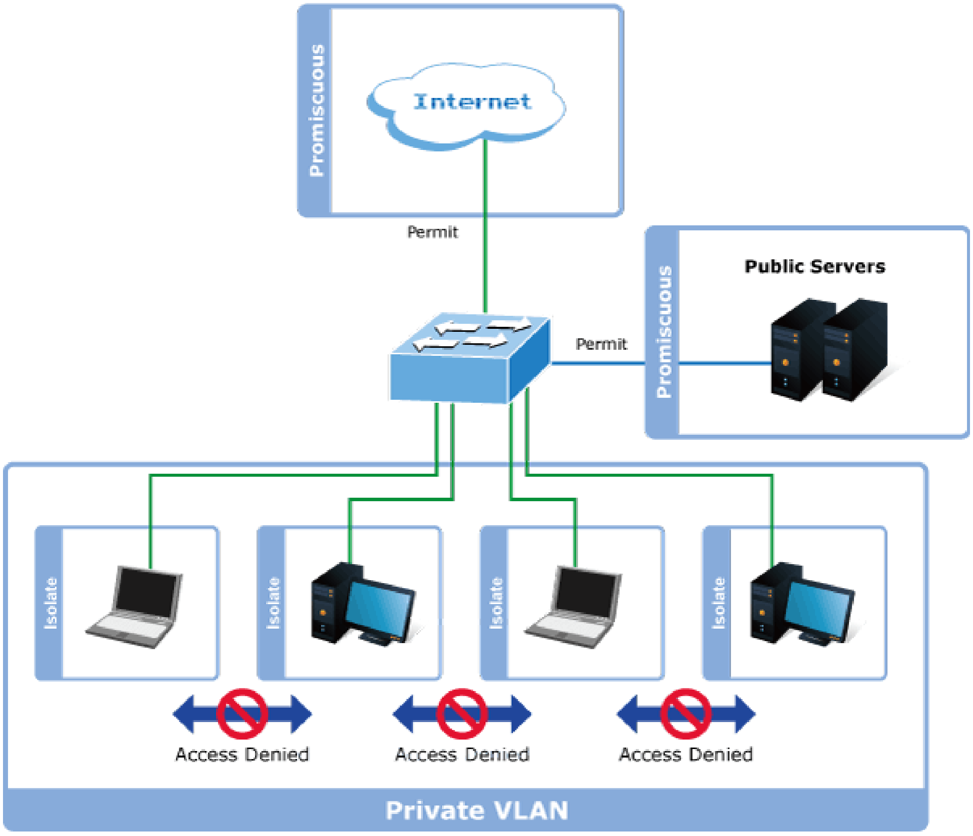
Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.5.2 Port Isolation

Overview

When a VLAN is configured to be a private VLAN, communication between ports within that VLAN can be prevented. Two application examples are provided in this section:

- Customers connected to an ISP can be members of the same VLAN, but they are not allowed to communicate with each other within that VLAN.
- Servers in a farm of web servers in a Demilitarized Zone (DMZ) are allowed to communicate with the outside world and with database servers on the inside segment, but are not allowed to communicate with each other



For private VLANs to be applied, the switch must first be configured for standard VLAN operation When this is in place, one or more of the configured VLANs can be configured as private VLANs. Ports in a private VLAN fall into one of these two groups:

■ **Promiscuous ports**

— Ports from which traffic can be forwarded to all ports in the private VLAN

— Ports which can receive traffic from all ports in the private VLAN

■ **Isolated ports**

— Ports from which traffic can only be forwarded to promiscuous ports in the private VLAN

— Ports which can receive traffic from only promiscuous ports in the private VLAN

The configuration of promiscuous and isolated ports applies to all private VLANs. When traffic comes in on a promiscuous port in a private VLAN, the VLAN mask from the VLAN table is applied. When traffic comes in on an isolated port, the private VLAN mask is applied in addition to the VLAN mask from the VLAN table. This reduces the ports to which forwarding can be done to just the promiscuous ports within the private VLAN.

This page is used for enabling or disabling port isolation on ports in a Private VLAN. A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN. The Port Isolation screen in Figure 4-3-26 appears.

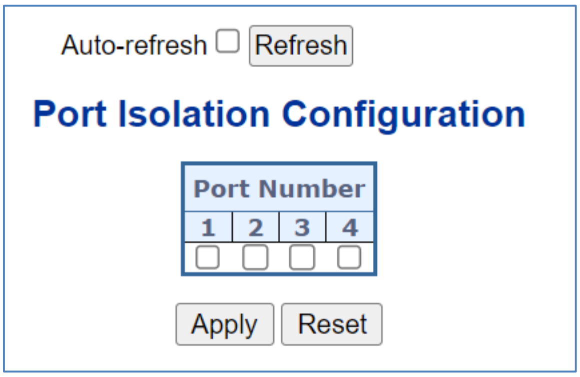


Figure 4-3-26: Port Isolation Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port Members**	A check box is provided for each port of a private VLAN. When checked, port isolation is enabled on that port. When unchecked, port isolation is disabled on that port. By default, port isolation is **disabled** on all ports.

Buttons

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4.3.6 VCL

4.3.6.1 MAC-based VLAN

The MAC-based VLAN entries can be configured here. This page allows for adding and deleting MAC-based VLAN entries and assigning the entries to different ports. This page shows only static entries. The MAC-based VLAN screen in Figure 4-3-27 appears.

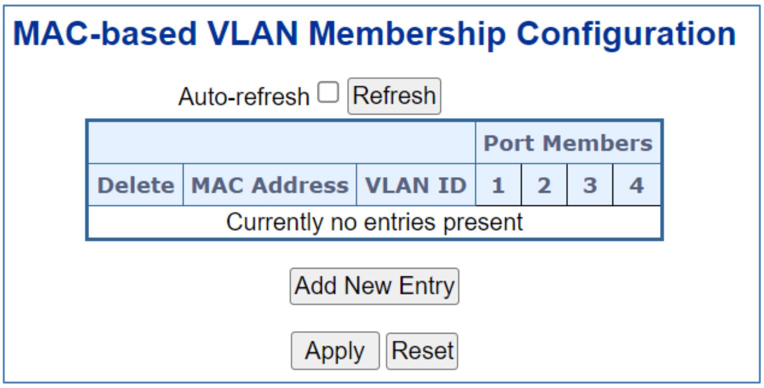


Figure 4-3-27: MAC-based VLAN Membership Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	To delete a MAC-based VLAN entry, check this box and press save.
• **MAC Address**	Indicates the MAC address.
• **VLAN ID**	Indicates the VLAN ID.
• **Port Members**	A row of check boxes for each port is displayed for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, check the box. To remove or exclude the port from the MAC-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
• **Adding a New MAC-based VLAN**	Click "Add New Entry" to add a new MAC-based VLAN entry. An empty row is added to the table, and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 through 4095. The MAC-based VLAN entry is enabled when you click on "Save". A MAC-based VLAN without any port members will be deleted when you click "Save". The "Delete" button can be used to undo the addition of new MAC-based VLANs.

Buttons

Add New Entry: Click to add a new MAC-based VLAN entry.

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

|<<: Updates the table starting from the first entry in the MAC-based VLAN Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

4.3.6.2 IP Subnet-based VLAN

The IP subnet to VLAN ID mappings can be configured here. This page allows adding, updating and deleting IP subnet to VLAN ID mapping entries and assigning them to different ports.

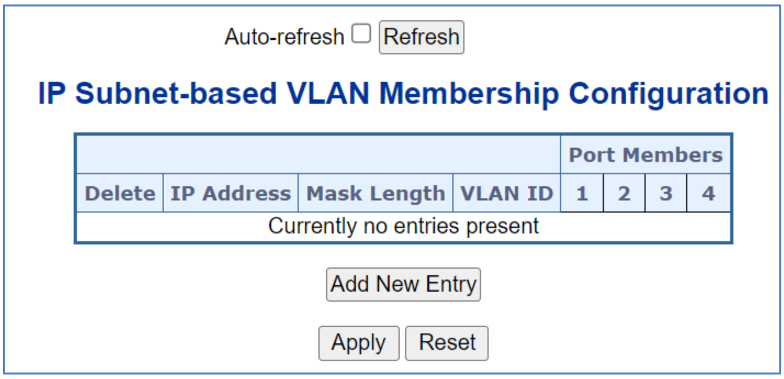


Figure 4-3-28: IP Subnet-based VLAN Membership Configuration Page Screenshot

The displayed settings are:

Object	Description
• **Delete**	To delete a mapping, check this box and press save. The entry will be deleted in the stack.
• **IP Address**	Indicates the subnet's IP address (Any of the subnet's host addresses can be also provided here, the application will convert it automatically).
• **Mask Length**	Indicates the subnet's mask length.
• **VLAN ID**	Indicates the VLAN ID the subnet will be mapped to. IP Subnet to VLAN ID is a unique matching.
• **Port Members**	A row of check boxes for each port is displayed for each IP subnet to VLAN ID mapping entry. To include a port in a mapping, simply check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members and all boxes are unchecked.
• **Adding a New IP subnet-based VLAN**	Click to add a new IP subnet to VLAN ID mapping entry. An empty row is added to the table, and the mapping can be configured as needed. Any IP address/mask can be configured for the mapping. Legal values for the VLAN ID are 1 to 4095. The IP subnet to VLAN ID mapping entry is enabled when you click on "Save". The button can be used to undo the addition of new mappings. The maximum possible IP subnet to VLAN ID mappings are limited to 128

Buttons

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4.3.6.3 Protocol-based VLAN

This page allows you to add new protocols to Group Name (unique for each Group) mapping entries as well as allow you to see and delete already mapped entries for the switch. The Protocol-based VLAN screen in Figure 4-3-29 appears.

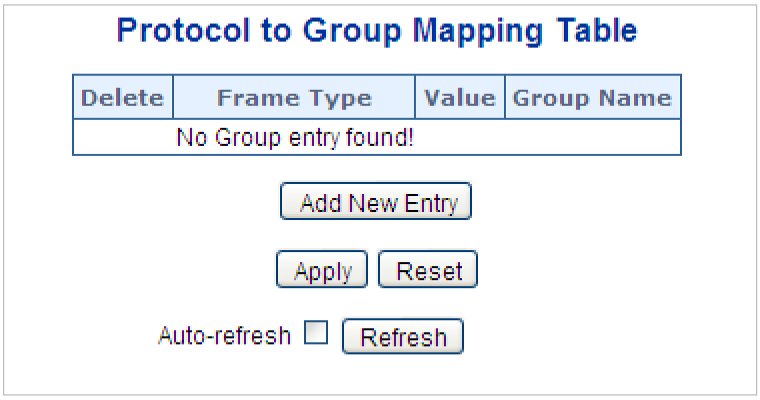


Figure 4-3-29: Protocol to Group Mapping Table Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	To delete a Protocol to Group Name map entry, check this box. The entry will be deleted on the switch during the next Save.
• **Frame Type**	Frame Type can have one of the following values: 1. **Ethernet** 2. **LLC** 3. **SNAP** Note: On changing the Frame type field, valid value of the following text field will vary depending on the new frame type you selected.
• **Value**	Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu. Below is the criteria for three different Frame Types: 1. **For Ethernet**: Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff 2. **For LLC**: Valid value in this case is comprised of two different sub-values. a. **DSAP**: 1-byte long string (0x00-0xff) b. **SSAP**: 1-byte long string (0x00-0xff) 3. **For SNAP**: Valid value in this case also is comprised of two different sub-values.

	a. **OUI**: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff. b. **PID**: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.
• **Group Name**	A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers(0-9). **Note**: special character and underscore(_) are not allowed.
• **Adding a New Group to VLAN mapping entry**	Click "Add New Entry" to add a new entry in mapping table. An empty row is added to the table; Frame Type, Value and the Group Name can be configured as needed. The "Delete" button can be used to undo the addition of new entry.

Buttons

Add New Entry: Click to add a new entry in mapping table.

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4.3.6.4 Protocol-based VLAN Membership

This page allows you to map a already configured Group Name to a VLAN for the switch. The Group Name to VLAN Mapping Table screen in Figure 4-3-30 appears.

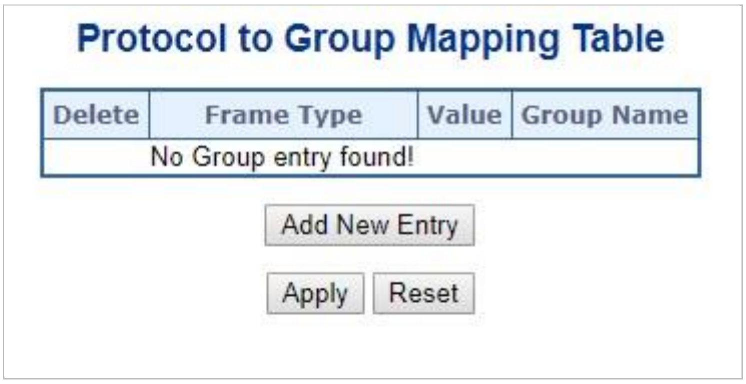


Figure 4-3-30: Group Name to VLAN Mapping Table Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	To delete a Group Name to VLAN map entry, check this box. The entry will be deleted on the switch during the next Save
• **Group Name**	A valid Group Name is a string of almost 16 characters which consists of a combination of alphabets (a-z or A-Z) and integers(0-9), no special character is allowed. Whichever Group name you try map to a VLAN must be present in Protocol to Group mapping table and must not be preused by any other existing mapping entry on this page.
• **VLAN ID**	Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4095.
• **Port Members**	A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
• **Adding a New Group to VLAN mapping entry**	Click "Add New Entry" to add a new entry in mapping table. An empty row is added to the table, the Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The "Delete" button can be used to undo the addition of new entry.

Buttons

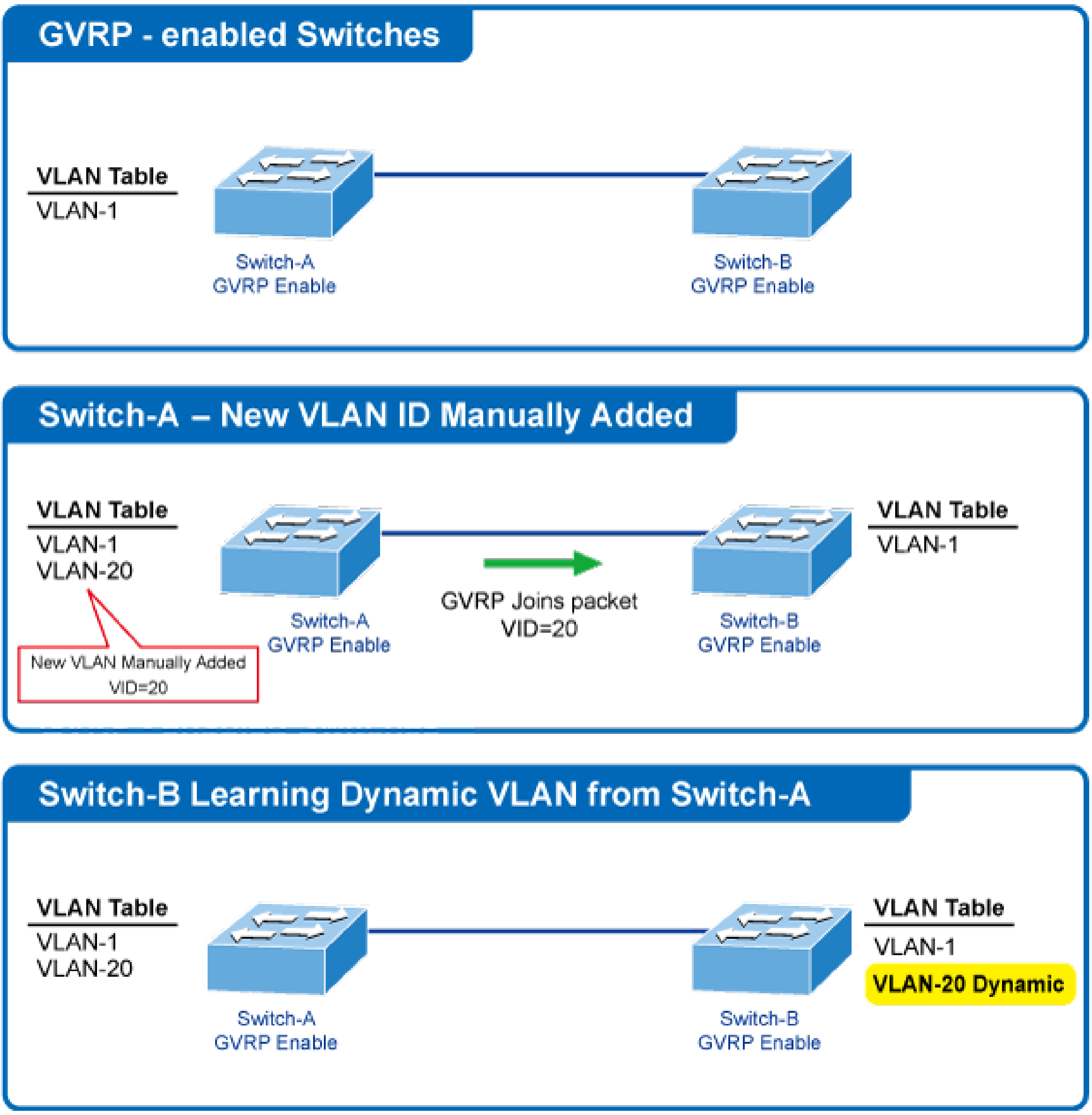
: Click to apply changes

: Click to undo any changes made locally and revert to previously saved values.

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.3.7 GVRP

GVRP (**G**ARP **V**LAN **R**egistration **P**rotocol or **G**eneric **V**LAN **R**egistration **P**rotocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network. It defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network.



VLANs are **dynamically** configured based on **join messages** issued by host devices and propagated throughout the network. GVRP must be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.

4.3.7.1 Global Configuration

This page allows you to configure the global GVRP configuration settings that are commonly applied to all GVRP enabled ports. as well. as screen in Figure 4-3-31 appears.

Figure 4-3-31: GVRP Configuration Page Screenshot

The page includes the following fields:

General Settings

Object	Description
• **Enable GVRP globally**	The GVRP feature is globally enabled by setting the check mark in the checkbox named Enable GVRP and pressing the Save button.
GVRP protocol timers	
• **Join-time**	Join-time is a value in the range of 1-20cs, i.e. in units of one hundredth of a second. The default value is 20cs.
• **Leave-time**	Leave-time is a value in the range of 60-300cs, i.e. in units of one hundredth of a second. The default is 60cs.
• **LeaveAll-time**	LeaveAll-time is a value in the range of 1000-5000cs, i.e. in units of one hundredth of a second. The default is 1000cs
• **Max number of VLANs**	When GVRP is enabled, a maximum number of VLANs supported by GVRP is specified. By default this number is 20. This number can only be changed when GVRP is turned off.

Buttons

: Click to refresh the page. Note that unsaved changes will be lost.

: Click to undo any changes made locally and revert to previously saved values.

4.3.7.2 Port Configuration

This configuration can be performed either before or after GVRP is configured globally - the protocol operation will be the same. as well. as screen in Figure 4-3-32 appears.

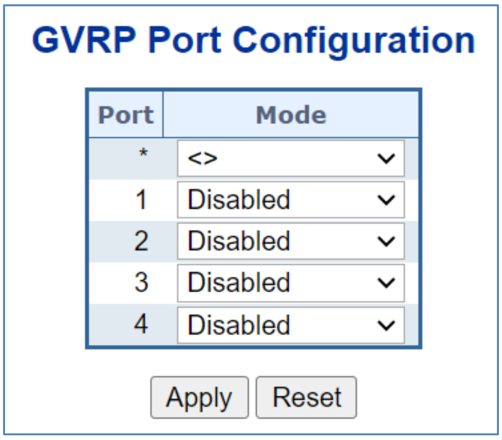


Figure 4-3-32: GVRP Port Configuration Page Screenshot

The page includes the following fields:

General Settings

Object	Description
• **Port**	The logical port that is to be configured.
• **Mode**	Mode can be either 'Disabled' or 'GVRP enabled'. These values turn the GVRP feature off or on respectively for the port in question.

Buttons

Apply : Click to refresh the page. Note that unsaved changes will be lost.

Reset : Click to undo any changes made locally and revert to previously saved values.

4.3.8 MRP

4.3.8.1 Port Configuration

This page allows you to configure the MRP generic settings for all switch ports.

The displayed settings are:

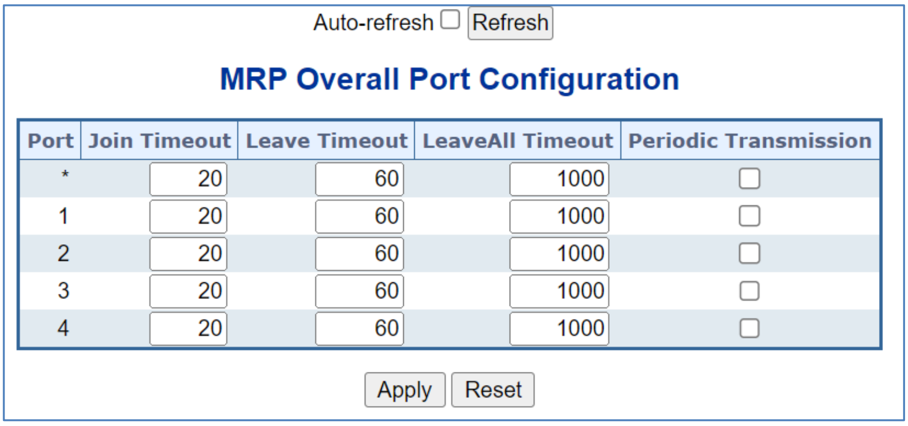


Figure 4-3-33: MRP Port Configuration Page Screenshot

The displayed settings are:

Object	Description
• **Port**	The port number for which the following configuration applies.
• **Join Timeout**	Controls the timeout of the Join Timer for all MRP Applications on this switch port. This value is restricted to 1-20 centiseconds.
• **Leave Timeout**	Controls the timeout of the Leave Timer for all MRP Applications on this switch port. This value is restricted to 60- 300 centiseconds.
• **LeaveAll Timeout**	Controls the timeout of the LeaveAll Timer for all MRP Applications on this switch port. This value is restricted to 1000- 5000 centiseconds.
• **Periodic Transmission**	Enable or disable the PeriodicTransmission feature for all MRP Applications on this switch port.

Buttons

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4.3.8.2 MVRP Global Configuration

This page allows you to configure the MVRP global and per port settings altogether. The page is divided into a global section and a per-port configuration section.

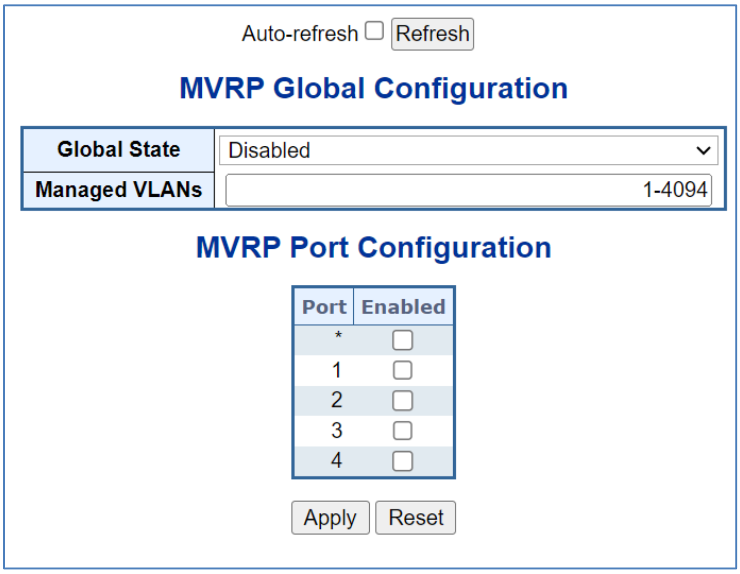


Figure 4-3-34: MVRP Global Configuration Page Screenshot

The displayed settings are:

Object	Description
• **Global State**	Enable or disable the MVRP protocol globally. This will enable or disable the protocol globally and at the same time on the switch ports that are MVRP enabled.
• **Managed VLANs**	This field shows the managed VLANs, i.e. the VLANs that MVRP will operate upon. By default, only VLANs 1- 4094 are managed, i.e. the entire range as defined in IEEE802.1Q-2014 for MVRP. However this range can be limited by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters.
MVRP Port Configuration	
• **Port**	The port number for which the following configuration applies.
• **Enabled**	Enable or disable the MVRP protocol on this switch port. This will enable or disable the protocol on the switch port given that MVRP is also globally enabled.
• **Default**	To set the switch port to use the default VL

Buttons

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4.3.9 Spanning Tree

4.3.9.1 Theory

The Spanning Tree protocol can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down. The spanning tree algorithms supported by this switch include these versions:

- **STP – Spanning Tree Protocol (IEEE 802.1D)**
- **RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)**
- **MSTP – Multiple Spanning Tree Protocol (IEEE 802.1s)**

The **IEEE 802.1D Spanning Tree** Protocol and **IEEE 802.1w Rapid Spanning Tree** Protocol allow for the blocking of links between switches that form loops within the network. When multiple links between switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. The protocol allows for the duplicate links to be used in the event of a failure of the primary link. Once the Spanning Tree Protocol is configured and enabled, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links (at the time of a primary link failure) is also accomplished automatically without operator intervention.

This automatic network reconfiguration provides maximum uptime to network users. However, the concepts of the Spanning Tree Algorithm and protocol are a complicated and complex subject and must be fully researched and understood. It is possible to cause serious degradation of the performance of the network if the Spanning Tree is incorrectly configured. Please read the following before making any changes from the default values.

The Switch STP performs the following functions:

- Creates a single spanning tree from any combination of switching or bridging elements.
- Creates multiple spanning trees – from any combination of ports contained within a single switch, in user specified groups.
- Automatically reconfigures the spanning tree to compensate for the failure, addition, or removal of any element in the tree.
- Reconfigures the spanning tree without operator intervention.

Bridge Protocol Data Units

For STP to arrive at a stable network topology, the following information is used:

- The unique switch identifier
- The path cost to the root associated with each switch port
- The port identifier

STP communicates between switches on the network using Bridge Protocol Data Units (BPDUs). Each BPDU contains the following information:

- The unique identifier of the switch that the transmitting switch currently believes is the root switch
- The path cost to the root from the transmitting port
- The port identifier of the transmitting port

The switch sends BPDUs to communicate and construct the spanning-tree topology. All switches connected to the LAN on which the packet is transmitted will receive the BPDU. BPDUs are not directly forwarded by the switch, but the receiving switch uses the information in the frame to calculate a BPDU, and, if the topology changes, initiates a BPDU transmission.

The communication between switches via BPDUs results in the following:

- One switch is elected as the root switch
- The shortest distance to the root switch is calculated for each switch
- A designated switch is selected. This is the switch closest to the root switch through which packets will be forwarded to the root.
- A port for each switch is selected. This is the port providing the best path from the switch to the root switch.
- Ports included in the STP are selected.

Creating a Stable STP Topology

It is to make the root port a fastest link. If all switches have STP enabled with default settings, the switch with the lowest MAC address in the network will become the root switch. By increasing the priority (lowering the priority number) of the best switch, STP can be forced to select the best switch as the root switch.

When STP is enabled using the default parameters, the path between source and destination stations in a switched network might not be ideal. For instance, connecting higher-speed links to a port that has a higher number than the current root port can cause a root-port change.

STP Port States

The BPDUs take some time to pass through a network. This propagation delay can result in topology changes where a port that transitioned directly from a Blocking state to a Forwarding state could create temporary data loops. Ports must wait for new network topology information to propagate throughout the network before starting to forward packets. They must also wait for the packet lifetime to expire for BPDU packets that were forwarded based on the old topology. The forward delay timer is used to allow the network topology to stabilize after a topology change. In addition, STP specifies a series of states a port must transition through to further ensure that a stable network topology is created after a topology change.

Each port on a switch using STP exists is in one of the following five states:

- **Blocking** – the port is blocked from forwarding or receiving packets
- **Listening** – the port is waiting to receive BPDU packets that may tell the port to go back to the blocking state
- **Learning** – the port is adding addresses to its forwarding database, but not yet forwarding packets
- **Forwarding** – the port is forwarding packets
- **Disabled** – the port only responds to network management messages and must return to the blocking state first

A port transitions from one state to another as follows:

- From initialization (switch boot) to blocking
- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled
- From disabled to blocking

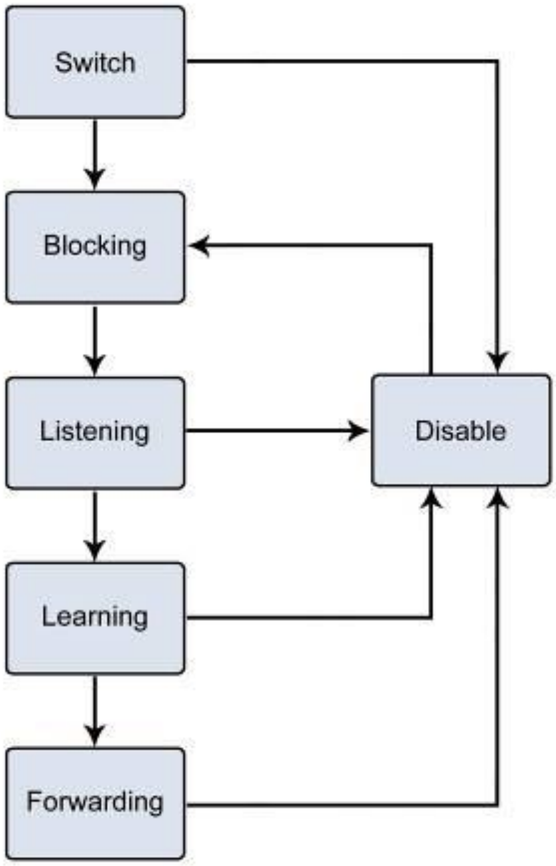


Figure 4-3-35: STP Port State Transitions

You can modify each port state by using management software. When you enable STP, every port on every switch in the network goes through the blocking state and then transitions through the states of listening and learning at power up. If properly configured, each port stabilizes to the forwarding or blocking state. No packets (except BPDUs) are forwarded from, or received by, STP enabled ports until the forwarding state is enabled for that port.

2. STP Parameters

STP Operation Levels

The Switch allows for two levels of operation: the switch level and the port level. The switch level forms a spanning tree consisting of links between one or more switches. The port level constructs a spanning tree consisting of groups of one or more ports. The STP operates in much the same way for both levels.

Note	On the switch level, STP calculates the Bridge Identifier for each switch and then sets the Root Bridge and the Designated Bridges. On the port level, STP sets the Root Port and the Designated Ports.

The following are the user-configurable STP parameters for the switch level:

Parameter	Description	Default Value
Bridge Identifier(Not user configurable except by setting priority below)	A combination of the User-set priority and the switch's MAC address. The Bridge Identifier consists of two parts: a 16-bit priority and a 48-bit Ethernet MAC address 32768 + MAC	32768 + MAC
Priority	A relative priority for each switch – lower numbers give a higher priority and a greater chance of a given switch being elected as the root bridge	32768
Hello Time	The length of time between broadcasts of the hello message by the switch	2 seconds
Maximum Age Timer	Measures the age of a received BPDU for a port and ensures that the BPDU is discarded when its age exceeds the value of the maximum age timer.	20 seconds
Forward Delay Timer	The amount time spent by a port in the learning and listening states waiting for a BPDU that may return the port to the blocking state.	15 seconds

The following are the user-configurable STP parameters for the port or port group level:

Variable	Description	Default Value
Port Priority	A relative priority for each port –lower numbers give a higher priority and a greater chance of a given port being elected as the root port	128
Port Cost	A value used by STP to evaluate paths – STP calculates path costs and selects the path with the minimum cost as the active path	200,000-100Mbps Fast Ethernet ports 20,000-1000Mbps Gigabit Ethernet ports 0 - Auto

Default Spanning-Tree Configuration

Feature	Default Value
Enable state	STP disabled for all ports
Port priority	128
Port cost	0
Bridge Priority	32,768

User-Changeable STA Parameters

The Switch's factory default setting should cover the majority of installations. However, it is advisable to keep the default settings as set at the factory; unless, it is absolutely necessary. The user changeable parameters in the Switch are as follows:

Priority – A Priority for the switch can be set from 0 to 65535. 0 is equal to the highest Priority.

Hello Time – The Hello Time can be from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other Switches that it is indeed the Root Bridge. If you set a Hello Time for your Switch, and it is not the Root Bridge, the set Hello Time will be used if and when your Switch becomes the Root Bridge.

Note

The Hello Time cannot be longer than the Max. Age; otherwise, a configuration error will occur.

Max. Age – The Max Age can be from 6 to 40 seconds. At the end of the Max Age, if a BPDU has still not been received from the Root Bridge, your Switch will start sending its own BPDU to all other Switches for permission to become the Root Bridge. If it turns out that your Switch has the lowest Bridge Identifier, it will become the Root Bridge.

Forward Delay Timer – The Forward Delay can be from 4 to 30 seconds. This is the time any port on the

Switch spends in the listening state while moving from the blocking state to the forwarding state.

Note

Observe the following formulas when setting the above parameters:

Max. Age _ 2 x (Forward Delay - 1 second)

Max. Age _ 2 x (Hello Time + 1 second)

Port Priority – A Port Priority can be from 0 to 240. The lower the number, the greater the probability the port will be chosen as the Root Port.

Port Cost – A Port Cost can be set from 0 to 200000000. The lower the number, the greater the probability the port will be chosen to forward packets.

3. Illustration of STP

A simple illustration of three switches connected in a loop is depicted in the below diagram. In this example, you can anticipate some major network problems if the STP assistance is not applied.

If switch A broadcasts a packet to switch B, switch B will broadcast it to switch C, and switch C will broadcast it to back to switch A and so on. The broadcast packet will be passed indefinitely in a loop, potentially causing a network failure. In this example, STP breaks the loop by blocking the connection between switch B and C. The decision to block a particular connection is based on the STP calculation of the most current Bridge and Port settings.

Now, if switch A broadcasts a packet to switch C, then switch C will drop the packet at port 2 and the broadcast will end there.

Setting-up STP using values other than the defaults, can be complex. Therefore, you are advised to keep the default factory settings and STP will automatically assign root bridges/ports and block loop connections. Influencing STP to choose a particular switch as the root bridge using the Priority setting, or influencing STP to choose a particular port to block using the Port Priority and Port Cost settings is, however, relatively straight forward.

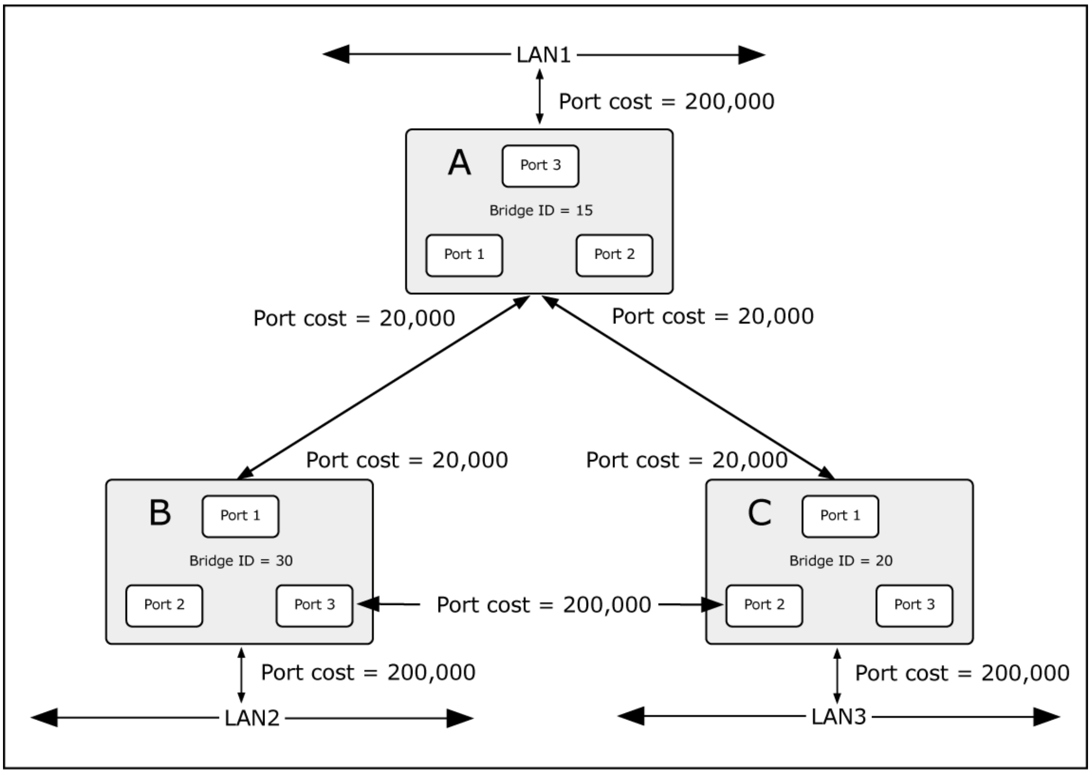


Figure 4-3-36: Before Applying the STA Rules

In this example, only the default STP values are used.

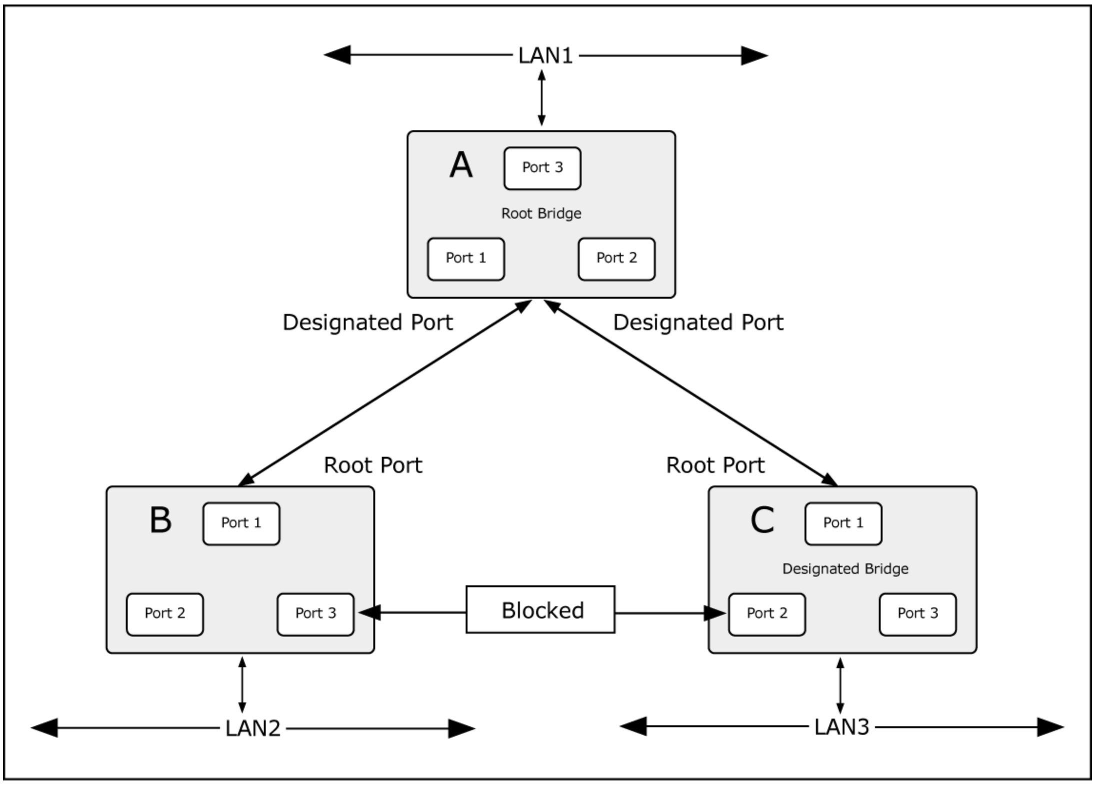


Figure 4-3-37: After Applying the STA Rules

The switch with the lowest Bridge ID (switch C) was elected the root bridge, and the ports were selected to give a high port cost between switches B and C. The two (optional) Gigabit ports (default port cost = 20,000) on switch A are connected to one (optional) Gigabit port on both switch B and C. The redundant link between switch B and C is deliberately chosen as a 100 Mbps Fast Ethernet link (default port cost = 200,000). Gigabit ports could be used, but the port cost should be increased from the default to ensure that the link between switch B and switch C is the blocked link.

4.3.9.2 STP System Configuration

This page allows you to configure STP system settings. The settings are used by all STP Bridge instances in the Switch. The **Industrial Managed TSN Device** support the following Spanning Tree protocols:

- **Compatiable -- Spanning Tree Protocol (STP):**Provides a single path between end stations, avoiding and eliminating loops.
- **Normal -- Rapid Spanning Tree Protocol (RSTP) :** Detects and uses of network topologies that provide faster spanning tree convergence, without creating forwarding loops.
- **Extension – Multiple Spanning Tree Protocol (MSTP) :** Defines an extension to RSTP to further develop the usefulness of virtual LANs (VLANs). This "Per-VLAN" Multiple Spanning Tree Protocol configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each Spanning Tree.

The STP System Configuration screen in Figure 4-3-38 appears.

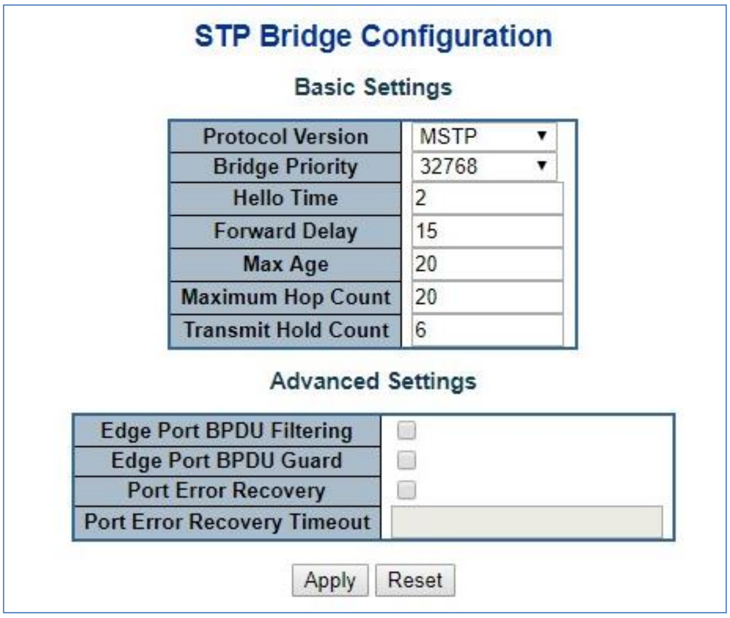


Figure 4-3-38: STP Bridge Configuration Page Screenshot

The page includes the following fields:

Basic Settings

Object	Description
• **Protocol Version**	The STP protocol version setting. Valid values are: ■ **STP** (IEEE 802.1D Spanning Tree Protocol) ■ **RSTP** (IEEE 802.2w Rapid Spanning Tree Protocol) ■ **MSTP** (IEEE 802.1s Multiple Spanning Tree Protocol)
• **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
• **Forward Delay**	The delay used by STP Bridges to transition Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds -Default: 15 -Minimum: The higher of 4 or [(Max. Message Age / 2) + 1] -Maximum: 30
• **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. -Default: 20 -Minimum: The higher of 6 or [2 x (Hello Time + 1)]. -Maximum: The lower of 40 or [2 x (Forward Delay -1)]
• **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. 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.

Advanced Settings

Object	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 that has to pass before a port in the *error-disabled* state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

Note

The **Industrial Managed TSN Device** implements the Rapid Spanning Protocol as the default spanning tree protocol. When selecting **"Compatibles"** mode, the system uses the RSTP (802.1w) to be compatible and to co-work with another STP (802.1D)'s BPDU control packet.

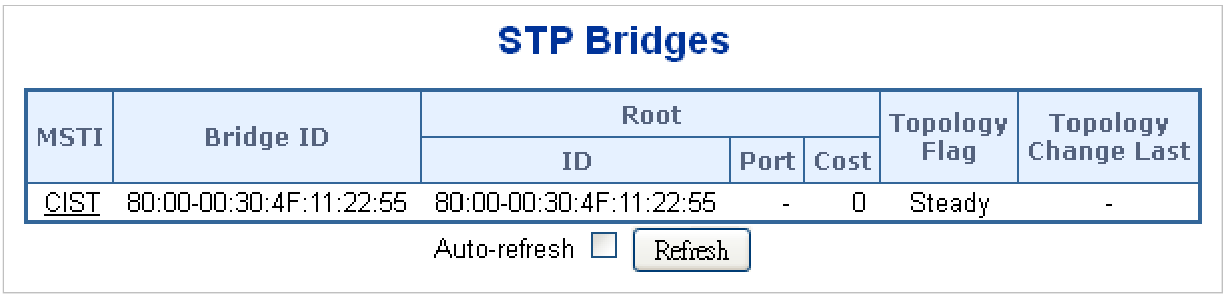
Buttons

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.9.3 Bridge Status

This page provides a status overview for all STP bridge instances. The displayed table contains a row for each STP bridge instance, where the column displays the following information: The Bridge Status screen in Figure 4-3-39 appears.


STP Bridges

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	80:00-00:30:4F:11:22:55	80:00-00:30:4F:11:22:55	-	0	Steady	-

Figure 4-3-39: STP Bridge Status Page Screenshot

The page includes the following fields:

Object	Description
• **MSTI**	The Bridge Instance. This is also a link to the STP Detailed Bridge Status.
• **Bridge ID**	The Bridge ID of this Bridge instance.
• **Root ID**	The Bridge ID of the currently elected root bridge.
• **Root Port**	The switch port currently assigned the *root* port role.
• **Root Cost**	Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
• **Topology Flag**	The current state of the Topology Change Flag for this Bridge instance.
• **Topology Change Last**	The time since last Topology Change occurred.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately.

4.3.9.4 CIST Port Configuration

This page allows the user to inspect the current STP CIST port configurations, and possibly change them as well. The CIST Port Configuration screen in Figure 4-3-40 appears.

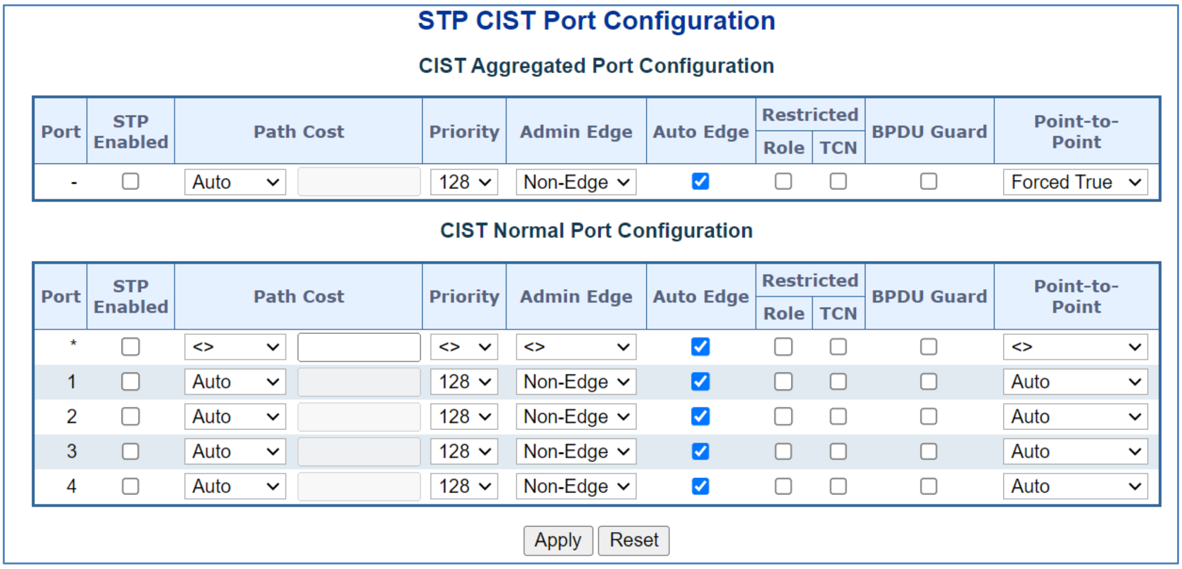


Figure 4-3-40: STP CIST Port Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical STP port.
• **STP Enabled**	Controls whether RSTP 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 favor 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). Default: **128** Range: 0-240, in steps of 16
• **AdminEdge**	Controls whether the operEdge flag should start as being 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. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as **Root Guard**.
• **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. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.
• **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 a shared medium. This can be automatically determined, or forced either true or false. Transitions to the forwarding state is faster for point-to-point LANs than for shared media.

Buttons

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

Table 4-3-2: Recommended STP Path Cost Range

Port Type	Link Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	Half Duplex Full Duplex Trunk	100 95 90	2,000,000 1,999,999 1,000,000
Fast Ethernet	Half Duplex Full Duplex Trunk	19 18 15	200,000 100,000 50,000
Gigabit Ethernet	Full Duplex Trunk	4 3	10,000 5,000

Table 4-3-3: Recommended STP Path Costs

Port Type	Link Type	IEEE 802.1w-2001
Ethernet	Half Duplex Full Duplex Trunk	2,000,000 1,000,000 500,000
Fast Ethernet	Half Duplex Full Duplex Trunk	200,000 100,000 50,000
Gigabit Ethernet	Full Duplex Trunk	10,000 5,000

Table 4-3-4: Default STP Path Costs

4.3.9.5 MSTI Priorities

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well. The MSTI Priority screen in Figure 4-3-41 appears.

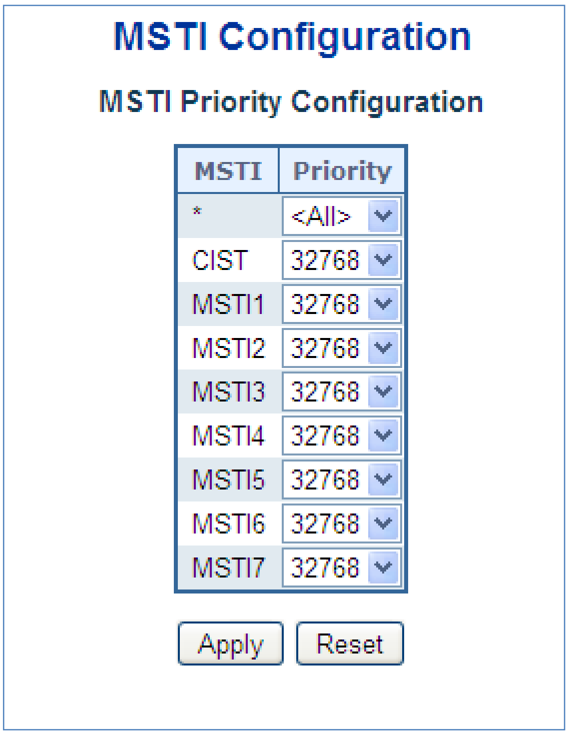


Figure 4-3-41: MSTI Priority Page Screenshot

The page includes the following fields:

Object	Description
• **MSTI**	The bridge instance. The CIST is the default instance, which is always active.
• **Priority**	Controls the bridge priority. Lower numerical 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.

Buttons

: Click to apply changes

: Click to undo any changes made locally and revert to previously saved values.

4.3.9.6 MSTI Configuration

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well. The MSTI Configuration screen in Figure 4-3-42 appears.

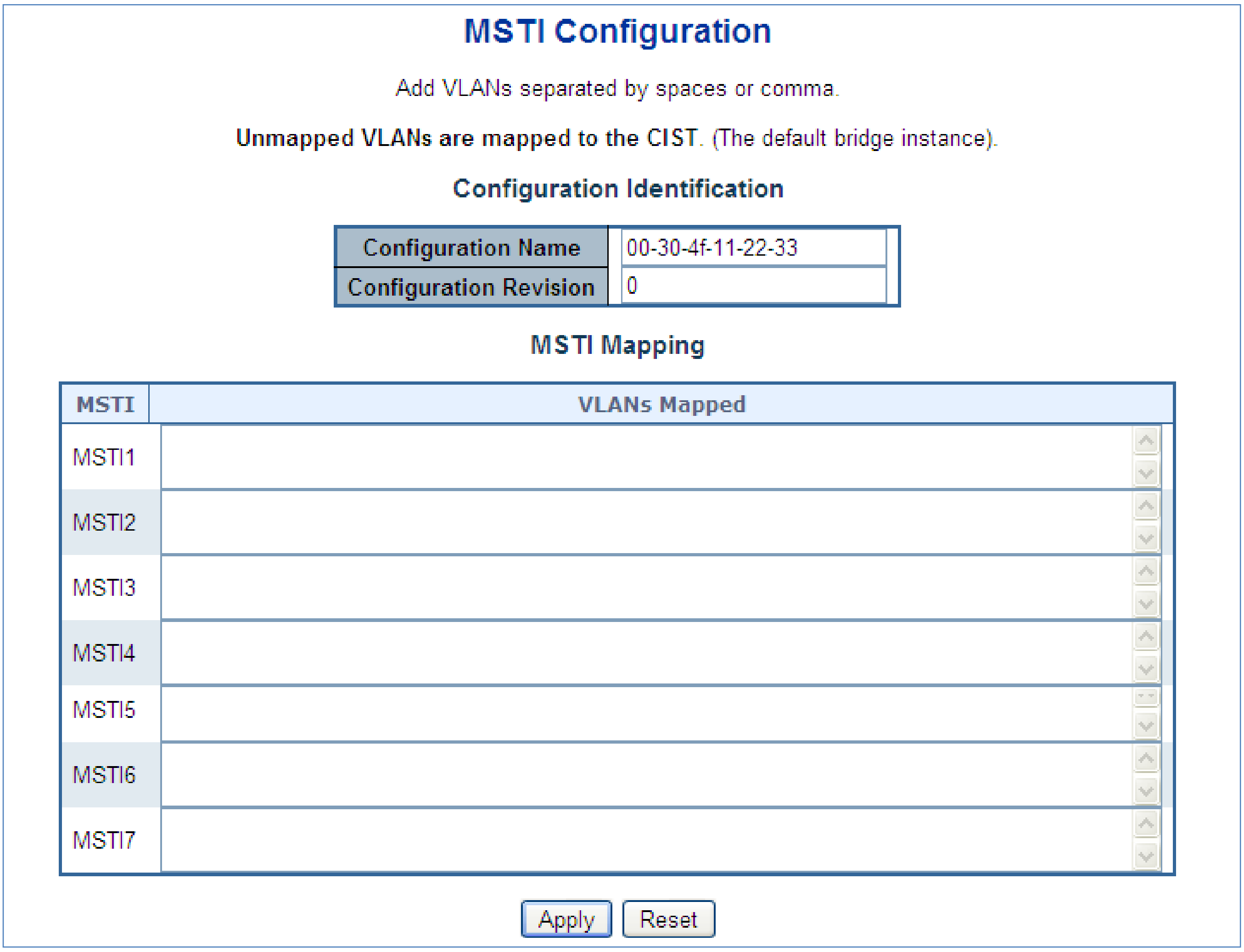


Figure 4-3-42: MSTI Configuration Page Screenshot

The page includes the following fields:

Configuration Identification

Object	Description
• **Configuration Name**	The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's. (Intra-region). The name is at most 32 characters.
• **Configuration Revision**	The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI Mapping

Object	Description
• **MSTI**	The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.
• **VLANs Mapped**	The list of VLAN's mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to *one* MSTI. A unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.)

Buttons

: Click to apply changes

: Click to undo any changes made locally and revert to previously saved values.

4.3.9.7 MSTI Ports Configuration

This page allows the user to inspect the current STP MSTI port configurations, and possibly change them as well. A MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured and applicable for the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.

This page contains MSTI port settings for physical and aggregated ports. The aggregation settings are global. The MSTI Port Configuration screen in Figure 4-3-43 & Figure 4-3-44 appears.

Figure 4-3-43: MSTI Port Configuration Page Screenshot

The page includes the following fields:

MSTI Port Configuration

Object	Description
• **Select MSTI**	Select the bridge instance and set more detail configuration.

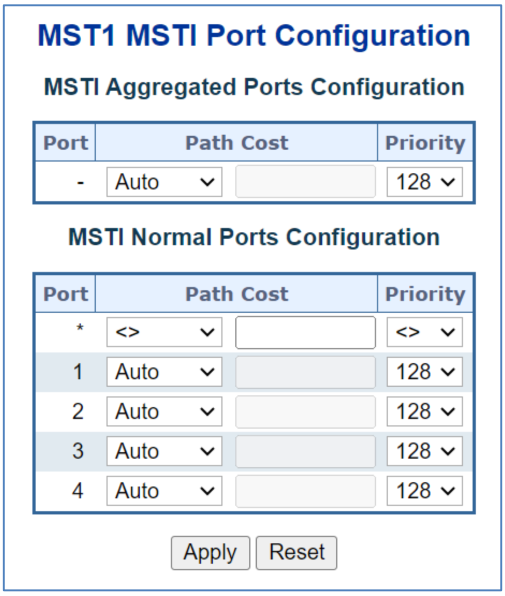


Figure 4-3-44: MST1 MSTI Port Configuration Page Screenshot

The page includes the following fields:

MSTx MSTI Port Configuration

Object	Description
• **Port**	The switch port number of the corresponding STP CIST (and MSTI) 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 favor 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.

Buttons

: Click to set MSTx configuration

: Click to apply changes

: Click to undo any changes made locally and revert to previously saved values.

4.3.9.8 Port Status

This page displays the STP CIST port status for port physical ports in the currently selected switch.

The STP Port Status screen in Figure 4-3-45 appears.

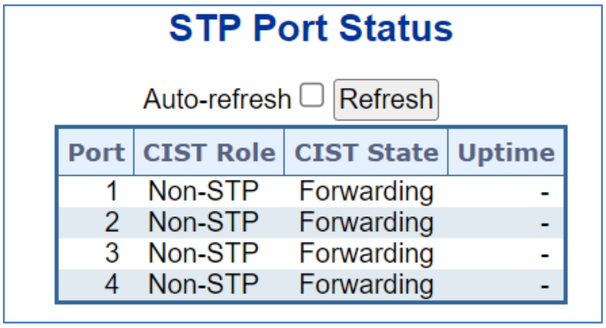


Figure 4-3-45: STP Port Status Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical STP port.
• **CIST Role**	The current STP port role of the ICST port. The port role can be one of the following values: ■ AlternatePort ■ BackupPort ■ RootPort ■ DesignatedPort ■ Disable
• **CIST State**	The current STP port state of the CIST port . The port state can be one of the following values: ■ Disabled ■ Learning ■ Forwarding
• **Uptime**	The time since the bridge port was last initialized.

Buttons

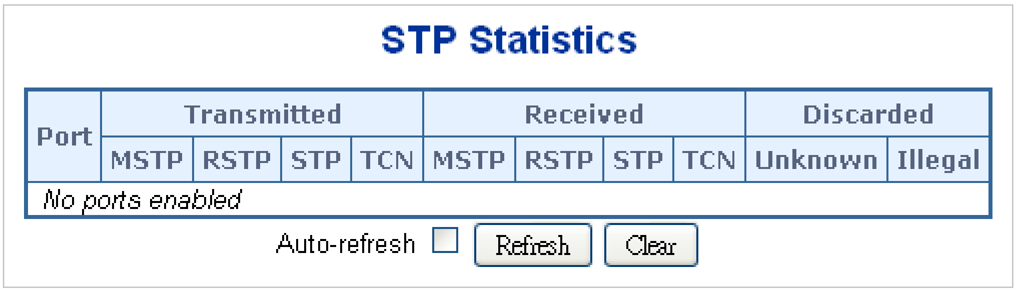
Refresh: Click to refresh the page immediately.

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds

4.3.9.9 Port Statistics

This page displays the STP port statistics counters for port physical ports in the currently selected switch.

The STP Port Statistics screen in Figure 4-3-46 appears.


STP Statistics

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
No ports enabled										

Figure 4-3-46: STP Statistics Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical RSTP port.
• **MSTP**	The number of MSTP Configuration BPDU's received/transmitted on the port.
• **RSTP**	The number of RSTP Configuration BPDU's received/transmitted on the port.
• **STP**	The number of legacy STP Configuration BPDU's received/transmitted on the port.
• **TCN**	The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.
• **Discarded Unknown**	The number of unknown Spanning Tree BPDU's received (and discarded) on the port.
• **Discarded Illegal**	The number of illegal Spanning Tree BPDU's received (and discarded) on the port.

Buttons

Auto-refresh ☐: Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

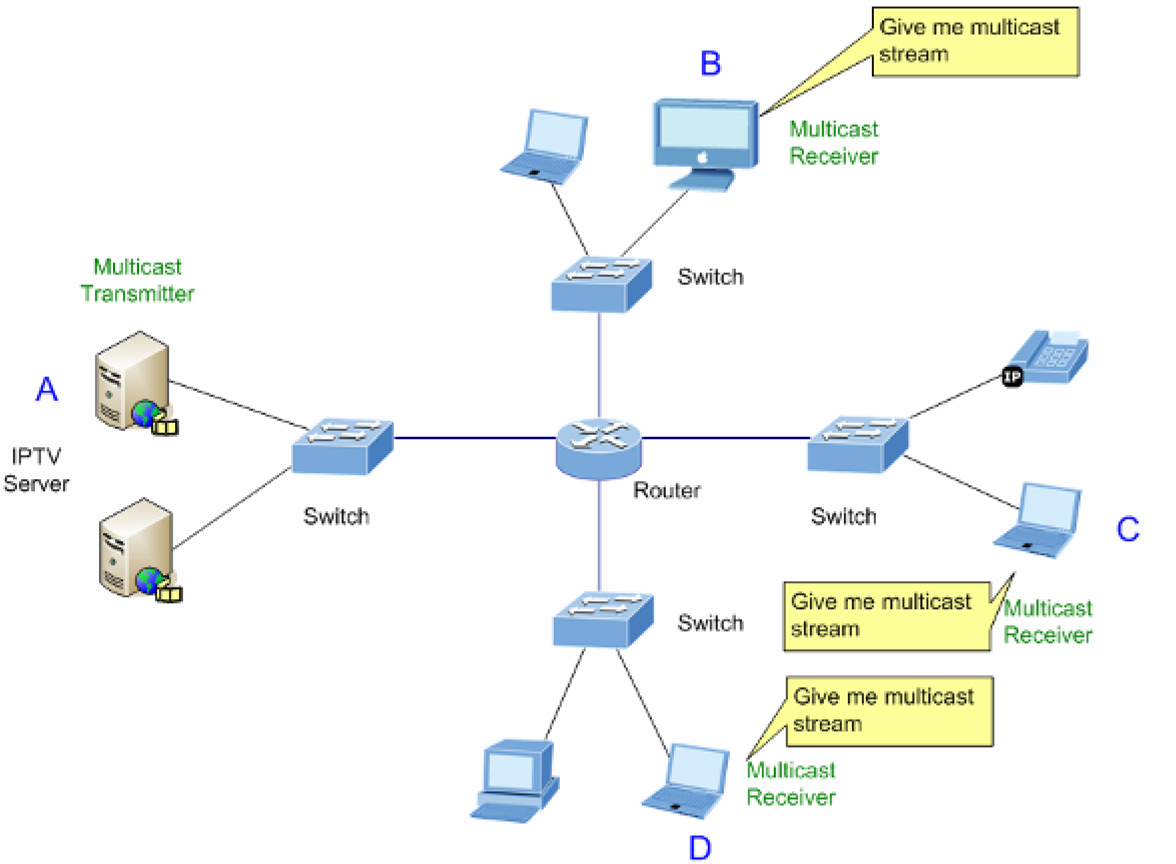
Clear: Clears the counters for all ports.

4.3.10 IGMP Snooping

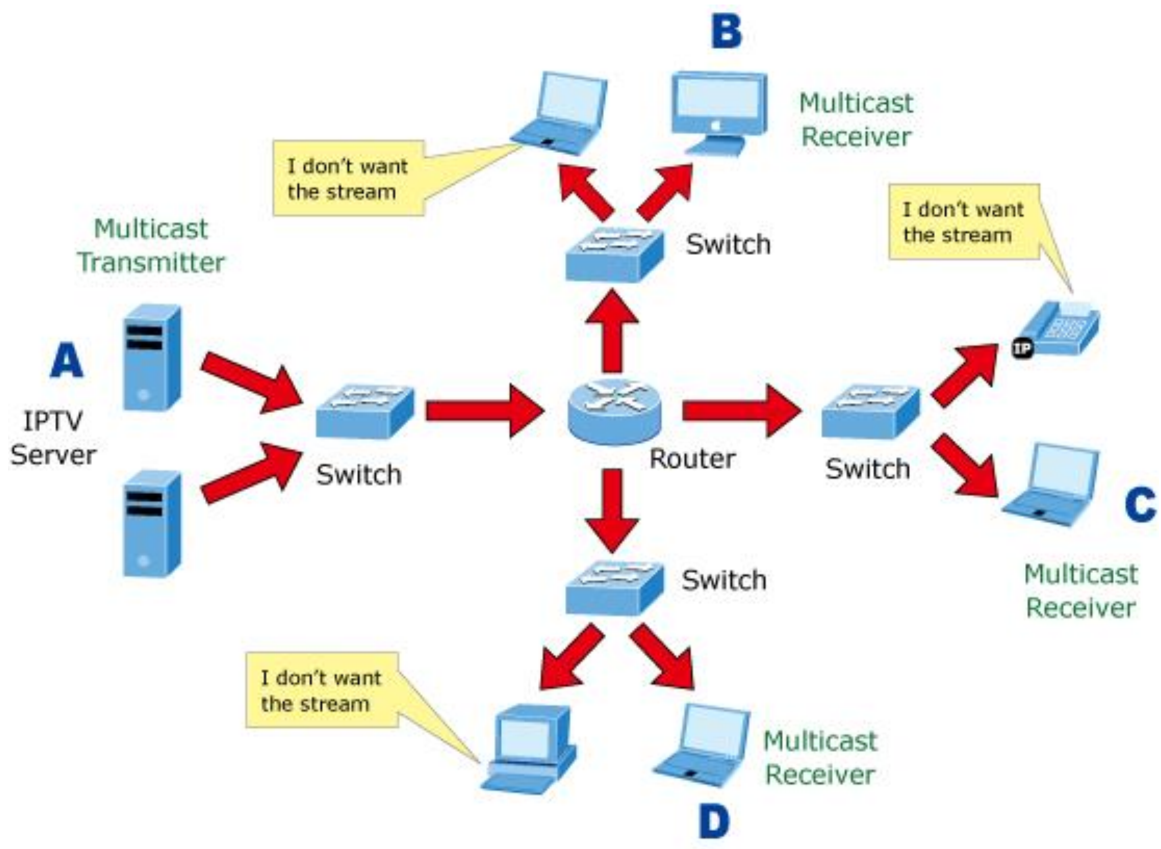
The **Internet Group Management Protocol (IGMP)** lets host and routers share information about multicast groups memberships. IGMP snooping is a switch feature that monitors the exchange of IGMP messages and copies them to the CPU for feature processing. The overall purpose of IGMP Snooping is to limit the forwarding of multicast frames to only ports that are a member of the multicast group.

About the Internet Group Management Protocol (IGMP) Snooping

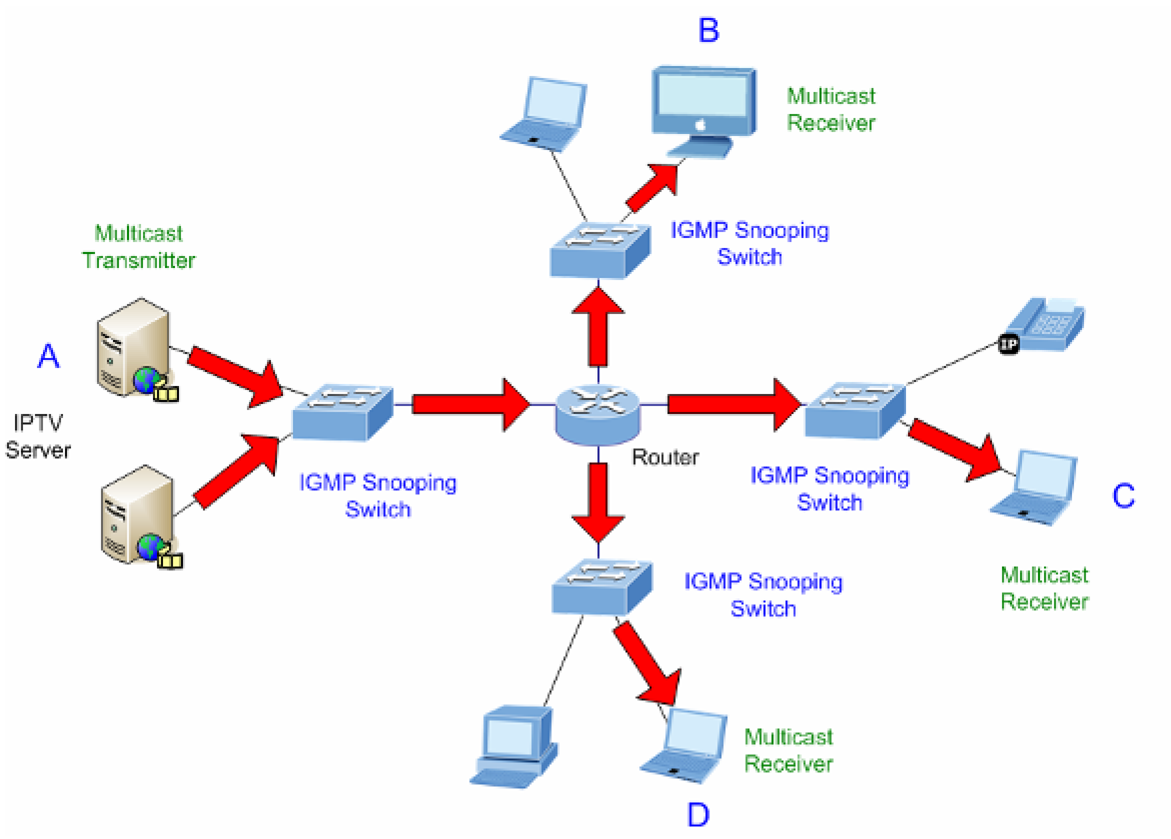
Computers and network devices that want to receive multicast transmissions need to inform nearby routers that they will become members of a multicast group. The **Internet Group Management Protocol (IGMP)** is used to communicate this information. IGMP is also used to periodically check the multicast group for members that are no longer active. In the case where there is more than one multicast router on a sub network, one router is elected as the 'queried'. This router then keeps track of the membership of the multicast groups that have active members. The information received from IGMP is then used to determine if multicast packets should be forwarded to a given sub network or not. The router can check, using IGMP, to see if there is at least one member of a multicast group on a given subnet work. If there are no members on a sub network, packets will not be forwarded to that sub network.



Multicast Service



Multicast Flooding



IGMP Snooping Multicast Stream Control

IGMP Versions 1 and 2

Multicast groups allow members to join or leave at any time. IGMP provides the method for members and multicast routers to communicate when joining or leaving a multicast group. IGMP version 1 is defined in RFC 1112. It has a fixed packet size and no optional data. The format of an IGMP packet is shown below:

IGMP Message Format

Octets

0	8	16	31
Type	Response Time	Checksum	
Group Address (all zeros if this is a query)			

The IGMP Type codes are shown below:

Type	Meaning
0x11	Membership Query (if Group Address is 0.0.0.0)
0x11	Specific Group Membership Query (if Group Address is Present)
0x16	**Membership Report (version 2)**
0x17	**Leave a Group (version 2)**
0x12	**Membership Report (version 1)**

IGMP packets enable multicast routers to keep track of the membership of multicast groups, on their respective sub networks. The following outlines what is communicated between a multicast router and a multicast group member using IGMP.

A host sends an IGMP **"report"** to join a group

A host will never send a report when it wants to leave a group (for version 1).

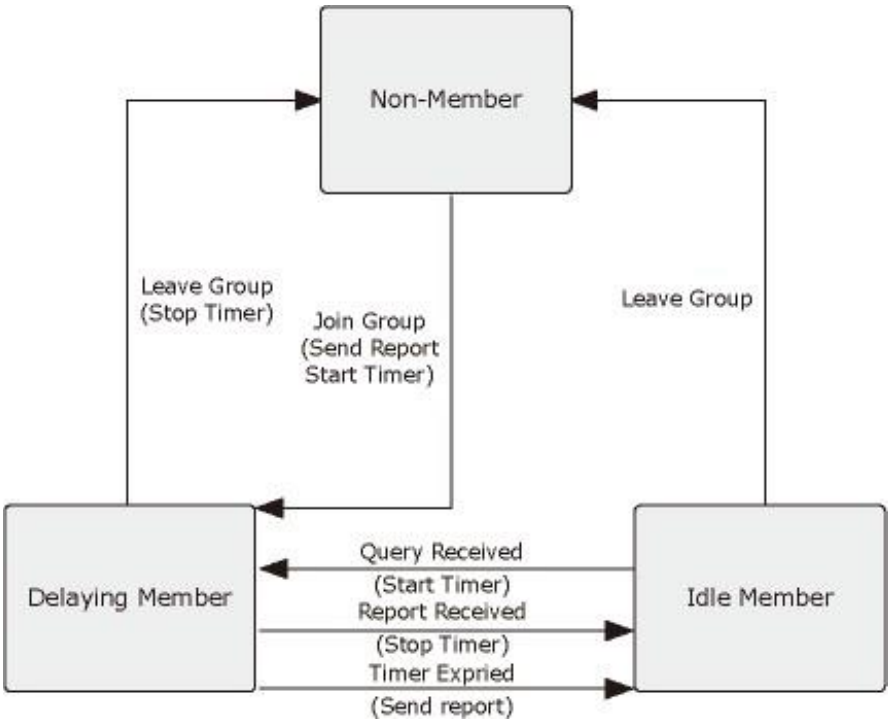
A host will send a **"leave"** report when it wants to leave a group (for version 2).

Multicast routers send IGMP queries (to the all-hosts group address: 224.0.0.1) periodically to see whether any group members exist on their sub networks. If there is no response from a particular group, the router assumes that there are no group members on the network.

The Time-to-Live (TTL) field of query messages is set to 1 so that the queries will not be forwarded to other sub networks.

IGMP version 2 introduces some enhancements such as a method to elect a multicast queried for each LAN, an explicit leave message, and query messages that are specific to a given group.

The states a computer will go through to join or to leave a multicast group are shown below:



IGMP State Transitions

- **IGMP Querier**

  A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected "**querier**" and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.

Note

Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

4.3.10.1 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. The Profile Table screen in Figure 4-3-47 appears.

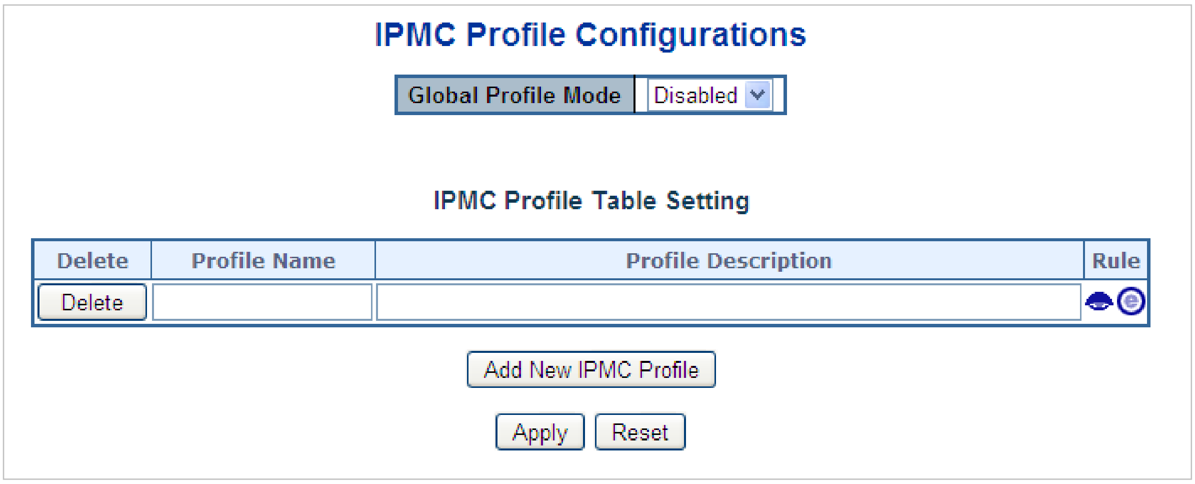


Figure 4-3-47: IPMC Profile Configuration Page

The page includes the following fields:

Object	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.

Buttons

Add New IPMC Profile: Click to add new IPMC profile. Specify the name and configure the new entry. Click "Save".

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.10.2 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. The Profile Table screen in Figure 4-3-48 appears.

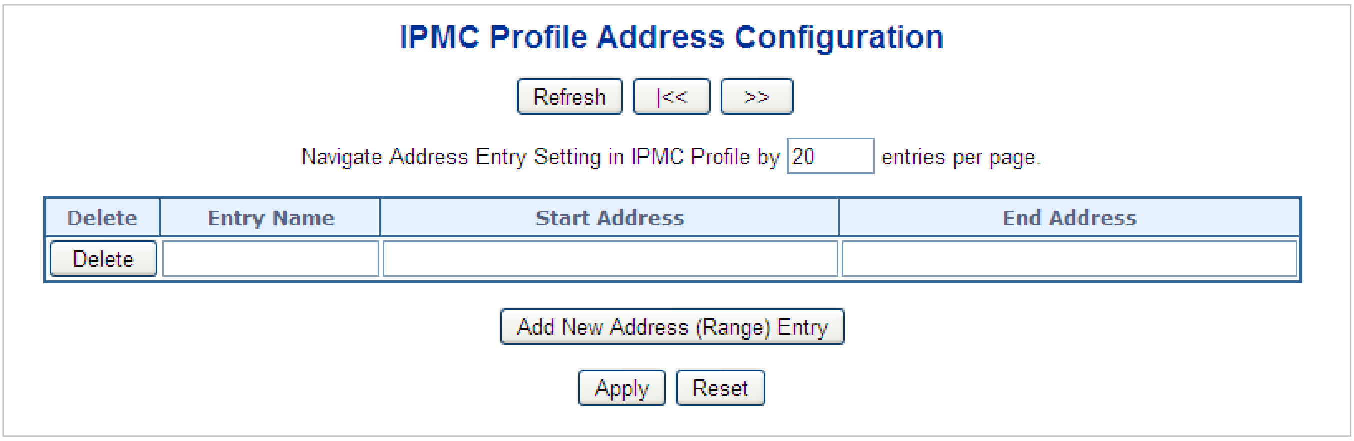


Figure 4-3-48: IPMC Profile Address Configuration Page

The page includes the following fields:

Object	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.

Buttons

Add New Address (Range) Entry: Click to add new address range. Specify the name and configure the addresses. Click "Save".

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

Refresh: Refreshes the displayed table starting from the input fields.

|<<: Updates the table starting from the first entry in the IPMC Profile Address Configuration.

>>: Updates the table, starting with the entry after the last entry currently displayed.

4.3.10.3 IGMP Snooping Configuration

This page provides IGMP Snooping related configuration. The IGMP Snooping Configuration screen in Figure 4-3-49 appears.

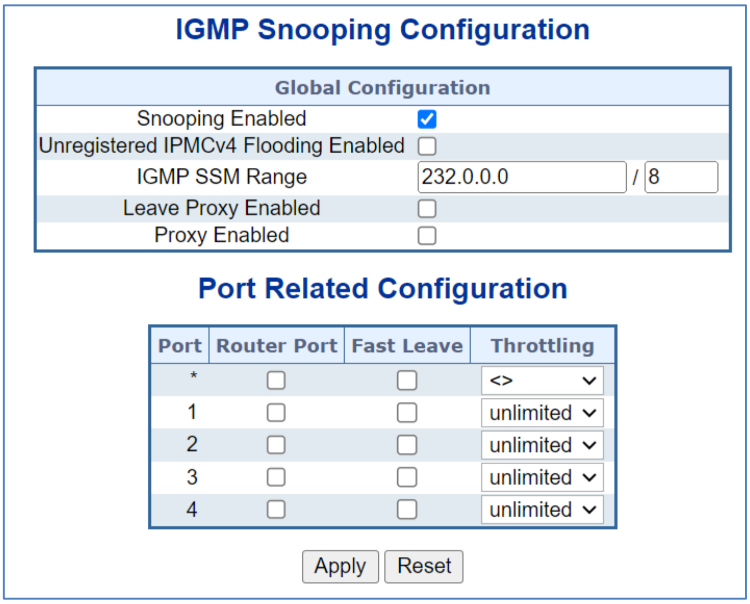


Figure 4-3-49: IGMP Snooping Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **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.
• **Leave Proxy Enable**	Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
• **Proxy Enable**	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 IGMP router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. The Switch forwards IGMP join or leave packets to an IGMP router port. ■ **Auto:** Select "Auto" to have the Managed Switch automatically uses the port as IGMP Router port if the port receives IGMP query packets. ■ **Fix**: The Managed Switch always uses the specified port as an IGMP

	Router port. Use this mode when you connect an IGMP multicast server or IP camera which applied with multicast protocol to the port. ■ **None:** The Managed Switch will not use the specified port as an IGMP Router port. The Managed Switch will not keep any record of an IGMP router being connected to this port. Use this mode when you connect other IGMP multicast servers directly on the non-querier Managed Switch and don't want the multicast stream to be flooded by uplinking switch through the port that is connected to the IGMP querier.
• **Fast Leave**	Enable the fast leave on the port.
• **Throtting**	Enable to limit the number of multicast groups to which a switch port can belong.

Buttons

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.10.4 IGMP Snooping VLAN Configuration

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. The IGMP Snooping VLAN Configuration screen in Figure 4-3-50 appears.

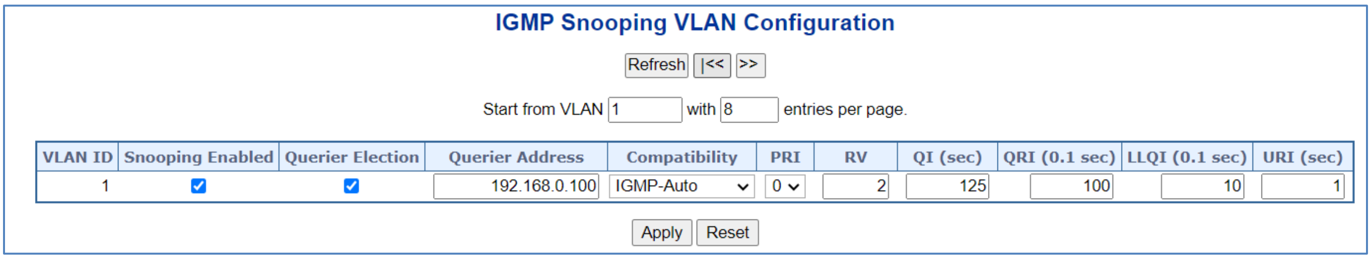


Figure 4-3-50: IGMP Snooping VLAN Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. The designated entry will be deleted during the next save.
• **VLAN ID**	The VLAN ID of the entry.
• **IGMP Snooping Enable**	Enable the per-VLAN IGMP Snooping. Only up to 32 VLANs can be selected.
• **Querier Election**	Enable the IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.
• **Querier Address**	Define the IPv4 address as source address used in IP header for IGMP Querier election. ■ When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. ■ When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1
• **Compatibility**	Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is **IGMP-Auto**, **Forced IGMPv1**, **Forced IGMPv2**, **Forced IGMPv3**. Default compatibility value is **IGMP-Auto**.
• **PRI**	(PRI) Priority of Interface. It indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic.

	The allowed range is **0** (best effort) to **7** (highest), default interface priority value is 0
• **RV**	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is **1** to **255**, default robustness variable value is 2.
• **QI**	Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is **1** to **31744** seconds, default query interval is 125 seconds.
• **QRI**	Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The allowed range is **0** to **31744** in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).
• **LLQI (LMQI for IGMP)**	Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is **0** to **31744** in tenths of seconds, default last member query interval is 10 in tenths of seconds (1 second).
• **URI**	Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is **0** to **31744** seconds, default unsolicited report interval is 1 second.

Buttons

Refresh: Refreshes the displayed table starting from the "VLAN" input fields.

|<<: Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.

>>: Updates the table, starting with the entry after the last entry currently displayed.

Add New IGMP VLAN: Click to add new IGMP VLAN. Specify the VID and configure the new entry. Click "Save". The specific IGMP VLAN starts working after the corresponding static VLAN is also created.

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.10.5 IGMP Snooping Port Group Filtering

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The IGMP filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and IGMP throttling limits the number of simultaneous multicast groups a port can join.

IGMP filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. An IGMP filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, IGMP join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the IGMP join report is forwarded as normal. If a requested multicast group is denied, the IGMP join report is dropped.

IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either "deny" or "replace". If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group. The IGMP Snooping Port Group Filtering Configuration screen in Figure 4-3-51 appears.

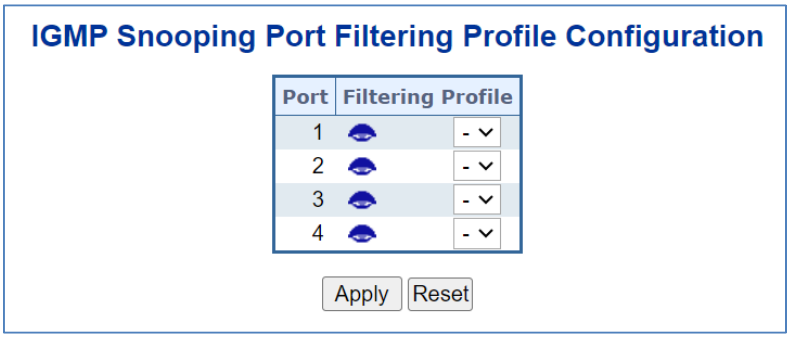


Figure 4-3-51: IGMP Snooping Port Filtering Profile Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The logical port for the settings.
• **Filtering Profile**	Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button

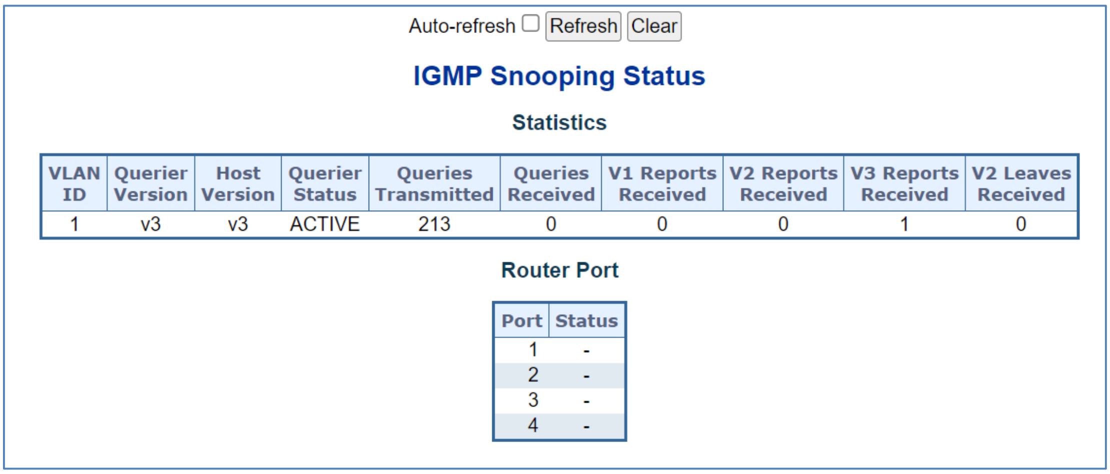
Buttons

: Click to apply changes

: Click to undo any changes made locally and revert to previously saved values.

4.3.10.6 IGMP Snooping Status

This page provides IGMP Snooping status. The IGMP Snooping Status screen in Figure 4-3-52 appears.



Auto-refresh ☐ Refresh Clear

IGMP Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
1	v3	v3	ACTIVE	213	0	0	0	1	0

Router Port

Port	Status
1	-
2	-
3	-
4	-

Figure 4-3-52: IGMP Snooping Status Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	The VLAN ID of the entry.
• **Querier Version**	Working Querier Version currently.
• **Host Version**	Working Host Version currently.
• **Querier Status**	Show the Querier status is "ACTIVE" or "IDLE".
• **Querier Transmitted**	The number of Transmitted Querier.
• **Querier Received**	The number of Received Querier.
• **V1 Reports Received**	The number of Received V1 Reports.
• **V2 Reports Received**	The number of Received V2 Reports.
• **V3 Reports Received**	The number of Received V3 Reports.
• **V2 Leave Received**	The number of Received V2 Leave.
• **Router Port**	Display 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. Static denotes the specific port is configured to be a router port. Dynamic denotes the specific port is learnt to be a router port. Both denote the specific port is configured or learnt to be a router port.
• **Port**	Switch port number.
• **Status**	Indicate whether specific port is a router port or not.

Buttons

Refresh: Click to refresh the page immediately.

Clear: Clears all Statistics counters.

Auto-refresh ☐: Automatic refresh occurs every 3 seconds.

4.3.10.7 IGMP Group Information

Entries in the IGMP Group Table are shown on this Page. The IGMP Group Table is sorted first by VLAN ID, and then by group. Each page shows up to 99 entries from the IGMP Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP Group Table. The "Start from VLAN", and "group" input fields allow the user to select the starting point in the IGMP Group Table. The IGMP Groups Information screen in Figure 4-3-53 appears.

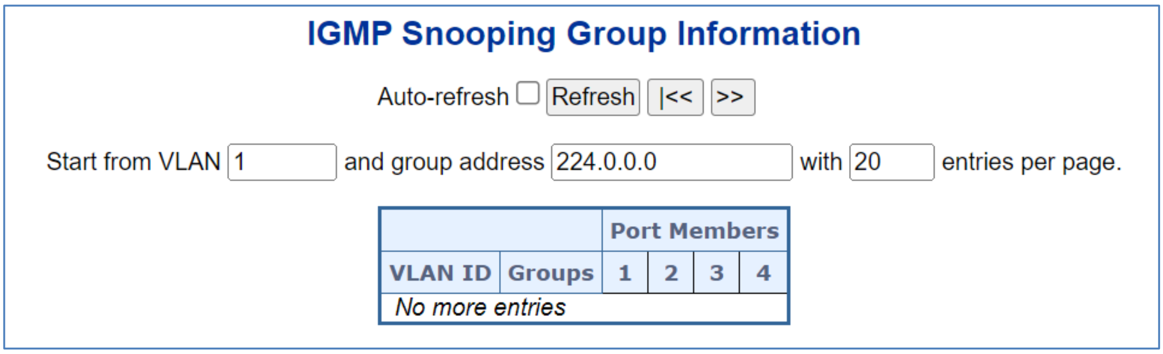


Figure 4-3-53: IGMP Snooping Groups Information Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	VLAN ID of the group.
• **Groups**	Group address of the group displayed.
• **Port Members**	Ports under this group.

Buttons

Auto-refresh ☐: Automatic refresh occurs every 3 seconds.

Refresh: Refreshes the displayed table starting from the input fields.

|<<: Updates the table, starting with the first entry in the IGMP Group Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

4.3.10.8 IGMPv3 SFM Information

Entries in the IGMP SSM Information Table are shown on this page. The IGMP SSM Information Table is sorted first by VLAN ID, then by group, and then by Port No. Diffrent source addresses belong to the same group are treated as single entry.

Each page shows up to 99 entries from the IGMP SSM (Source Specific Multicast) Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP SSM Information Table.

The "**Start from VLAN**", and "**Group**" input fields allow the user to select the starting point in the IGMP SSM Information Table. The IGMPv3 Information screen in Figure 4-3-54 appears.

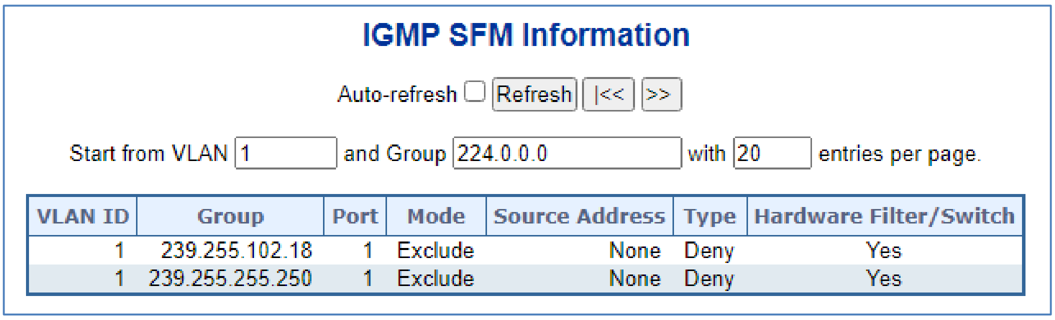


Figure 4-3-54: IGMP SSM Information Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	VLAN ID of the group.
• **Group**	Group address of the group displayed.
• **Port**	Switch port number.
• **Mode**	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
• **Source Address**	IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.
• **Type**	Indicates the Type. It can be either Allow or Deny.
• **Hardware Filter/Switch**	Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip or not.

Buttons

Auto-refresh ☐: Check this box to enable an automatic refresh of the page at regular intervals.

Refresh: Click to refresh the page immediately.

|<<: Updates the table, starting with the first entry in the IGMP Group Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

4.3.11 MLD Snooping

4.3.11.1 MLD Snooping Configuration

This page provides MLD Snooping related configuration. The MLD Snooping Configuration screen in Figure 4-3-55 appears.

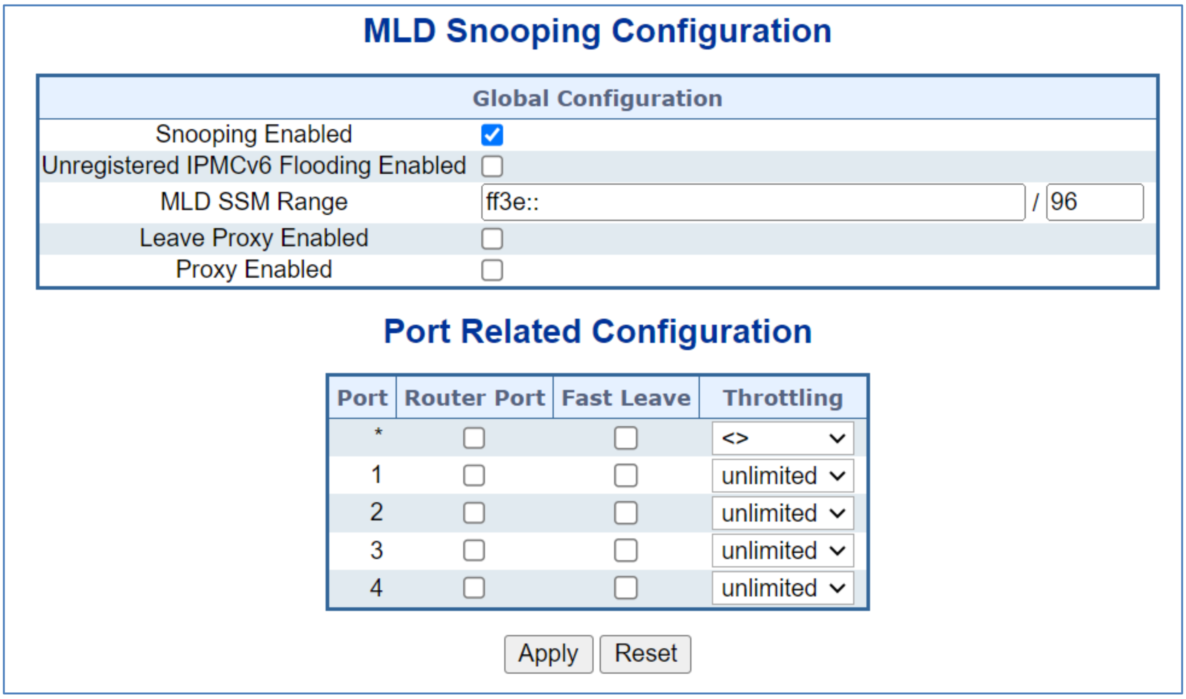


Figure 4-3-55: MLD Snooping Configuration Page Screenshot

The page includes the following fields:

Object	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.
• **Leave Proxy Enable**	Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
• **Proxy Enable**	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. The allowed selection is **Auto**, **Fix**, **Fone**,

	default compatibility value is Auto.
• **Fast Leave**	Enable the fast leave on the port.
• **Throtting**	Enable to limit the number of multicast groups to which a switch port can belong.

Buttons

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.11.2 MLD Snooping VLAN Configuration

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. The MLD Snooping VLAN Configuration screen in Figure 4-3-56 appears.

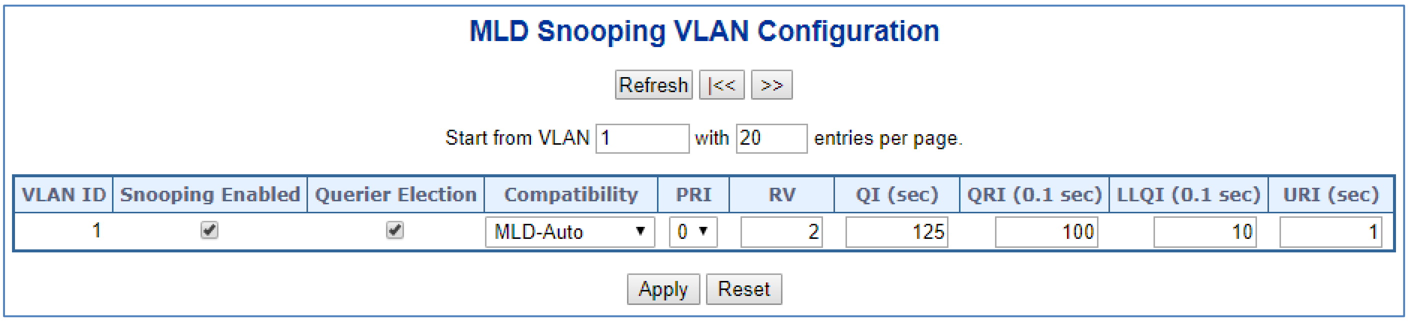


Figure 4-3-56: IGMP Snooping VLAN Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. The designated entry will be deleted during the next save.
• **VLAN ID**	The VLAN ID of the entry.
• **MLD Snooping Enable**	Enable the per-VLAN MLD Snooping. Up to 32 VLANs can be selected for MLD Snooping.
• **Querier Election**	Enable to join MLD Querier election in the VLAN. Disable to act as a MLD Non-Querier.
• **Compatibility**	Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The allowed selection is **MLD-Auto**, **Forced MLDv1**, **Forced MLDv2**, default compatibility value is MLD-Auto.
• **PRI**	(PRI) Priority of Interface. It indicates the MLD control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is **0** (best effort) to **7** (highest), default interface priority value is 0
• **RV**	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is **1** to **255**, default robustness variable value is **2**.
• **QI**	Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is **1** to **31744** seconds, default query interval is 125 seconds.

• **QRI**	Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The allowed range is **0** to **31744** in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).
• **LLQI (LMQI for IGMP)**	Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is **0** to **31744** in tenths of seconds, default last member query interval is 10 in tenths of seconds (1 second).
• **URI**	Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is **0** to **31744** seconds, default unsolicited report interval is 1 second.

Buttons

Refresh: Refreshes the displayed table starting from the "VLAN" input fields.

|<<: Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.

>>: Updates the table, starting with the entry after the last entry currently displayed.

Add New MLD VLAN:Click to add new MLD VLAN. Specify the VID and configure the new entry.

Click "Save". The specific MLD VLAN starts working after the corresponding static VLAN is also created.

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.11.3 MLD Snooping Port Group Filtering

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The MLD filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and MLD throttling limits the number of simultaneous multicast groups a port can join.

MLD filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. A MLD filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, MLD join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the MLD join report is forwarded as normal. If a requested multicast group is denied, the MLD join report is dropped.

MLD throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either "deny" or "replace". If the action is set to deny, any new MLD join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group. The MLD Snooping Port Group Filtering Configuration screen in Figure 4-3-57 appears.

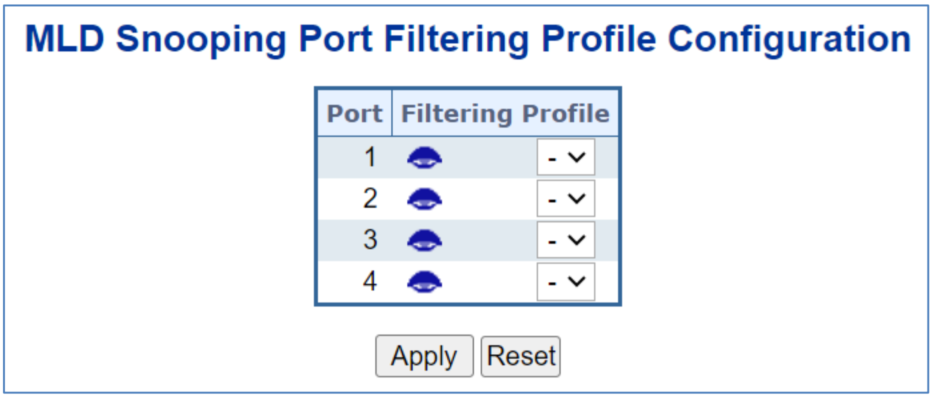


Figure 4-3-57: MLD Snooping Port Group Filtering Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The logical port for the settings.
• **Filtering Group**	Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.

Buttons

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.11.4 MLD Snooping Status

This page provides MLD Snooping status. The IGMP Snooping Status screen in Figure 4-3-58 appears.

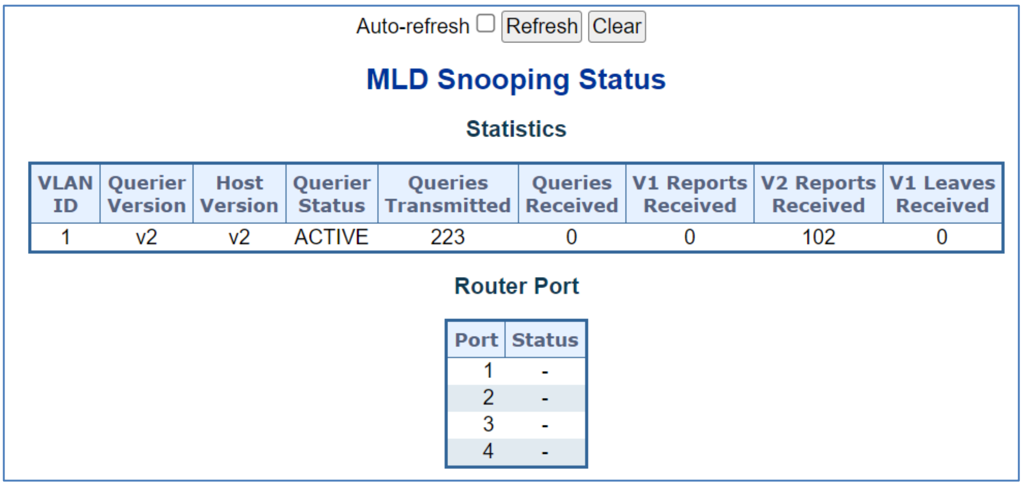


Figure 4-3-58: MLD Snooping Status Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	The VLAN ID of the entry.
• **Querier Version**	Working Querier Version currently.
• **Host Version**	Working Host Version currently.
• **Querier Status**	Shows the Querier status is "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.
• **Querier Transmitted**	The number of Transmitted Querier.
• **Querier Received**	The number of Received Querier.
• **V1 Reports Received**	The number of Received V1 Reports.
• **V2 Reports Received**	The number of Received V2 Reports.
• **V1 Leave Received**	The number of Received V1 Leaves.
• **Router Port**	Display 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. Static denotes the specific port is configured to be a router port. Dynamic denotes the specific port is learnt to be a router port. Both denote the specific port is configured or learnt to be a router port.
• **Port**	Switch port number.
• **Status**	Indicates whether specific port is a router port or not.

Buttons

Refresh: Click to refresh the page immediately.

Clear: Clears all Statistics counters.

Auto-refresh ☐: Automatic refresh occurs every 3 seconds.

4.3.11.5 MLD Group Information

Entries in the MLD Group Table are shown on this page. The MLD Group Table is sorted first by VLAN ID, and then by group. Each page shows up to 99 entries from the MLD Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD Group Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD Group Table. The MLD Groups Information screen in Figure 4-3-59 appears.

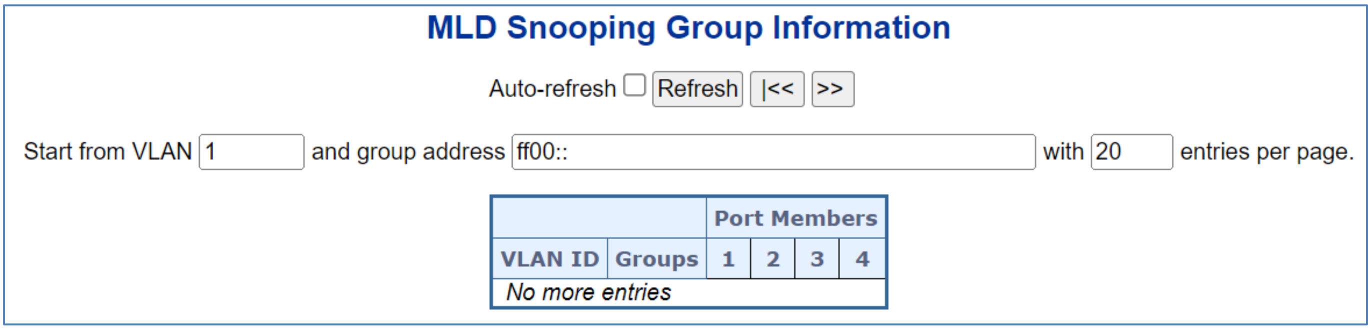


Figure 4-3-59: MLD Snooping Groups Information Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	VLAN ID of the group.
• **Groups**	Group address of the group displayed.
• **Port Members**	Ports under this group.

Buttons

Auto-refresh : Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately.

: Updates the table, starting with the first entry in the IGMP Group Table.

: Updates the table, starting with the entry after the last entry currently displayed.

4.3.11.6 MLDv2 SFM Information

Entries in the MLD SFM Information Table are shown on this page. The MLD SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry. Each page shows up to 99 entries from the MLD SFM Information table, default being 20, selected through the "entries per page" input field. When first visited, the web Page will show the first 20 entries from the beginning of the MLD SFM Information Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD SFM Information Table. The MLDv2 Information screen in Figure 4-3-60 appears.

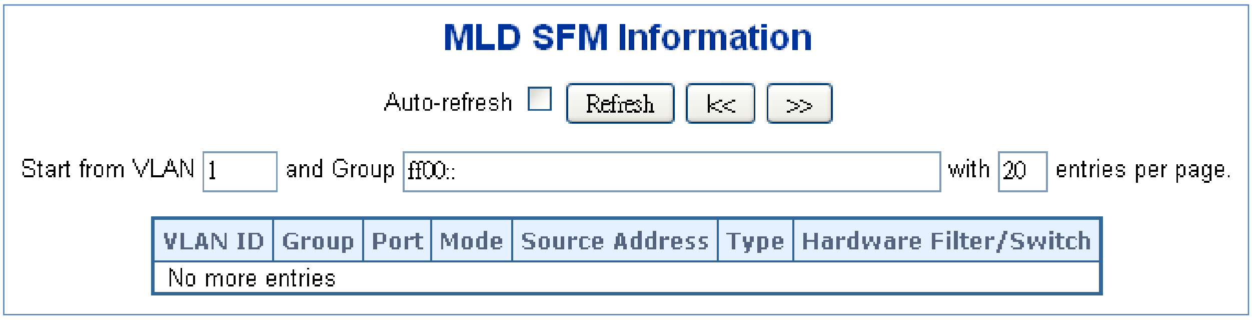


Figure 4-3-60: MLD SSM Information Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	VLAN ID of the group.
• **Group**	Group address of the group displayed.
• **Port**	Switch port number.
• **Mode**	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
• **Source Address**	IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.
• **Type**	Indicates the Type. It can be either Allow or Deny.
• **Hardware Filter/Switch**	Indicates whether data plane destined to the specific group address from the source IPv6 address could be handled by chip or not.

Buttons

Auto-refresh ☐: Automatic refresh occurs every 3 seconds.

Refresh: Refreshes the displayed table starting from the input fields.

|<<: Updates the table starting from the first entry in the MLD SFM Information Table.

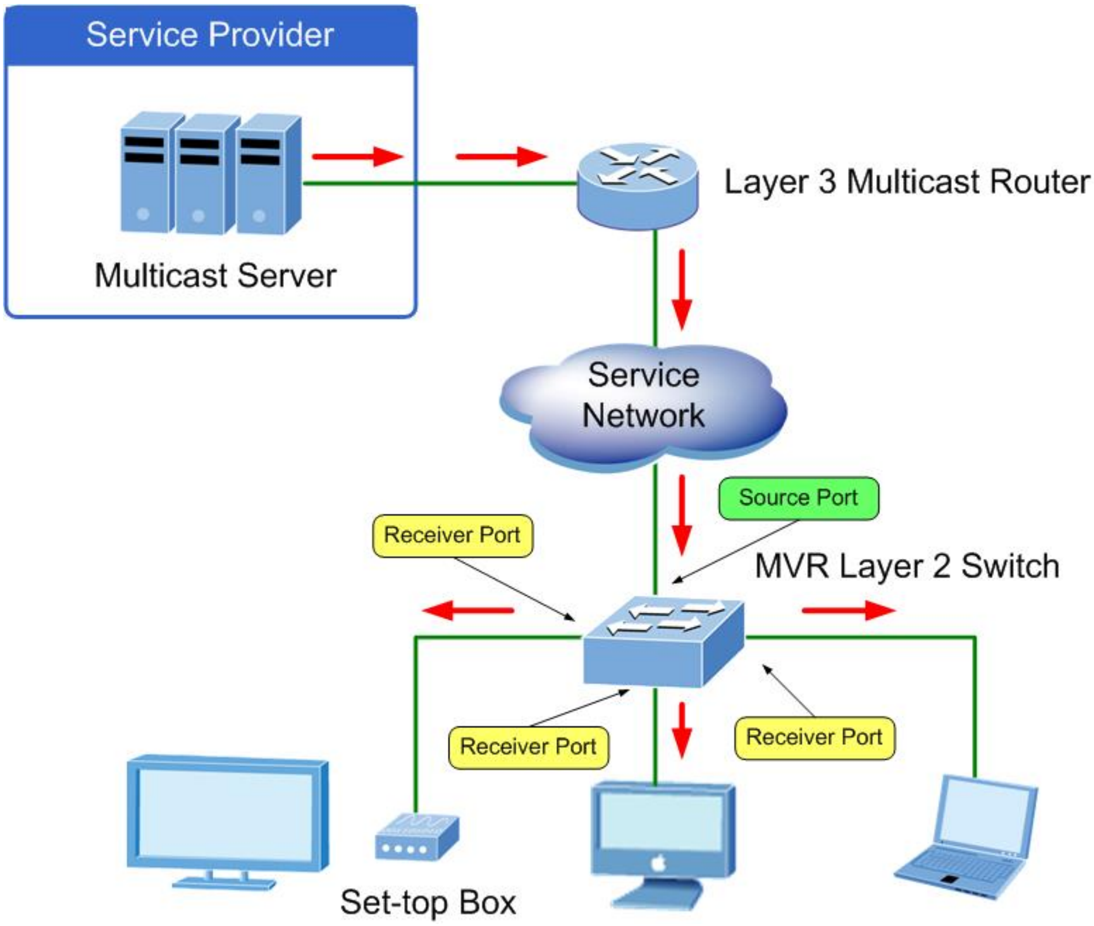
>>: Updates the table, starting with the entry after the last entry currently displayed.

4.3.12 MVR

The MVR feature enables multicast traffic forwarding on the Multicast VLANs.

- In a multicast television application, a PC or a network television or a set-top box can receive the multicast stream.
- Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP/MLD report message to Switch A to join the appropriate multicast group address.
- Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

It is allowed to create at maximum 8 MVR VLANs with corresponding channel settings for each Multicast VLAN. There will be totally at maximum 256 group addresses for channel settings.



4.3.12.1 MVR Configuration

This page provides MVR related configuration. The MVR screen in Figure 4-3-61 appears

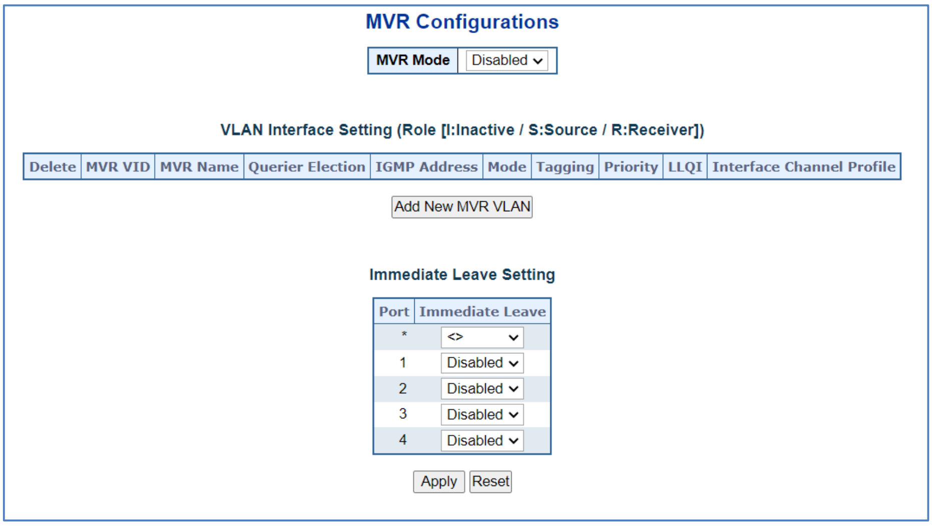


Figure 4-3-61: MVR Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **MVR Mode**	Enable/Disable the Global MVR. The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping. It is suggested to enable Unregistered Flooding control when the MVR group table is full.
• **Delete**	Check to delete the entry. The designated entry will be deleted during the next save.
• **MVR VID**	Specify the Multicast VLAN ID. **Be Caution**: MVR source ports are not recommended to be overlapped with management VLAN ports.
• **MVR Name**	MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 16. MVR VLAN Name can only contain alphabets or numbers. When the optional MVR VLAN name is given, it should contain at least one alphabet. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.
• **IGMP Address**	Define the IPv4 address as source address used in IP header for IGMP control frames. The default IGMP address is not set (0.0.0.0). When the IGMP address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

• **Mode**	Specify the MVR mode of operation. In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR membership reports are forbidden on source ports. The default is Dynamic mode.
• **Tagging**	Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is Tagged.
• **Priority**	Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.
• **LLQI**	Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a seconds. The range is from 0 to 31744. The default LLQI is 5 tenths or one-half second.
• **Interface Channel Setting**	When the MVR VLAN is created, select the IPMC Profile as the channel filtering condition for the specific MVR VLAN. Summary about the Interface Channel Profiling (of the MVR VLAN) will be shown by clicking the view button. Profile selected for designated interface channel is not allowed to have overlapped permit group address.
• **Port**	The logical port for the settings.
• **Port Role**	Configure an MVR port of the designated MVR VLAN as one of the following roles. ■ **Inactive**: The designated port does not participate MVR operations. ■ **Source**: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports. ■ **Receiver**: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages. **Be Caution**: MVR source ports are not recommended to be overlapped with management VLAN ports. Select the port role by clicking the Role symbol to switch the setting. I indicates Inactive; S indicates Source; R indicates Receiver The default Role is Inactive.
• **Immediate Leave**	Enable the fast leave on the port.

Buttons

Add New MVR VLAN: Click to add new MVR VLAN. Specify the VID and configure the new entry. Click "Save"

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.12.2 MVR Statistics

This page provides MVR status. The MVR Status screen in Figure 4-3-62 appears.

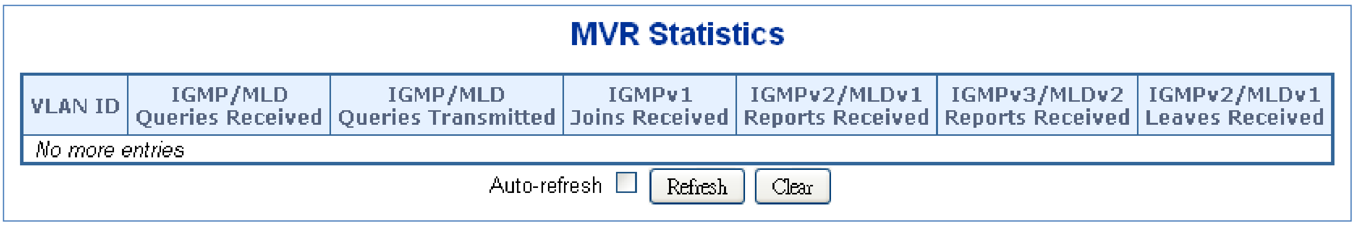


Figure 4-3-62: MVR Status Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	The Multicast VLAN ID.
• **IGMP/MLD Queries Received**	The number of Received Queries for IGMP and MLD, respectively.
• **IGMP/MLD Queries Transmitted**	The number of Transmitted Queries for IGMP and MLD, respectively.
• **IGMPv1 Joins Received**	The number of Received IGMPv1 Joins.
• **IGMPv2/MLDv1 Reports Received**	The number of Received IGMPv2 Joins and MLDv1 Reports, respectively.
• **IGMPv3/MLDv2 Reports Received**	The number of Received IGMPv1 Joins and MLDv2 Reports, respectively.
• **IGMPv2/MLDv1 Leaves Received**	The number of Received IGMPv2 Leaves and MLDv1 Dones, respectively.

Buttons

Refresh: Click to refresh the page immediately.

Clear: Clears all Statistics counters.

Auto-refresh : Automatic refresh occurs every 3 seconds.

4.3.12.3 MVR Groups Information

Entries in the MVR Group Table are shown on this page. The MVR Group Table is sorted first by VLAN ID, and then by group. Each page shows up to 99 entries from the MVR Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR Group Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MVR Group Table. The MVR Groups Information screen in Figure 4-3-63 appears.

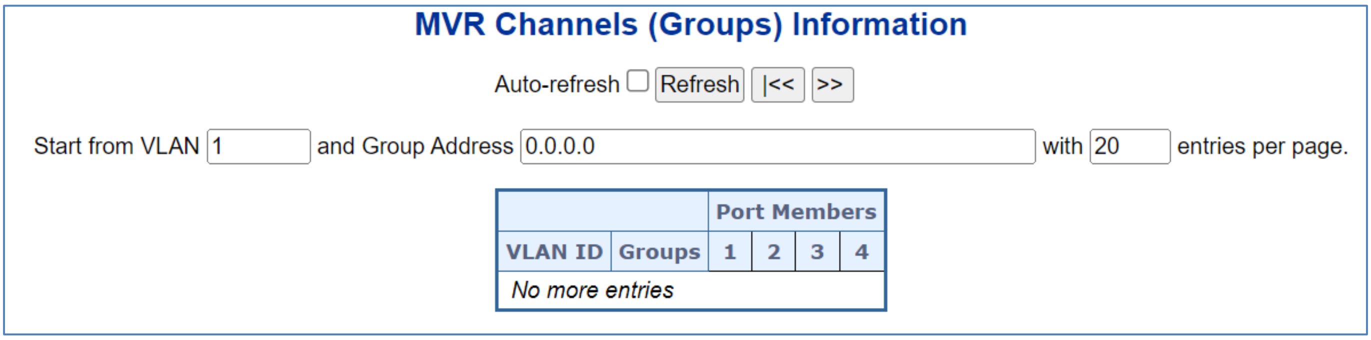


Figure 4-3-63: MVR Groups Information Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN**	VLAN ID of the group.
• **Groups**	Group ID of the group displayed.
• **Port Members**	Ports under this group.

Buttons

Auto-refresh ☐: Automatic refresh occurs every 3 seconds.

Refresh: Refreshes the displayed table starting from the input fields.

|<<: Updates the table starting from the first entry in the MVR Channels (Groups) Information Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

4.3.12.4 MVR SFM Information

Entries in the MVR SFM Information Table are shown on this page. The MVR **SFM** (**Source-Filtered Multicast**) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Each page shows up to 99 entries from the MVR SFM Information Table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR SFM Information Table.

The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR SFM Information Table. The MVR SFM Information screen in Figure 4-3-64 appears.

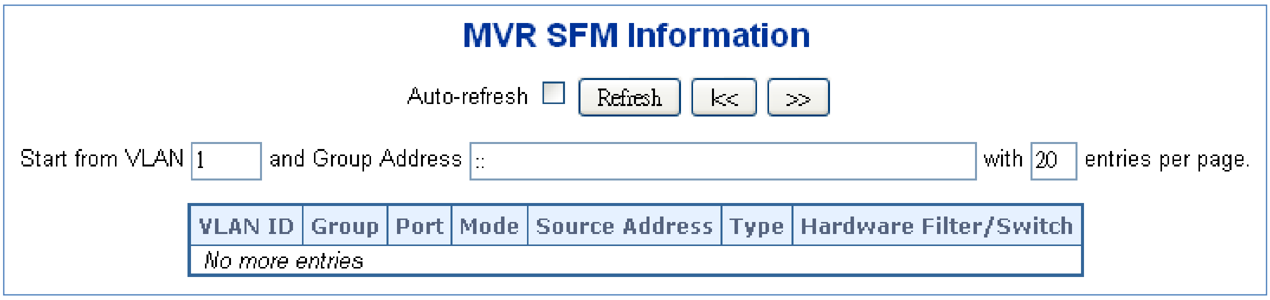


Figure 4-3-64: MVR SFM Information Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	VLAN ID of the group.
• **Group**	Group address of the group displayed.
• **Port**	Switch port number.
• **Mode**	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
• **Source Address**	IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128. When there is no any source filtering address, the text "None" is shown in the Source Address field.
• **Type**	Indicates the Type. It can be either Allow or Deny.
• **Hardware Filter / Switch**	Indicates whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by chip or not.

Buttons

Auto-refresh ☐: Automatic refresh occurs every 3 seconds.

Refresh: Refreshes the displayed table starting from the input fields.

|<<: Updates the table starting from the first entry in the MVR SFM Information Table.

4.3.13 LLDP

4.3.13.1 Link Layer Discovery Protocol

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in **Type Length Value (TLV)** format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) is an extension of LLDP intended for managing endpoint devices such as Voice over IP phones and network switches. The LLDP-MED TLVs advertise information such as network policy, power, inventory, and device location details. LLDP and LLDP-MED information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

4.3.13.2 LLDP Configuration

This page allows the user to inspect and configure the current LLDP port settings. The LLDP Configuration screen in Figure 4-3-65 appears.

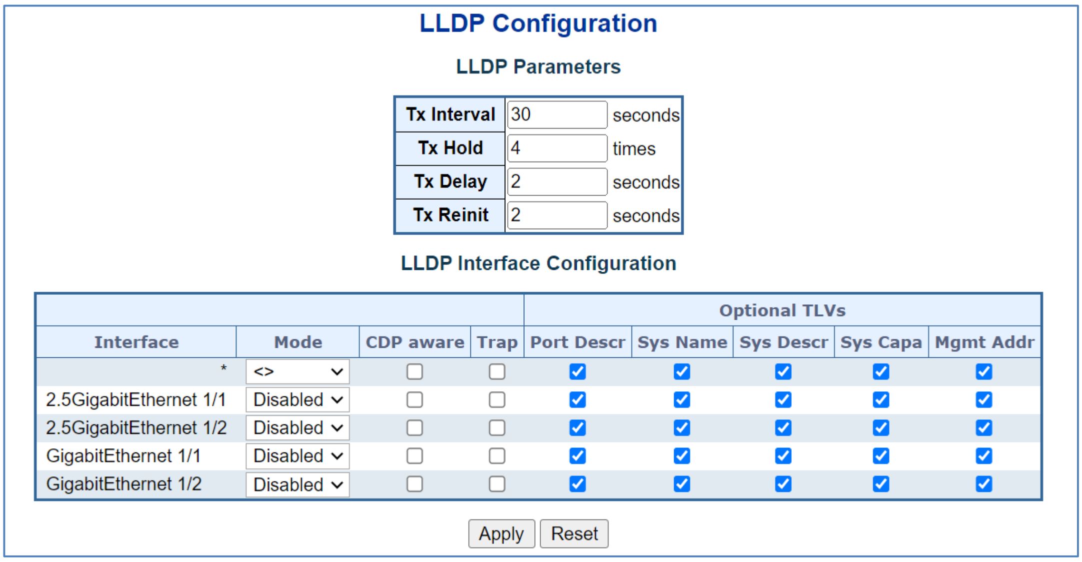


Figure 4-3-65: LLDP Configuration Page Screenshot

The page includes the following fields:

LLDP Parameters

Object	Description
• **Tx Interval**	The switch is periodically transmitting LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the **Tx Interval** value. Valid values are restricted to 5 - 32768 seconds. Default: **30** seconds This attribute must comply with the following rule:

	(Transmission Interval * Hold Time Multiplier) ≤65536, and Transmission Interval >= (4 * Delay Interval)
• **Tx Hold**	Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to **Tx Hold** multiplied by **Tx Interval** seconds. Valid values are restricted to 2 - 10 times. TTL in seconds is based on the following rule: (Transmission Interval * Holdtime Multiplier) ≤ 65536. Therefore, the default TTL is 4*30 = 120 seconds.
• **Tx Delay**	If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of **Tx Delay** seconds. **Tx Delay** cannot be larger than 1/4 of the **Tx Interval** value. Valid values are restricted to 1 - 8192 seconds. This attribute must comply with the rule: (4 * Delay Interval) ≤Transmission Interval
• **Tx Reinit**	When a port is disabled, LLDP is disabled or the switch is rebooted a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. **Tx Reinit** controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.

LLDP Port Configuration

The LLDP port settings relate to the switch, as reflected by the page header.

Object	Description
• **Port**	The switch port number of the logical LLDP port.
• **Mode**	Select LLDP mode. ■ **Rx only** The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed. ■ **Tx only** The switch will drop LLDP information received from neighbors, but will send out LLDP information. ■ **Disabled** The switch will not send out LLDP information, and will drop LLDP information received from neighbors. ■ **Enabled** The switch will send out LLDP information, and will analyze LLDP information received from neighbors.
• **CDP Aware**	Select CDP awareness. The CDP operation is restricted to decoding incoming CDP frames (**The switch doesn't transmit CDP frames**). CDP frames are only decoded if LLDP on the port is enabled.

	Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbours' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbours' table as shown below. CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field. CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbours table. CDP TLV "Port ID" is mapped to the LLDP "Port ID" field. CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field. Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbours' table. If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbour devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch. Note: When CDP awareness on a port is disabled the CDP information isn't removed immediately, but gets removed when the hold time is exceeded.
• **Port Description**	Optional TLV: When checked the "port description" is included in LLDP information transmitted.
• **System Name**	Optional TLV: When checked the "system name" is included in LLDP information transmitted.
• **System Description**	Optional TLV: When checked the "system description" is included in LLDP information transmitted.
• **System Capabilities**	Optional TLV: When checked the "system capability" is included in LLDP information transmitted.
• **Management Address**	Optional TLV: When checked the "management address" is included in LLDP information transmitted.

Buttons

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.13.3 Neighbor

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. The LLDP Neighbor Information screen in Figure 4-3-66 appears.

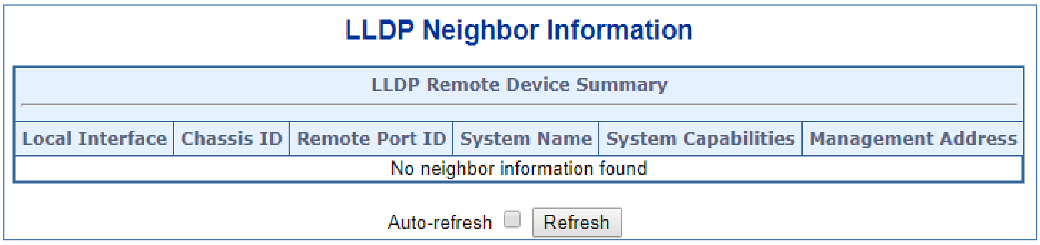


Figure 4-3-66: LLDP Neighbor Information Page Screenshot

The page includes the following fields:

Object	Description
• **Local Port**	The port on which the LLDP frame was received.
• **Chassis ID**	The Chassis ID is the identification of the neighbor's LLDP frames.
• **Remote Port ID**	The Remote Port ID is the identification of the neighbor port.
• **Port Description**	Port Description is the port description advertised by the neighbor unit.
• **System Name**	System Name is the name advertised by the neighbor unit.
• **System Capabilities**	System Capabilities describes the neighbor unit's capabilities. The possible capabilities are: 1. Other 2. Repeater 3. Bridge 4. WLAN Access Point 5. Router 6. Telephone 7. DOCSIS cable device 8. Station only 9. Reserved When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).
• **Management Address**	Management Address is the neighbor unit's address that is used for higher layer entities to assist the discovery by the network management. This could for instance hold the neighbor's IP address.

Refresh: Click to refresh the page immediately.

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.3.13.4 LLDP-MED Configuration

This page allows you to configure the LLDP-MED. The LLDPMED Configuration screen in Figure 4-3-67 appears.

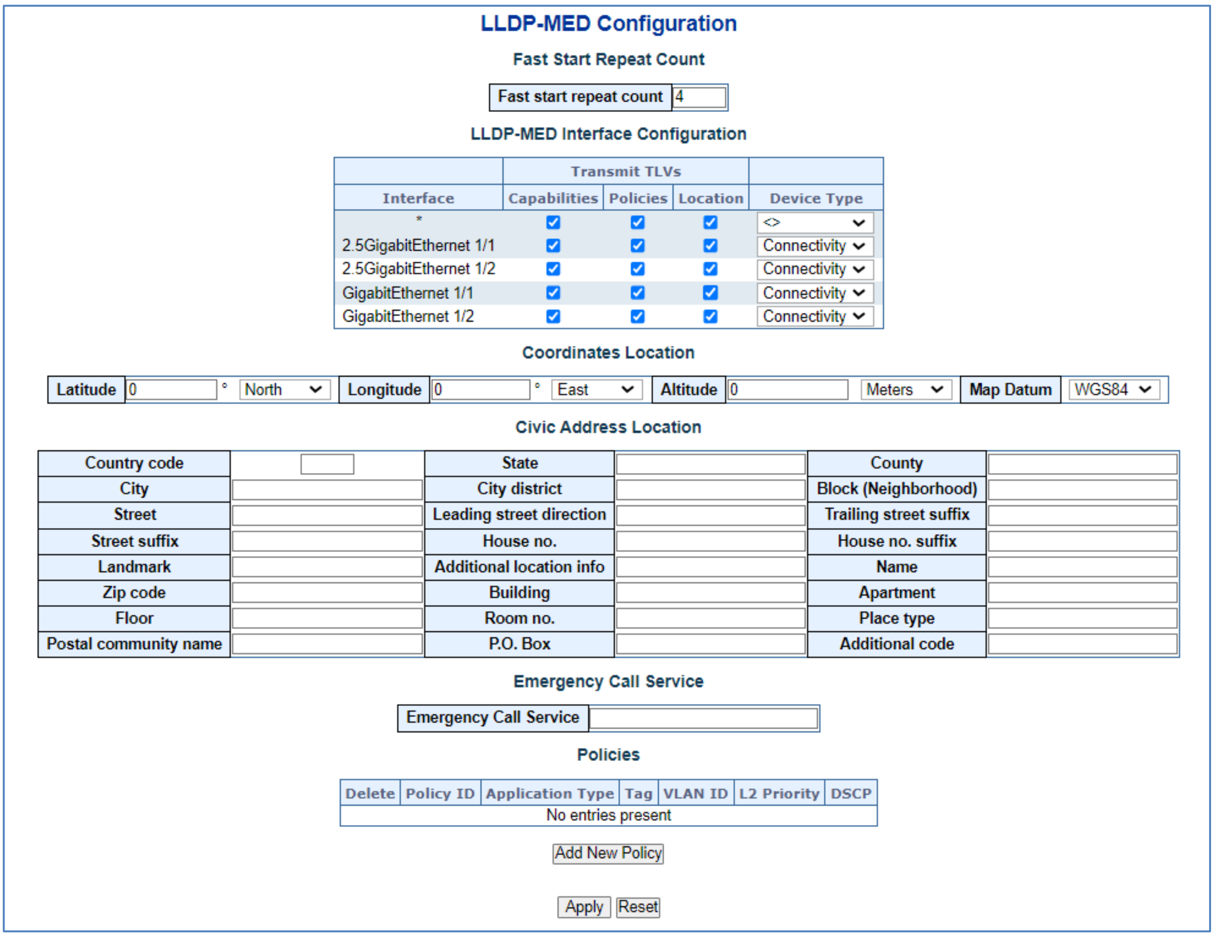


Figure 4-3-67: LLDP-MED Configuration Page Screenshot

The page includes the following fields:

Fast start repeat count

Object	Description
• **Fast start repeat count**	Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy. With this in mind LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device

	start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbour has been detected in order share LLDP-MED information as fast as possible to new neighbours. Because there is a risk of an LLDP frame being lost during transmission between neighbours, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbours receiving the LLDP frame. With **Fast start repeat count** it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received. It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including Network Connectivity Devices, or other types of links.

LLDP-MED Interface Configuration

Object	Description
• **Interface**	The interface name to which the configuration applies.
• **Transmit TLVs - Capabilities**	When checked the switch's capabilities is included in LLDP-MED information transmitted
• **Transmit TLVs - Policies**	When checked the configured policies for the interface is included in LLDP-MED information transmitted.
• **Transmit TLVs - Location**	When checked the configured location information for the switch is included in LLDP-MEDinformation transmitted.
• **Transmit TLVs - PoE**	When checked the configured PoE (Power Over Ethernet) information for the interface is included in LLDP-MED information transmitted
• **Device Type**	Any LLDP-MED Device is operating as a specific type of LLDP-MED Device, which may be either a Network Connectivity Device or a specific Class of Endpoint Device, as defined below. A Network Connectivity Device is a LLDP-MED Device that provides access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies : 1. LAN Switch/Router 2. IEEE 802.1 Bridge

	3. IEEE 802.3 Repeater (included for historical reasons) 4. IEEE 802.11 Wireless Access Point 5. Any device that supports the IEEE 802.1AB and MED extensions that can relay IEEE 802 frames via any method. An Endpoint Device a LLDP-MED Device that sits at the network edge and provides some aspect of IP communications service, based on IEEE 802 LAN technology. The main difference between a Network Connectivity Device and an Endpoint Device is that only an Endpoint Device can start the LLDP-MED information exchange. Even though a switch always should be a Network Connectivity Device, it is possible to configure it to act as an Endpoint Device, and thereby start the LLDP-MED information exchange (In the case where two Network Connectivity Devices are connected together)

Coordinates Location

Object	Description
• **Latitude**	**Latitude** SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either **North** of the equator or **South** of the equator.
• **Longitude**	**Longitude** SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either **East** of the prime meridian or **West** of the prime meridian.
• **Altitude**	**Altitude** SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (floors or meters). **Meters**: Representing meters of Altitude defined by the vertical datum specified. **Floors**: Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.
• **Map Datum**	The **Map Datum** used for the coordinates given in this Option ■ **WGS84**: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich. ■ **NAD83/NAVD88**: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North

	American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW). ■ **NAD83/MLLW**: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

Civic Address Location

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI).

Object	Description
• **Country code**	The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.
• **State**	National subdivisions (state, canton, region, province, prefecture).
• **County**	County, parish, gun (Japan), district.
• **City**	City, township, shi (Japan) - Example: Copenhagen
• **City district**	City division, borough, city district, ward, chou (Japan)
• **Block (Neighborhood)**	Neighborhood, block
• **Street**	Street - Example: Poppelvej
• **Leading street direction**	Leading street direction - Example: N
• **Trailing street suffix**	Trailing street suffix - Example: SW
• **Street suffix**	Street suffix - Example: Ave, Platz
• **House no.**	House number - Example: 21
• **House no. suffix**	House number suffix - Example: A, 1/2
• **Landmark**	Landmark or vanity address - Example: Columbia University
• **Additional location info**	Additional location info - Example: South Wing
• **Name**	Name (residence and office occupant) - Example: Flemming Jahn
• **Zip code**	Postal/zip code - Example: 2791
• **Building**	Building (structure) - Example: Low Library
• **Apartment**	Unit (Apartment, suite) - Example: Apt 42
• **Floor**	Floor - Example: 4
• **Room no.**	Room number - Example: 450F
• **Place type**	Place type - Example: Office
• **Postal community name**	Postal community name - Example: Leonia
• **P.O. Box**	Post office box (P.O. BOX) - Example: 12345
• **Additional code**	Additional code - Example: 1320300003

Emergency Call Service

Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

Object	Description
• **Emergency Call Service**	**Emergency Call Service** ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Policies

Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service.

Policies are only intended for use with applications that have specific 'real-time' network policy requirements, such as interactive voice and/or video services.

The network policy attributes advertised are:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)
2. Layer 2 priority value (IEEE 802.1D-2004)
3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:

1. Voice
2. Guest Voice
3. Softphone Voice
4. Video Conferencing
5. Streaming Video
6. Control / Signaling (conditionally support a separate network policy for the media types above)

A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration.

It should be noted that LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

Object	Description
• **Delete**	Check to delete the policy. It will be deleted during the next save.
• **Policy ID**	ID for the policy. This is auto generated and shall be used when selecting the polices that shall be mapped to the specific ports.
• **Application Type**	Intended use of the application types: ■ **Voice** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications. ■ **Voice Signaling (conditional)** - for use in network topologies that require a different policy for the voice signaling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy. ■ **Guest Voice** - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services. ■ **Guest Voice Signaling (conditional)** - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy. ■ **Softphone Voice** - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance. ■ **Video Conferencing** - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services. ■ **Streaming Video** - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type. ■ **Video Signaling (conditional)** - for use in network topologies that require a separate policy for the video signaling than for the video media. This application type should not be advertised if all the same

	network policies apply as those advertised in the Video Conferencing application policy.
• **Tag**	**Tag** indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN. ■ **Untagged** indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance. ■ **Tagged** indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.
• **VLAN ID**	VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003
• **L2 Priority**	L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.
• **DSCP**	DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.
• **Adding a new policy**	Click [Add New Policy] to add a new policy. Specify the **Application type**, **Tag**, **VLAN ID**, **L2 Priority** and **DSCP** for the new policy. Click "Save". The number of policies supported is 32

Port Policies Configuration

Every port may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or port configuration.

Object	Description
• **Port**	The port number for which the configuration applies.
• **Policy ID**	The set of policies that shall apply for a given port. The set of policies is selected by checkmarking the checkboxes that corresponds to the policies

Buttons

[Apply]: Click to apply changes

[Reset]: Click to undo any changes made locally and revert to previously saved values.

4.3.13.5 LLDP-MED Neighbor

This page provides a status overview for all LLDP-MED neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. The LLDP-MED Neighbor Information screen in Figure 4-3-68 appears. The columns hold the following information:

LLDP-MED Neighbour Information

Port 1					
Device Type	Capabilities				
Endpoint Class III	LLDP-MED Capabilities, Network Policy, Extended Power via MDI - PD, Inventory				
Application Type	Policy	Tag	VLAN ID	Priority	DSCP
Voice	Defined	Untagged	-	-	46
Voice Signaling	Defined	Untagged	-	-	32
Auto-negotiation	Auto-negotiation status	Auto-negotiation Capabilities	MAU Type		
Supported	Enabled	1000BASE-T half duplex mode, 1000BASE-X, -LX, -SX, -CX full duplex mode , Asymmetric and Symmetric PAUSE for full-duplex inks, Symmetric PAUSE for full-duplex links	100BaseTXFD - 2 pair category 5 UTP, full duplex mode		

Figure 4-3-68: LLDP-MED Neighbor Information Page Screenshot

The page includes the following fields:

Fast start repeat count

Object	Description
• **Port**	The port on which the LLDP frame was received.
• **Device Type**	LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices. **LLDP-MED Network Connectivity Device Definition** LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies: 1. LAN Switch/Router 2. IEEE 802.1 Bridge 3. IEEE 802.3 Repeater (included for historical reasons) 4. IEEE 802.11 Wireless Access Point 5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method. **LLDP-MED Endpoint Device Definition** Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following. Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. Fore-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and

	any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I). **LLDP-MED Generic Endpoint (Class I)** The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057. Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management. **LLDP-MED Media Endpoint (Class II)** The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar. Discovery services defined in this class include media-type-specific network layer policy discovery. **LLDP-MED Communication Endpoint (Class III)** The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user. Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management
• **LLDP-MED Capabilities**	LLDP-MED Capabilities describes the neighbor unit's LLDP-MED capabilities. The possible capabilities are: 1. LLDP-MED capabilities 2. Network Policy 3. Location Identification 4. Extended Power via MDI - PSE

	5. Extended Power via MDI - PD 6. Inventory 7. Reserved
• **Application Type**	Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below. ■ **Voice** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications. ■ **Voice Signaling** - for use in network topologies that require a different policy for the voice signaling than for the voice media. ■ **Guest Voice** - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services. ■ Guest Voice Signaling - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. ■ **Softphone Voice** - for use by softphone applications on typical data centric devices, such as PCs or laptops. ■ **Video Conferencing** - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services. ■ **Streaming Video** - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type. ■ **Video Signaling** - for use in network topologies that require a separate policy for the video signaling than for the video media.
• **Policy**	**Policy** indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either Defined or Unknown ■ **Unknown**: The network policy for the specified application type is currently unknown. ■ **Defined**: The network policy is defined.
• **TAG**	TAG is indicating whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged or Untagged ■ **Untagged**: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. ■ **Tagged**: The device is using the IEEE 802.1Q tagged frame format
• **VLAN ID**	VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-

	2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.
• **Priority**	Priority is the Layer 2 priority to be used for the specified application type. One of eight priority levels (0 through 7)
• **DSCP**	DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).
• **Auto-negotiation**	**Auto-negotiation** identifies if MAC/PHY auto-negotiation is supported by the link partner.
• **Auto-negotiation status**	**Auto-negotiation status** identifies if auto-negotiation is currently enabled at the link partner. If **Auto-negotiation** is supported and **Auto-negotiation status** is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.
• **Auto-negotiation Capabilities**	**Auto-negotiation Capabilities** shows the link partners MAC/PHY capabilities.

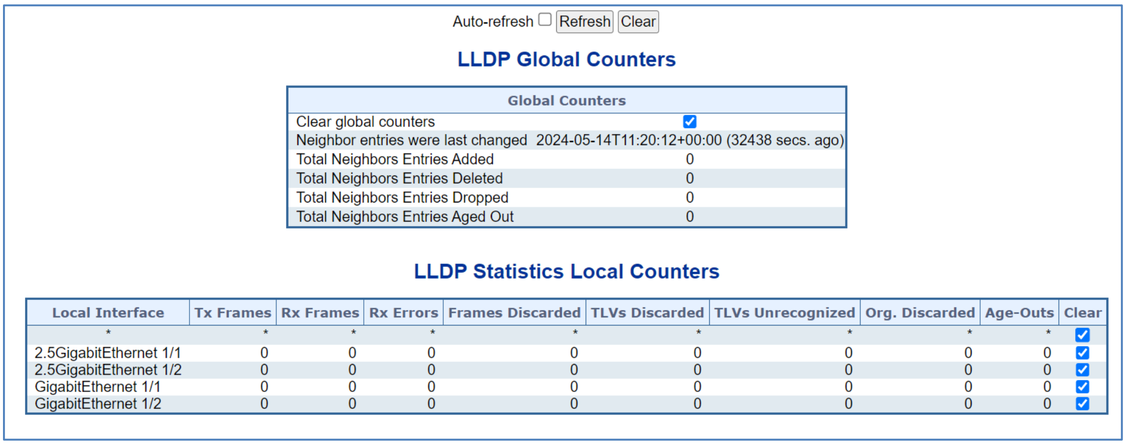
Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.3.13.6 Port Statistics

This page provides an overview of all LLDP traffic. Two types of counters are shown. Global counters are counters that refer to the whole switch, while local counters refers to counters for the currently selected switch. The LLDP Statistics screen in Figure 4-3-69 appears.


Auto-refresh ☐ Refresh Clear

LLDP Global Counters

Global Counters	
Clear global counters	☑
Neighbor entries were last changed	2024-05-14T11:20:12+00:00 (32438 secs. ago)
Total Neighbors Entries Added	0
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics Local Counters

Local Interface	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs	Clear
*	*	*	*	*	*	*	*	*	☑
2.5GigabitEthernet 1/1	0	0	0	0	0	0	0	0	☑
2.5GigabitEthernet 1/2	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/1	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/2	0	0	0	0	0	0	0	0	☑

Figure 4-3-69: LLDP Statistics Page Screenshot

The page includes the following fields:

Global Counters

Object	Description
• **Clear global counters**	If checked the global counters are cleared when Clear is pressed.
• **Neighbor entries were last changed**	It also shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.
• **Total Neighbors Entries Added**	Shows the number of new entries added since switch reboot.
• **Total Neighbors Entries Deleted**	Shows the number of new entries deleted since switch reboot.
• **Total Neighbors Entries Dropped**	Shows the number of LLDP frames dropped due to that the entry table was full.
• **Total Neighbors Entries Aged Out**	Shows the number of entries deleted due to Time-To-Live expiring.

LLDP Statistics Local Counters

The displayed table contains a row for each port. The columns hold the following information:

Object	Description
• **Local Port**	The port on which LLDP frames are received or transmitted.
• **Tx Frames**	The number of LLDP frames transmitted on the port.
• **Rx Frames**	The number of LLDP frames received on the port.
• **Rx Errors**	The number of received LLDP frames containing some kind of error.
• **Frames Discarded**	If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port links down, an LLDP shutdown frame is received, or when the entry ages out.
• **TLVs Discarded**	Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
• **TLVs Unrecognized**	The number of well-formed TLVs, but with an unknown type value.
• **Org. Discarded**	The number of organizationally TLVs received.
• **Age-Outs**	Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the **Age-Out** counter is incremented.

Buttons

Refresh: Click to refresh the page immediately.

Clear: Clears the local counters. All counters (including global counters) are cleared upon reboot.

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.3.14 MAC Address Table

Switching of frames is based upon the DMAC address contained in the frame. The **Industrial Managed TSN Device** builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

4.3.14.1 MAC Table Configuration

The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here. The MAC Address Table Configuration screen in Figure 4-3-70 appears.

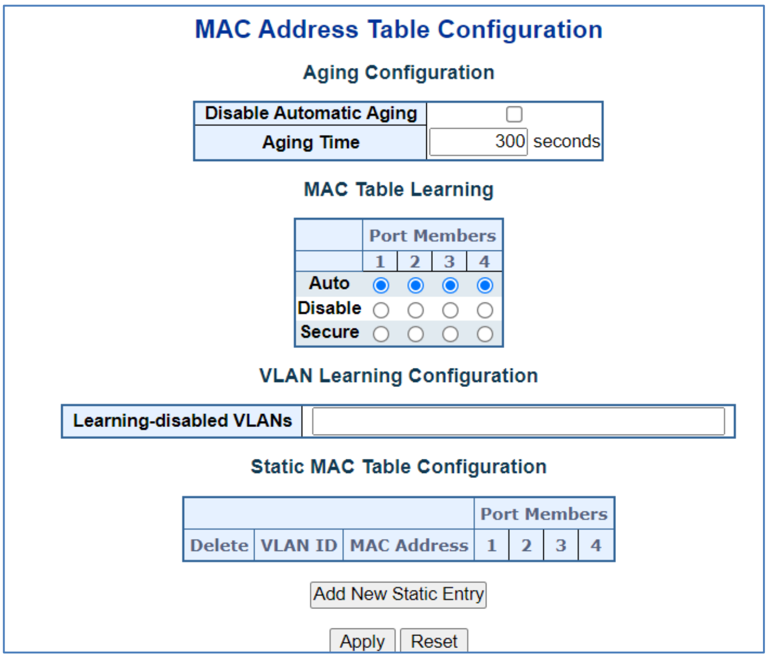


Figure 4-3-70: MAC Address Table Configuration Page Screenshot

The page includes the following fields:

Aging Configuration

By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging.

Object	Description
• **Disable Automatic Aging**	Enables/disables the automatic aging of dynamic entries
• **Aging Time**	The time after which a learned entry is discarded. By default, dynamic entries are removed from the MAC after 300 seconds. This removal is also called aging. (Range: 10-10000000 seconds; Default: 300 seconds)

MAC Table Learning

If the learning mode for a given port is grayed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X.

Object	Description
• **Auto**	Learning is done automatically as soon as a frame with unknown SMAC is received.
• **Disable**	No learning is done.
• **Secure**	Only static MAC entries are learned, all other frames are dropped. **Note:** Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries. The MAC table is sorted first by VLAN ID and then by MAC address.

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **VLAN ID**	The VLAN ID of the entry.
• **MAC Address**	The MAC address of the entry.
• **Port Members**	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
• **Adding a New Static Entry**	Click [Add New Static Entry] to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save".

Buttons

[Apply]: Click to apply changes

[Reset]: Click to undo any changes made locally and revert to previously saved values.

4.3.14.2 MAC Address Table Status

Dynamic MAC Table

Entries in the MAC Table are shown on this page. The MAC Table contains up to **8192** entries, and is sorted first by VLAN ID, then by MAC address. The MAC Address Table screen in Figure 4-3-71 appears.

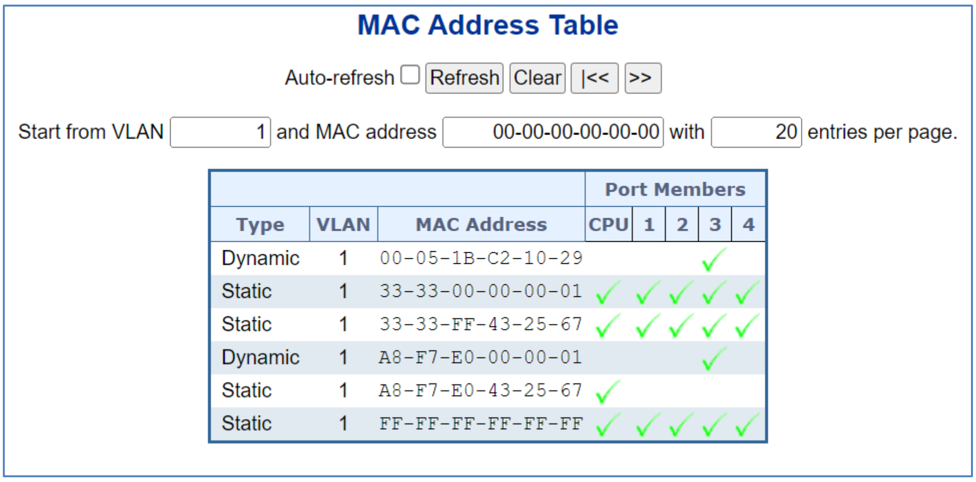


Figure 4-3-71: MAC Address Table Status Page Screenshot

Navigating the MAC Table

Each page shows up to 999 entries from the MAC table, default being 20, selected through the "**entries per page"** input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The "**Start from MAC address**" and "**VLAN**" input fields allow the user to select the starting point in the MAC Table. Clicking the "**Refresh**" button will update the displayed table starting from that or the closest next MAC Table match.

In addition, the two input fields will - upon a "**Refresh**" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The "**>>**" will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached the text "no more entries" is shown in the displayed table. Use the "**|<<**" button to start over.

The page includes the following fields:

Object	Description
• **Type**	Indicates whether the entry is a static or dynamic entry.
• **VLAN**	The VLAN ID of the entry.
• **MAC Address**	The MAC address of the entry.
• **Port Members**	The ports that are members of the entry.

Buttons

Auto-refresh ☐: Automatic refresh occurs every 3 seconds.

Refresh: Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.

Clear: Flushes all dynamic entries.

|<<: Updates the table starting from the first entry in the MAC Table, i.e. the entry with the lowest VLAN ID and MAC address.

>>: Updates the table, starting with the entry after the last entry currently displayed.

4.3.15 Loop Protection

This chapter describes enabling loop protection function that provides loop protection to prevent broadcast loops in **Industrial Managed TSN Device**.

4.3.15.1 Configuration

This page allows the user to inspect the current Loop Protection configurations, and possibly change them as well as screen in Figure 4-3-72 appears.

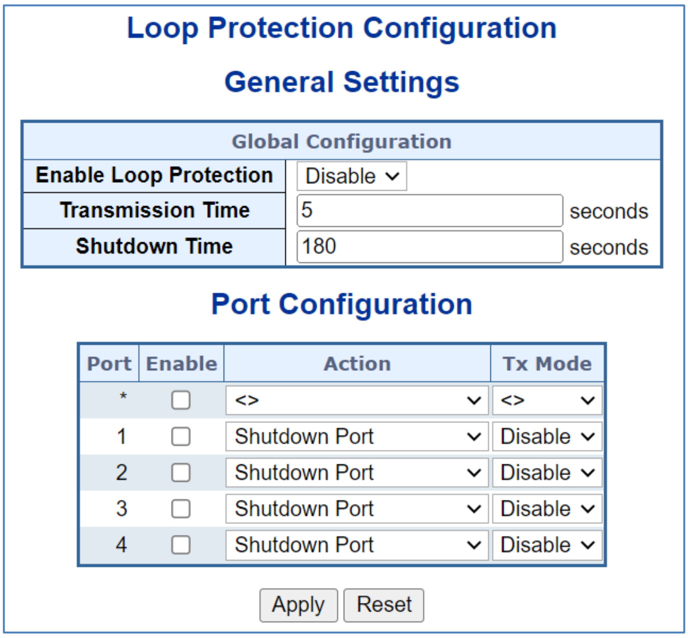


Figure 4-3-72: Loop Protection Configuration Page Screenshot

The page includes the following fields:

General Settings

Object	Description
• **Enable Loop Protection**	Controls whether loop protection is enabled (as a whole).

Port Configuration

Object	Description
• **Port**	The switch port number of the port.
• **Enable**	Controls whether loop protection is enabled on this switch port.
• **Action**	Configures the action performed when a loop is detected on a port. Valid values are **Shutdown Port**, **Shutdown Port and Log** or **Log Only**.
• **Tx Mode**	Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

Buttons

: Click to apply changes

: Click to undo any changes made locally and revert to previously saved values.

4.3.15.2 Status

This page displays the loop protection port status of the switch; screen in Figure 4-3-73 appears.

Figure 4-3-73: Loop Protection Status Screenshot

The page includes the following fields:

Object	Description
• **Port**	The **Industrial Managed TSN Device** port number of the logical port.
• **Action**	The currently configured port action.
• **Transmit**	The currently configured port transmit mode.
• **Loops**	The number of loops detected on this port.
• **Status**	The current loop protection status of the port.
• **Loop**	Whether a loop is currently detected on the port.
• **Time of Last Loop**	The time of the last loop event detected.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh ☐: Check this box to enable an automatic refresh of the page at regular intervals.

4.3.16 UDLD

Unidirectional Link Detection (UDLD) is a data link layer protocol from Cisco Systems to monitor the physical configuration of the cables and detect unidirectional links. UDLD complements the Spanning Tree Protocol which is used to eliminate switching loops.

4.3.16.1 UDLD Port Configuration

This page allows the user to inspect the current UDLDconfigurations, and possibly change them as well. as screen in Figure 4-3-74 appears.

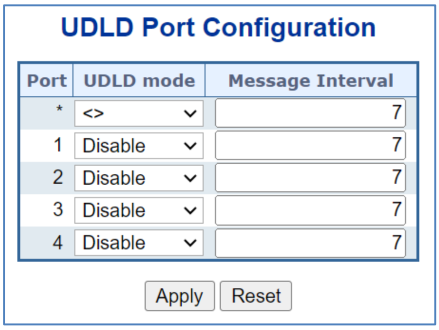


Figure 4-3-74: UDLD Configuration Page Screenshot

The page includes the following fields:

General Settings

Object	Description
• **Port**	Port number of the switch.
• **UDLD Mode**	Configures the UDLD mode on a port. Valid values are **Disable**, **Normal** and **Aggressive**. Default mode is Disable. **Disable**: In disabled mode, UDLD functionality doesn't exists on port.. **Normal:** In normal mode, if the link state of the port was determined to be unidirectional, it will not affect the port state. **Aggressive:** In aggressive mode, unidirectional detected ports will get shutdown. To bring back the ports up, need to disable UDLDon that port
• **Message Interval**	Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is from 7 to 90 seconds(Default value is 7 seconds)(Currently default time interval is supported, due to lack of detailed information in RFC 5171).

Buttons

: Click to apply changes

: Click to undo any changes made locally and revert to previously saved values.

4.3.16.2 UDLD Status

This page displays the UDLD status of the ports as well. as screen in Figure 4-3-75 appears.

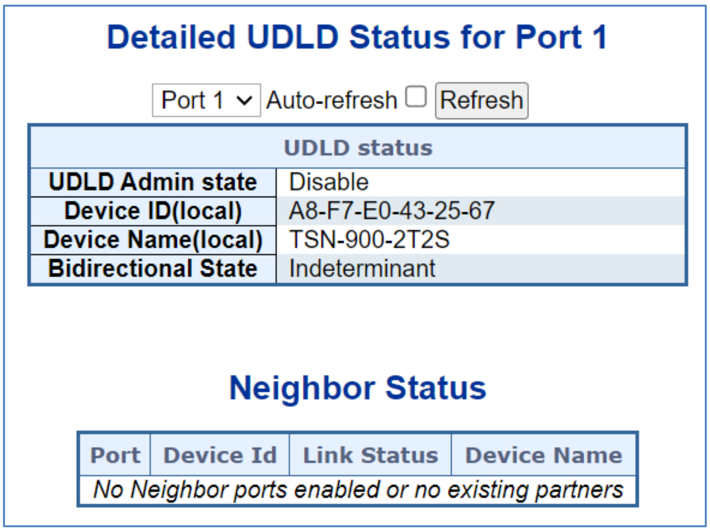


Figure 4-3-75: UDLD status Page Screenshot

The page includes the following fields:

UDLD port status

Object	Description
• **UDLD Admin State**	The current port state of the logical port, Enabled if any of state(Normal,Aggressive) is Enabled.
• **Device ID(local)**	The ID of Device
• **Device Name(local)**	Name of the Device.
• **Bidirectional State**	The current state of the port.

Neighbour Status

Object	Description
• **Port**	The current port of neighbour device
• **Device ID**	The current ID of neighbour device.
• **Link Status**	The current link status of neighbour port.
• **Device Name**	Name of the Neighbour Device.

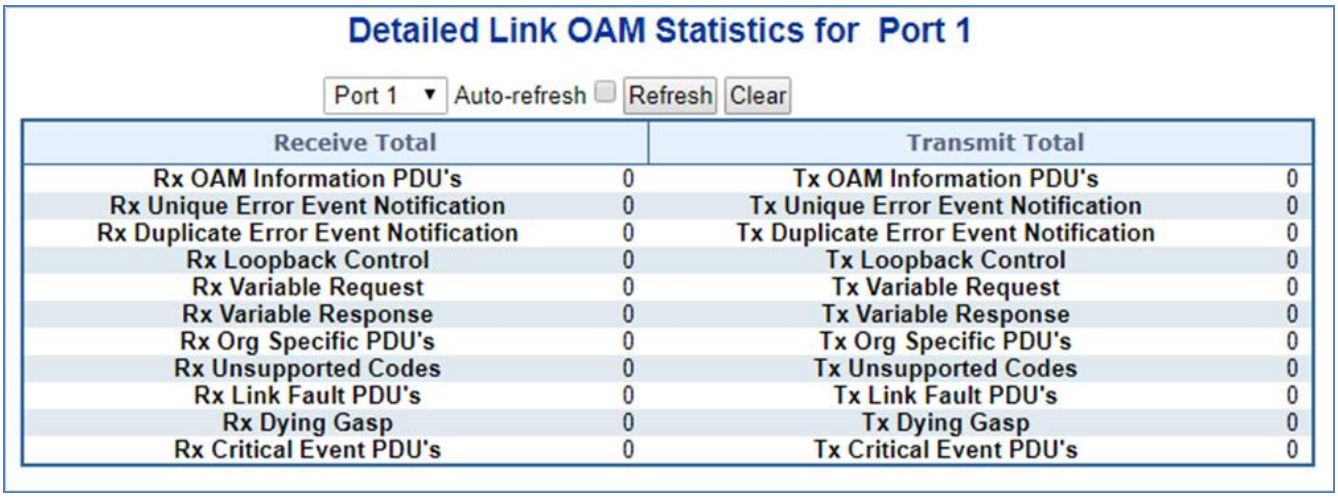
Buttons

Refresh: Click to refresh the page immediately..

4.3.17 Link OAM

4.3.17.1 Statistics

This page provides detailed OAM traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.The displayed counters represent the total number of OAM frames received and transmitted for the selected port. Discontinuities of these counter can occur at re-initialization of the management system. as screen in Figure 4-3-76 appears.


Detailed Link OAM Statistics for Port 1

Port 1 Auto-refresh Refresh Clear

Receive Total		Transmit Total	
Rx OAM Information PDU's	0	Tx OAM Information PDU's	0
Rx Unique Error Event Notification	0	Tx Unique Error Event Notification	0
Rx Duplicate Error Event Notification	0	Tx Duplicate Error Event Notification	0
Rx Loopback Control	0	Tx Loopback Control	0
Rx Variable Request	0	Tx Variable Request	0
Rx Variable Response	0	Tx Variable Response	0
Rx Org Specific PDU's	0	Tx Org Specific PDU's	0
Rx Unsupported Codes	0	Tx Unsupported Codes	0
Rx Link Fault PDU's	0	Tx Link Fault PDU's	0
Rx Dying Gasp	0	Tx Dying Gasp	0
Rx Critical Event PDU's	0	Tx Critical Event PDU's	0

Figure 4-3-76: Link OAM Statistic Page Screenshot

The page includes the following fields:

General Settings

Object	Description
• **Rx and Tx OAM Information PDU's**	The number of received and transmitted OAM Information PDU's. Discontinuities of this counter can occur at re-initialization of the management system.
• **Rx and Tx Unique Error Event Notification**	A count of the number of unique Event OAMPDUs received and transmitted on this interface. Event Notifications may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. Duplicate Event Notification transmissions are counted by Duplicate Event Notification counters for Tx and Rx respectively. A unique Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is distinct from the previously transmitted Event Notification OAMPDU Sequence Number.
• **Rx and Tx Duplicate Error Event Notification**	A count of the number of duplicate Event OAMPDUs received and transmitted on this interface. Event Notification OAMPDUs may be sent in duplicate to increase the probability of successfully being received, given the possibility that

	a frame may be lost in transit. A duplicate Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is identical to the previously transmitted Event Notification OAMPDU Sequence Number.
• **Rx and Tx Loopback Control**	A count of the number of Loopback Control OAMPDUs received and transmitted on this interface.
• **Rx and Tx Variable Request**	A count of the number of Variable Request OAMPDUs received and transmitted on this interface.
• **Rx and Tx Variable Response**	A count of the number of Variable Response OAMPDUs received and transmitted on this interface.
• **Rx and Tx Org Specific PDU's**	A count of the number of Organization Specific OAMPDUs transmitted on this interface.
• **Rx and Tx Unsupported Codes**	A count of the number of OAMPDUs transmitted on this interface with an unsupported op-code.
• **Rx and Tx Link fault PDU's**	A count of the number of Link fault PDU's received and transmitted on this interface.
• **Rx and Tx Dying Gasp**	A count of the number of Dying Gasp events received and transmitted on this interface.
• **Rx and Tx Critical Event PDU's**	A count of the number of Critical event PDU's received and transmitted on this interface.

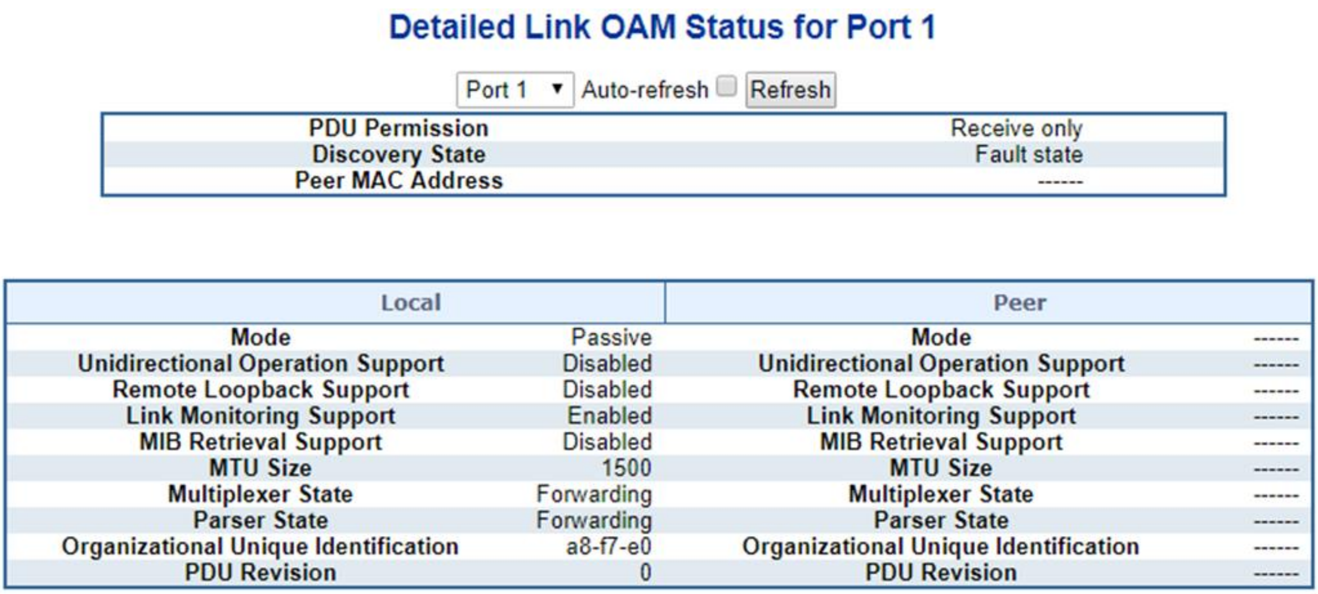
Buttons

: Click to refresh the page immediately.

: Clears the counters for the selected port.

4.3.17.2 Port Status

This page provides Link OAM configuration operational status. The displayed fields shows the active configuration status for the selected port. as well. as screen in Figure 4-3-77 appears.



Detailed Link OAM Status for Port 1

Port 1 ▾ Auto-refresh ☐ Refresh

PDU Permission	Receive only
Discovery State	Fault state
Peer MAC Address	------

Local		Peer	
Mode	Passive	Mode	------
Unidirectional Operation Support	Disabled	Unidirectional Operation Support	------
Remote Loopback Support	Disabled	Remote Loopback Support	------
Link Monitoring Support	Enabled	Link Monitoring Support	------
MIB Retrieval Support	Disabled	MIB Retrieval Support	------
MTU Size	1500	MTU Size	------
Multiplexer State	Forwarding	Multiplexer State	------
Parser State	Forwarding	Parser State	------
Organizational Unique Identification	a8-f7-e0	Organizational Unique Identification	------
PDU Revision	0	PDU Revision	------

Figure 4-3-77: Port Status Page Screenshot

The page includes the following fields:

General Settings

Object	Description
• **PDU Permission**	This field is available only for the Local DTE. It displays the current permission rules set for the local DTE. Possible values are ■ **Link fault** ■ **Receive only** ■ **Information exchange only** ■ **ANY**
• **Discovery State**	Displays the current state of the discovery process. Possible states are ■ **Fault state** ■ **Active state** ■ **Passive state** ■ **SEND_LOCAL_REMOTE_STATE** ■ **SEND_LOCAL_REMOTE_OK_STATE** ■ **SEND_ANY_STATE**
• **Mode**	The Mode in which the Link OAM is operating, Active or Passive.

• **Unidirectional Operation Support**	This feature is not available to be configured by the user. The status of this configuration is retrieved from the PHY.
• **Remote Loopback Support**	If status is enabled, DTE is capable of OAM remote loopback mode.
• **Link Monitoring Support**	If status is enabled, DTE supports interpreting Link Events.
• **MIB Retrieval Support**	If status ie enabled DTE supports sending Variable Response OAMPDUs.
• **MTU Size**	It represents the largest OAMPDU, in octets, supported by the DTE. This value is compared to the remotes Maximum PDU Size and the smaller of the two is used.
• **Multiplexer State**	When in forwarding state, the Device is forwarding non-OAMPDUs to the lower sublayer. Incase of discarding, the device discards all the non-OAMPDU's.
• **Parser State**	When in **forwarding** state, Device is forwarding non-OAMPDUs to higher sublayer. When in **loopback**, Device is looping back non-OAMPDUs to the lower sublayer. When in **discarding** state, Device is discarding non-OAMPDUs.
• **Organizational Unique Identification**	24-bit Organizationally Unique Identifier of the vendor.
• **PDU Revision**	It indicates the current revision of the Information TLV. The value of this field shall start at zero and be incremented each time something in the Information TLV changes. Upon reception of an Information TLV from a peer, an OAM client may use this field to decide if it needs to be processed (an Information TLV that is identical to the previous Information TLV doesn't need to be parsed as nothing in it has changed).

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh ☐: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

4.3.17.3 Event Status

This page allows the user to inspect the current Link OAM Link Event configurations, and change them as well. as screen in Figure 4-3-78 appears.

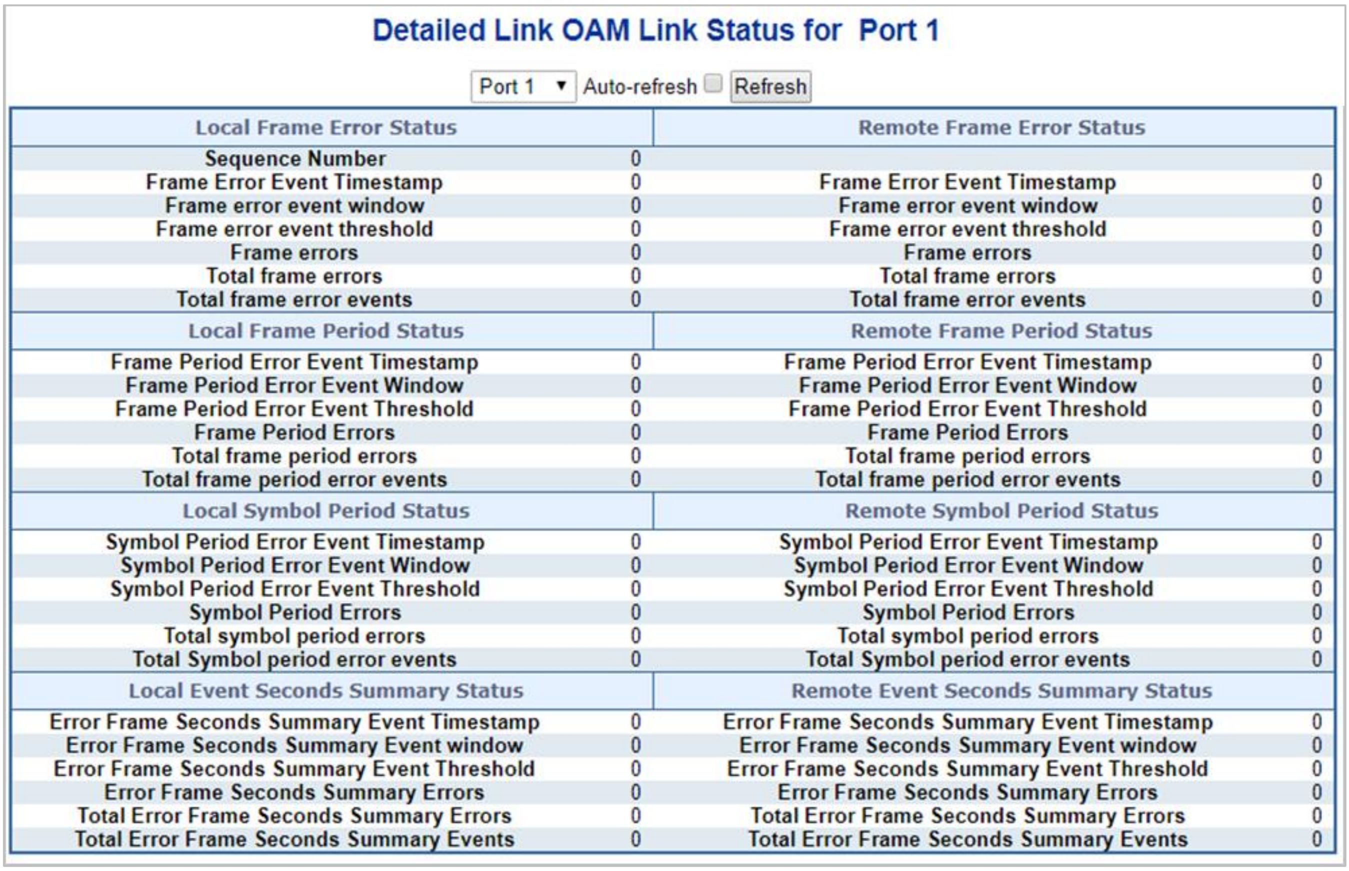


Figure 4-3-78: Link OAM Statistic Page Screenshot

The page includes the following fields:

General Settings

Object	Description
• **Port**	The switch port number.
• **Sequence Number**	This two-octet field indicates the total number of events occurred at the remote end.
• **Frame Error Event Timestamp**	This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.
• **Frame error event window**	This two-octet field indicates the duration of the period in terms of 100 ms intervals. 1) The default value is one second. 2) The lower bound is one second. 3) The upper bound is one minute.
• **Frame error event threshold**	This four-octet field indicates the number of detected errored frames in the period is required to be equal to or greater than in order for the event to be

	generated. 1) The default value is one frame error. 2) The lower bound is zero frame errors. 3) The upper bound is unspecified.
• **Frame errors**	This four-octet field indicates the number of detected errored frames in the period.
• **Total frame errors**	This eight-octet field indicates the sum of errored frames that have been detected since the OAM sublayer was reset.
• **Total frame error events**	This four-octet field indicates the number of Errored Frame Event TLVs that have been generated since the OAM sublayer was reset.
• **Frame Period Error Event Timestamp**	This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.
• **Frame Period Error Event Window**	This four-octet field indicates the duration of period in terms of frames.
• **Frame Period Error Event Threshold**	This four-octet field indicates the number of errored frames in the period is required to be equal to or greater than in order for the event to be generated.
• **Frame Period Errors**	This four-octet field indicates the number of frame errors in the period.
• **Total frame period errors**	This eight-octet field indicates the sum of frame errors that have been detected since the OAM sublayer was reset.
• **Total frame period error events**	This four-octet field indicates the number of Errored Frame Period Event TLVs that have been generated since the OAM sublayer was reset
• **Symbol Period Error Event Timestamp**	This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.
• **Symbol Period Error Event Window**	This eight-octet field indicates the number of symbols in the period.
• **Symbol Period Error Event Threshold**	This eight-octet field indicates the number of errored symbols in the period is required to be equal to or greater than in order for the event to be generated.
• **Symbol Period Errors**	This eight-octet field indicates the number of symbol errors in the period.
• **Total symbol period errors**	This eight-octet field indicates the sum of symbol errors since the OAM sublayer was reset.
• **Total Symbol period error events**	This four-octet field indicates the number of Errored Symbol Period Event TLVs that have been generated since the OAM sublayer was reset.
• **Error Frame Seconds Summary Event Timestamp**	This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.
• **Error Frame Seconds Summary Event window**	This two-octet field indicates the duration of the period in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.
• **Error Frame Seconds Summary Event Threshold**	This two-octet field indicates the number of errored frame seconds in the period is required to be equal to or greater than in order for the event to be generated, encoded as a 16-bit unsigned integer.

• **Error Frame Seconds Summary Errors**	This two-octet field indicates the number of errored frame seconds in the period, encoded as a 16-bit unsigned integer.
• **Total Error Frame Seconds Summary Errors**	This four-octet field indicates the sum of errored frame seconds that have been detected since the OAM sublayer was reset.
• **Total Error Frame Seconds Summary Events**	This four-octet field indicates the number of Errored Frame Seconds Summary Event TLVs that have been generated since the OAM sublayer was reset, encoded as a 32bit unsigned integer.

Buttons

Refresh: Click to refresh the page.

Clear: Click to clear the data.

4.3.17.4 Port Settings

This page allows the user to inspect the current Link OAM port configurations, and change them as well, as screen in Figure 4-3-79 appears.

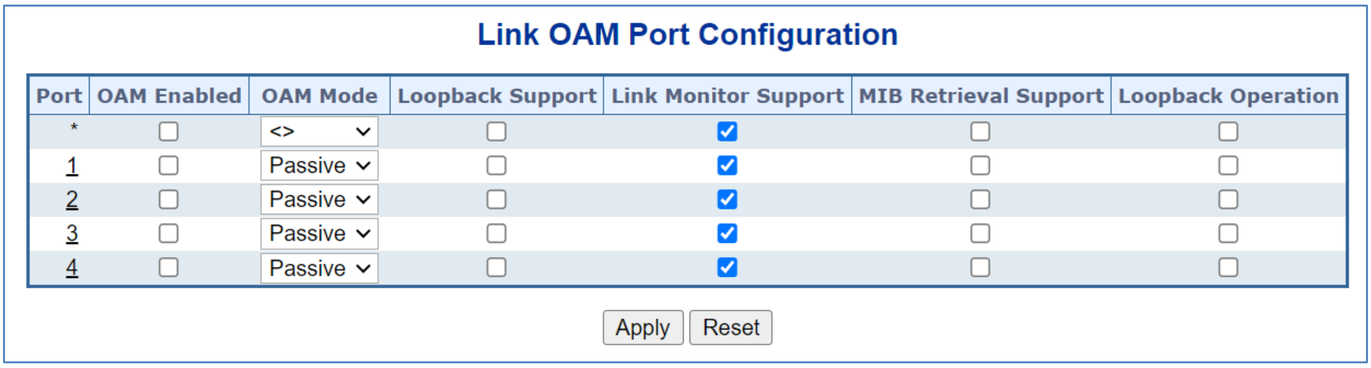


Figure 4-3-79: Port Status Page Screenshot

The page includes the following fields:

General Settings

Object	Description
• **Port**	The switch port number.
• **OAM Enabled**	Controls whether Link OAM is enabled on this switch port. Enabling Link OAM provides the network operators the ability to monitor the health of the network and quickly determine the location of failing links or fault conditions.
• **OAM Mode**	Configures the OAM Mode as Active or Passive. The default mode is Passive. ■ **Active mode** DTE's configured in Active mode initiate the exchange of Information OAMPDUs as defined by the Discovery process. Once the Discovery process completes, Active DTE's are permitted to send any OAMPDU while connected to a remote OAM peer entity in Active mode. Active DTE's operate in a limited respect if the remote OAM entity is operating in Passive mode. Active devices should not respond to OAM remote loopback commands and variable requests from a Passive peer. ■ **Passive mode** DTE's configured in Passive mode do not initiate the Discovery process. Passive DTE's react to the initiation of the Discovery process by the remote DTE. This eliminates the possibility of passive to passive links. Passive DTE's shall not send Variable Request or Loopback Control OAMPDUs.
• **Loopback Support**	Controls whether the loopback support is enabled for the switch port. Link OAM remote loopback can be used for fault localization and link performance testing. Enabling the loopback support will allow the DTE to execute the remote loopback command that helps in the fault detection.

• **Link Monitor Support**	Controls whether the Link Monitor support is enabled for the switch port. On enabling the Link Monitor support, the DTE supports event notification that permits the inclusion of diagnostic information.
• **MIB Retrieval Support**	Controls whether the MIB Retrieval Support is enabled for the switch port. On enabling the MIB retrieval support, the DTE supports polling of various Link OAM based MIB variables' contents.
• **Loopback Operation**	If the Loopback support is enabled, enabling this field will start a loopback operation for the port.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.17.5 Event Settings

This page allows the user to inspect the current Link OAM Link Event configurations, and change them as well, as screen in Figure 4-3-80 appears.

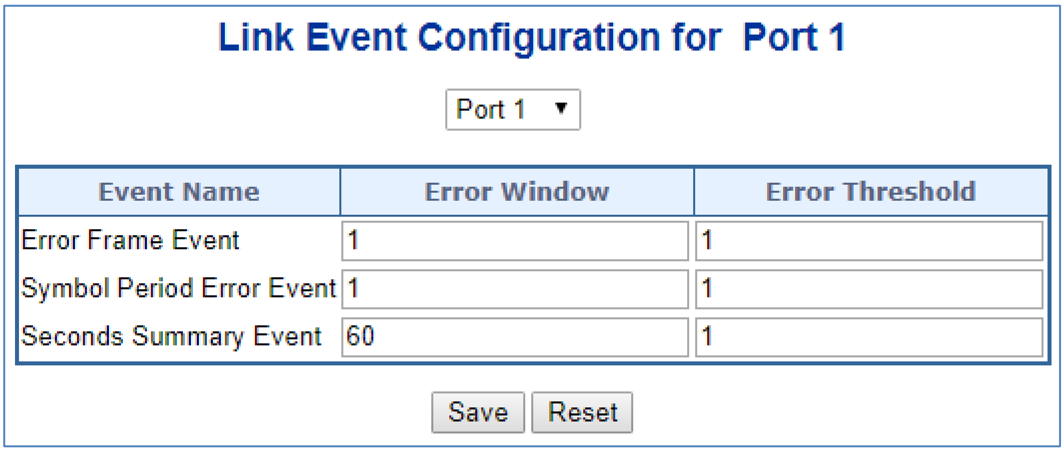


Figure 4-3-80: Event Settings Page Screenshot

The page includes the following fields:

General Settings

Object	Description
• **Port**	The switch port number.
• **Event Name**	Name of the Link Event which is being configured.
• **Error Window**	Represents the window period in the order of 1 sec for the observation of various link events.
• **Error Threshold**	Represents the threshold value for the window period for the appropriate Link event so as to notify the peer of this error.
• **Error Frame Event**	The Errored Frame Event counts the number of errored frames detected during the specified period. The period is specified by a time interval (Window in order of 1 sec). This event is generated if the errored frame count is equal to or greater than the specified threshold for that period (Period Threshold). Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Error Frame Event' must be an integer value between 1-60 and its default value is '1'. Whereas Error Threshold must be between 0-4294967295 and its default value is '1'.
• **Symbol Period Error Event**	ved in a time interval on the underlying physical layer. This event is generated if the symbol error count is equal to or greater than the specified threshold for that period. Error Window for 'Symbol Period Error Event' must be an integer value between 1-60 and its default value is '1'. Whereas Error Threshold must be between 0-4294967295 and its default value is '1'.

• **Seconds Summary Event**	The Errored Frame Seconds Summary Event TLV counts the number of errored frame seconds that occurred during the specified period. The period is specified by a time interval. This event is generated if the number of errored frame seconds is equal to or greater than the specified threshold for that period. An errored frame second is a one second interval wherein at least one frame error was detected. Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Seconds Summary Event' must be an integer value between 10-900 and its default value is '60'. Whereas Error Threshold must be between 0-65535 and its default value is '1'.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.17.6 MIB Retrieval

This page allows you to configure Link OAM MIB Retrieval, as screen in Figure 4-3-81 appears.

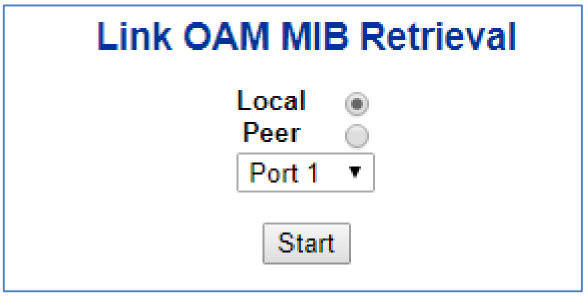


Figure 4-3-81: MIB Retrieval Page Screenshot

4.3.17.7 Link-OAM Example

CE and PE devices with point-to-point link enable EFM OAM to monitor "the First Mile" link performance. It will report the log information to network management system when occurring fault event and use remote loopback function to detect the link in necessary instance

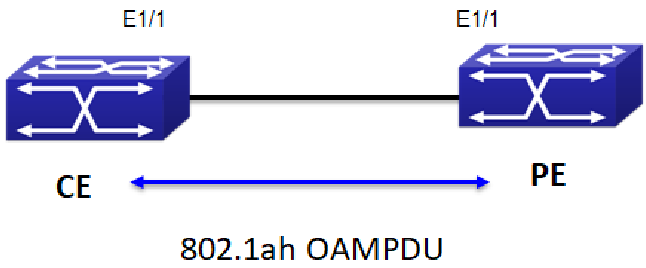


Figure 4-3-82: Typical OAM application topology

The configuration of link-oam is quite simple.

Step 1. Set CE as Passive OAM mode

Link OAM Port Configuration

Port	OAM Enabled	OAM Mode	Loopback Support	Link Monitor Support	MIB Retrieval Support	Loopback Operation
*	☐	<All>	☐	☐	☐	☐
1	☑	Passive	☐	☑	☐	☐

Step 2. Set PE as Active OAM mode

Link OAM Port Configuration

Port	OAM Enabled	OAM Mode	Loopback Support	Link Monitor Support	MIB Retrieval Support	Loopback Operation
*	☐	<All>	☐	☐	☐	☐
1	☑	Active	☐	☑	☐	☐

Step 3. Check OAM status and statistic from CE device

Detailed Link OAM Status for Port 1

Port 1 Auto-refresh ☑ Refresh

PDU Permission	Any
Discovery State	SEND_ANY_STATE
Peer MAC Address	00:30:4f:11:22:55

Local		Peer	
Mode	Passive	Mode	Active
Unidirectional Operation Support	Disabled	Unidirectional Operation Support	Disabled
Remote Loopback Support	Disabled	Remote Loopback Support	Disabled
Link Monitoring Support	Enabled	Link Monitoring Support	Enabled
MIB Retrieval Support	Disabled	MIB Retrieval Support	Disabled
MTU Size	1500	MTU Size	1500
Multiplexer State	Forwarding	Multiplexer State	Forwarding
Parser State	Forwarding	Parser State	Forwarding
Organizational Unique Identification	00-30-4f	Organizational Unique Identification	00-30-4f
PDU Revision	1	PDU Revision	0

Detailed Link OAM Statistics for Port 1

Port 1 Auto-refresh ☐ Refresh Clear

Receive Total		Transmit Total	
Rx OAM Information PDU's	232	Tx OAM Information PDU's	232

4.3.18 CFM

4.3.18.1 Global Configuration

CFM stands for Connectivity Fault Management. It is a protocol used in network switches to detect connectivity issues and faults in the network. It can detect faults such as link failures, and it can also locate the source of the fault. This page allows you to configure CFM Global parameters, as screen in Figure 4-3-83 appears. on this page.

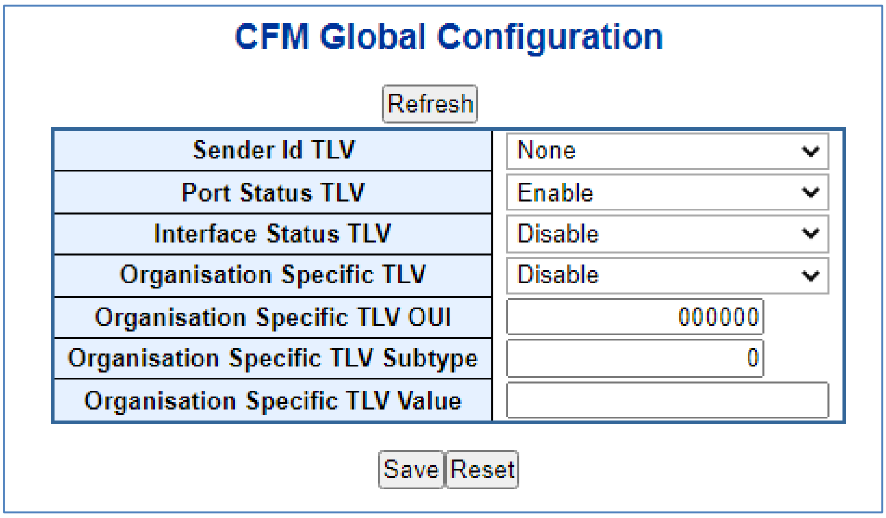


Figure 4-3-83: CFM Global Configuration Page Screenshot

The displayed settings are:

Object	Description
• **Sender Id TLV**	Choose whether and what to use as Sender ID TLVs in CCMs generated by this switch. Can be overridden by Domain and Service level configuration. None Chassis Manage ChassisManage
• **Port Status TLV**	Choose whether to send Port Status TLVs in CCMs generated by this switch. Can be overridden by Domain and Service level configuration. Enable Send Port Status TLVs in CCMs generated by this switch. Disable Do not send Port Status TLVs in CCMs generated by this switch.
• **Interface Status TLV**	Choose whether to send Interface Status TLVs in CCMs generated by this switch. Can be overridden by Domain and Service level configuration. Enable Send Interface Status TLVs in CCMs generated by this switch. Disable Do not Send Interface Status TLVs in CCMs generated by this switch.
• **Organisation Specific TLV**	Choose whether to send Organisation Specific TLVs in CCMs generated by this switch. Can be overridden by Domain and Service level configuration. Enable Send Organisation Specific TLVs in CCMs generated by this switch. Disable Do not send Organisation Specific TLVs in CCMs generated by this

	switch.
• **Organisation Specific TLV OUI**	This is the three-bytes OUI transmitted with the Organization-Specific TLVs. Enter as 6 characters 0-9, a-f.
• **Organisation Specific TLV Subtype**	This is the subtype transmitted with the Organization-Specific TLV. Can be any value in range [0; 255]
• **Organisation Specific TLV Value**	This is the value transmitted in the Organization-Specific TLVs. Value is a printable character string of length 0-63.
• **Default**	To set the switch port to use the default VL

Buttons

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.18.2 Port Status

Configure CFM Domain parameters on this page.

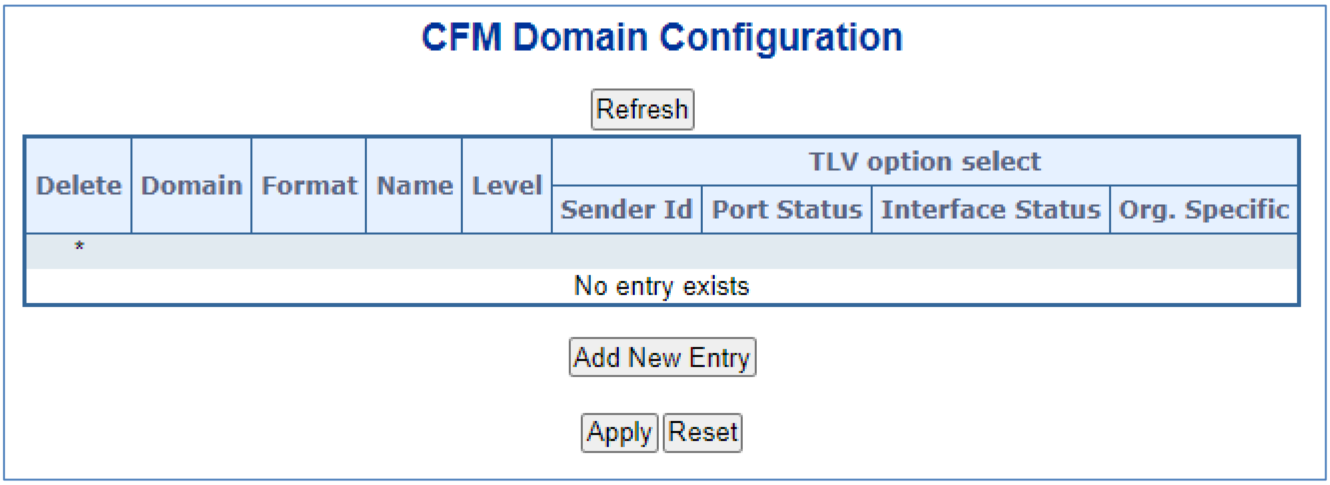


Figure 4-3-84: CFM Domain Configuration

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Domain**	Name of Domain. Value is a single word which begins with an alphabetic letter A-Z or a-z with length 1-15.
• **Format**	Select the MD name format. To mimic Y.1731 MEG IDs, use type None. **None** **String**
• **Name**	The contents of this pamameter depends on the value of the format member. If format is **None**: Name is not used, but will be set to all-zeros behind the scenes. This format is typically used by Y.1731-kind-of-PDUs. If format is **String**: Name must contain a string from 1 to 43 characters long.
• **Level**	MD/MEG level of this domain. Valid values are restricted to 0 - 7. **About leak prevention** Leak prevention is about discarding OAM PDUs with MEG levels lower than the MEP they hit when the OAM PDUs are ingressing the port on which the MEP resides, and to discard OAM PDUs with MEG levels at or lower than the MEP's when the OAM PDUs are ingressing other ports. There are two categories of architectures, when it comes to leak-prevention: Those that use Shared MEG level and those that use Independent MEG level: **Shared MEG level** On Shared MEG level architectures, Port Down MEPs always perform level filtering no matter which VLAN ID (VID) OAM PDUs get classified to, unless the same port has a VLAN MEP on the VID in question. So if you have a Port MEP

	in VID X and a VLAN MEP in VID Y, an OAM frame arriving on the port and gets classified to VID X or VID Z will be handled/level-filtered by the Port MEP, whereas an OAM frame ingressing the port in VID Y will be handled by the VLAN MEP. Likewise, if the switch has a Port MEP on VID X on Port X and an OAM frame ingresses on VID Y on Port Y, it is subject to level filtering before egressing Port X, unless Port X also has a VLAN MEP on VID Y, in which case the VLAN MEP will take care of level-filtering the OAM PDU. On Shared MEG level architectures, all Port MEPs must have the same MEG level and any VLAN MEP must have a MEG level higher than the Port MEPs' MEG level. **Independent MEG level** On Independent MEG level architectures, Port Down MEPs never perform level filtering on frames not classified to the MEP's VID. So if you have a Port MEP on VID X and a VLAN MEP on VID Y and an OAM frame ingresses any port on VID Z, it is not subject to handling/level-filtering by any of the two MEPs. **This switch exhibits Independent MEG level.**
• **TLV option select**	**Sender Id**: Default Sender ID TLV format to be used in CCMs generated by this Domain (may be overridden in service) **None** Do not include Sender ID TLVs. **Chassis** Enable Sender ID TLV and send Chassis ID (MAC Address). **Manage** Enable Sender ID TLV and send Management address (IPv4 Address). **ChassisManage** Enable Sender ID TLV and send both Chassis ID (MAC Address) and Management Address (IPv4 Address). **Defer** Let the global configuration decide if Sender ID TLVs shall be included (may be overridden in service). **Port Status**: Include or exclude Port Status TLV in CCMs generated by this Domain or let higher level determine (may be overridden in Service). **Disable** Do not include Port Status TLVs. **Enable** Include Port Status TLVs. **Defer** Let the global configuration decide if Port Status TLVs shall be included (may be overridden in Service). **Interface Status**: Include or exclude Interface Status TLV in CCMs generated by this Domain or let higher level determine (may be overridden in Service).

	Disable Do not include Interface Status TLVs. **Enable** Include Interface Status TLVs. **Defer** Let the global configuration decide if Interface Status TLVs shall be included (may be overridden in Service). **Org. Specific**: Exclude Organization-Specific TLV in CCMs generated by this Domain or let higher level determine (may be overridden in Service). **Disable** Do not include Organization-Specific TLVs. **Defer** Let the global configuration decide if Organization-Specific TLVs shall be included (may be overridden in Service).

Buttons

Add New Entry: Click to add Flow Meter entry.

Apply: Click to apply changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.18.3 Service

Configure CFM Service parameters on this page.

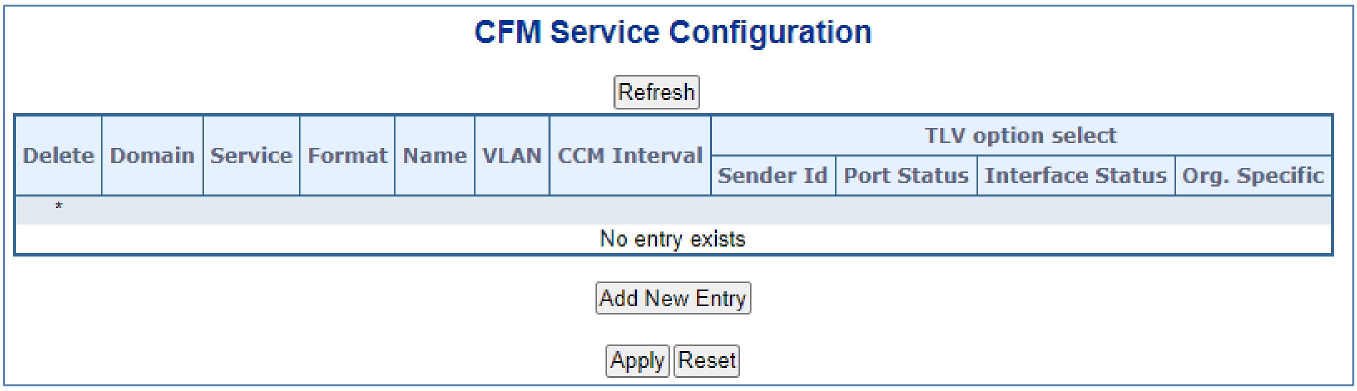


Figure 4-3-85: CFM Service Configuration

Configure CFM Service parameters on this page.

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Domain**	Name of Domain under which this Service resides.
• **Service**	Name of Service. Value is a single word which begins with an alphabetic letter A-Z or a-z with length 1-15.
• **Format**	Select the short Service name format. This decides how the value of the Name parameter will be interpreted. To mimic Y.1731 MEG IDs, create an MD instance with an empty name and use **Y1731 ICC** or **Y1731 ICC CC**. Possible values are: **String** **Two Octets** **Y1731 ICC** **Y1731 ICC CC** Look under **Name** for explanation.
• **Name**	The contents of this parameter depends on the value of the format member. Besides the limitations explained for each of them, the following applies in general: If the Domain **Format** is **None**, the size of this cannot exceed 45 bytes. If the Domain **Format** is not **None**, the size of this cannot exceed 44 bytes. If **Format** is **String**, the following applies: length must be in range [1; 44] Contents must be in range [32; 126] If **Format** is **Two Octets**, the following applies: **Name[0]** and **Name[1]** will both be interpreted as unsigned 8-bit integers (allowing a range of [0;

	255]). **Name[0]** will be placed in the PDU before **Name[1]**. The remaining available bytes in name will not be used. If **Format** is **Y1731 ICC**, the following applies: length must be 13. Contents must be in range [a-z,A-Z,0-9] Y.1731 specifies that it is a concatenation of ICC (ITU Carrier Code) and UMC (Unique MEG ID Code): ICC: 1-6 bytes UMC: 7-12 bytes In principle UMC can be any value in range [1; 127], but this API does not allow for specifying length of ICC, so the underlying code doesn't know where ICC ends and UMC starts. The Domain **Format** must be **None**. If **Format** is **Y1731 ICC CC**, the following applies: length must be 15. First 2 chars (CC): Must be amongst [A-Z] Next 1-6 chars (ICC): Must be amongst [a-z,A-Z,0-9] Next 7-12 chars (UMC): Must be amongst [a-z,A-Z,0-9] There may be ONE (slash) present in name[3-7]. The Domain **format** must be **None**.
• **VLAN**	The MA's primary VID. A primary VID of 0 means that all MEPs created within this MA will be created as port MEPs (interface MEPs). There can only be one port MEP per interface. A given port MEP may still be created with tags, if that MEP's VLAN is non-zero." A non-zero primary VID means that all MEPs created within this MA will be created as VLAN MEPs. A given MEP may be configured with another VLAN than the MA's primary VID, but it is impossible to have untagged VLAN MEPs.
• **CCM Interval**	The CCM rate of all MEPs bound to this Service.
• **TLV Option Select**	**Sender Id**: Default Sender ID TLV format to be used in CCMs generated by this Service. **None** Do not include Sender ID TLVs. **Chassis** Enable Sender ID TLV and send Chassis ID (MAC Address). **Manage** Enable Sender ID TLV and send Management address (IPv4 Address). **ChassisManage** Enable Sender ID TLV and send both Chassis ID (MAC Address) and Management Address (IPv4 Address). **Defer** Let the Domain configuration decide if Sender ID TLVs shall be included. **Port Status**: Include or exclude Port Status TLV in CCMs generated by this Service or let higher level determine.

	Disable Do not include Port Status TLVs. **Enable** Include Port Status TLVs. **Defer** Let the Domain configuration decide if Port Status TLVs shall be included. **Interface Status**: Include or exclude Interface Status TLV in CCMs generated by this Service or let higher level determine. **Disable** Do not include Interface Status TLVs. **Enable** Include Interface Status TLVs. **Defer** Let the Domain configuration decide if Interface Status TLVs shall be included. **Org. Specific**: Exclude Organization-Specific TLV in CCMs generated by this Service or let higher level determine. **Disable** Do not include Organization-Specific TLVs. **Defer** Let the Domain configuration decide if Organization-Specific TLVs shall be included.

Buttons

Add New Entry : Click to add Flow Meter entry.

Apply : Click to apply changes.

Reset : Click to undo any changes made locally and revert to previously saved values.

4.3.18.4 MEP

This switch supports two types of MEP: Port Down-MEPs and VLAN Down-MEPs.

Port Down-MEPs

In 802.1Q terminology, Port MEPs are located below the EISS entity, that is, closest to the physical port. Port MEPs are used by e.g. APS for protection purposes.

Port MEPs are created when the encompassing service has type "Port".

Port MEPs may send OAM PDUs tagged or untagged. An OAM PDU will be sent untagged only if the MEP's VLAN is set to "Inherit" (0). Any other value will cause it to be sent tagged with the port's TPID, whether or not the VLAN matches the port's PVID and that PVID is meant to be sent untagged.

VLAN Down-MEPs

in 802.1Q terminology, VLAN MEPs are located above the EISS entity.

This means that tagging of OAM PDUs will follow the port's VLAN configuration.

Thus, if a VLAN MEP is created on the Port's PVID and PVID is configured to be untagged, OAM PDUs will be transmitted untagged.

VLAN MEPs are created when the encompassing service has type "VLAN".

Down-MEP creation rules

There are a few rules to obey when creating Down-MEPs:

1. There can only be one Port MEP on the same port.
2. There can only be one VLAN MEP on the same port and VLAN.
3. A VLAN MEP must have a higher MD/MEG level than a Port MEP on the same port and VLAN.

These checks are performed automatically on administratively enabled MEPs when you change a particular MEP, change the Service Type from Port to VLAN or vice versa, or change the domain's MD/MEG level.

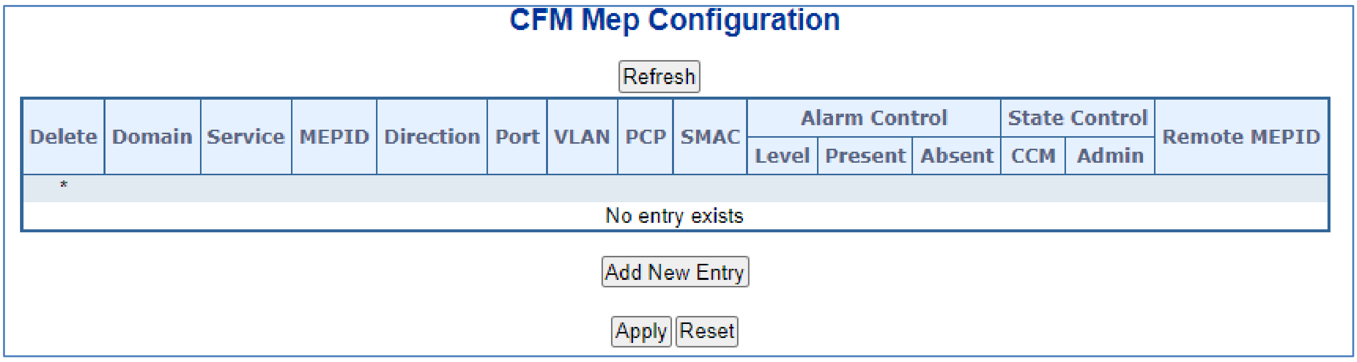


Figure 4-3-86: CFM MEP Configuration

The following explains the settings when configuring the MEP.

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Domain**	Name of Domain under which this Service resides.
• **Name**	Name of Service under which this MEP resides.
• **MEPID**	The identification of this MEP. Must be an integer [1..8091]
• **Direction**	Set whether this MEP is an Up- or a Down-MEP.
• **Port**	Port on which this MEP resides.
• **VLAN**	VLAN ID. Use the value 0 to indicate untagged traffic (implies a port MEP)..
• **PCP**	Choose PCP value in PDUs' VLAN tag. Not used if untagged.
• **SMAC**	Set a Source MAC address to be used in CCM PDUs originating at this MEP. Must be a unicast address. Format is XX:XX:XX:XX:XX:XX. If all-zeros, the switch port's MAC address will be used instead.
• **Alarm Control**	**Level:** If a defect is detected with a priority higher than this level, a fault alarm notification will be generated. Valid range is [1; 6] with 1 indicating that any defect will cause a fault alarm and 6 indicating that no defect can cause a fault alarm. See 802.1Q-2018, clause 20.9.5, LowestAlarmPri The possible defects and their priorities are: Short name / Description / Priority DefRDICCM / Remote Defect Indication / 1 DefMACstatus / MAC Status / 2 DefRemoteCCM / Remote CCM / 3 DefErrorCCM / Error CCM Received / 4 DefXconCCM / Cross Connect CCM Received / 5 **Present:** The time in milliseconds that defects must be present before a fault alarm notification is issued. Default is 2500 ms. **Absent:** The time in milliseconds that defects must be absent before a fault alarm notification is reset. Default is 10000 ms.
• **State Control**	**CCM:** Enable or disable generation of continuity-check messages (CCMs) **Admin:** Enable or disable this MEP. When this MEP is enabled, it will check received/missing CCMs and can raise defects.
• **Remote MEPID**	Specify the Remote MEP that this MEP is expected to receive CCM PDUs from. Must be an integer [0..8091] where 0 means undefined. The value of Remote MEPID must be different from the value of MEPID.

4.3.18.5 Status

Monitor CFM Status on this page.

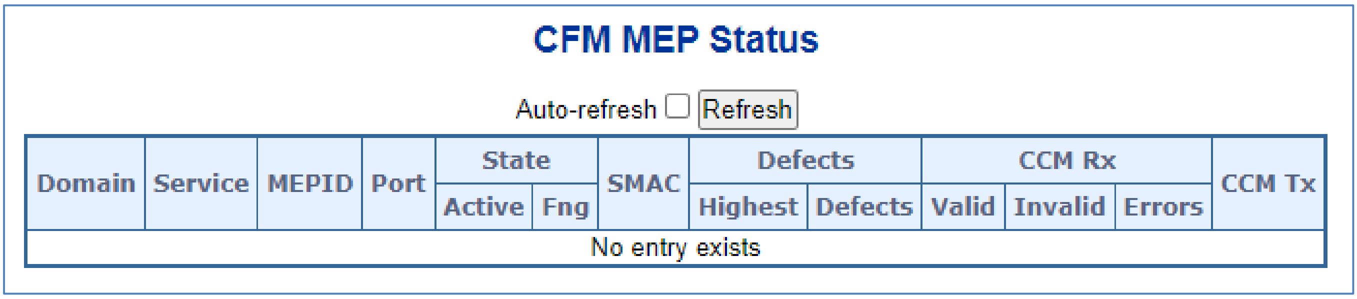


Figure 4-3-87: CFM MEP Status

Monitor CFM Status on this page.

Object	Description
• **Domain**	Name of Domain under which this Service resides.
• **Service**	Name of Service under which this MEP resides.
• **MEPID**	The identification of this MEP. Must be an integer [1..8091]
• **Port**	Port on which this MEP resides.
• **State**	**Active** Operational state of the MEP. : OFF. This indicates that the MEP Admin State is disabled. : DOWN. The MEP Admin State is enabled, but an error state exists. : UP. The MEP Admin State is enabled, and no errors and defects exists. **Fng** : Holds the current state of the Fault Notification Generator State Machine. Values will be one of the following: state — Description reset — No defect has been present since reset timer expired or the State Machine was last reset. defect — A defect is present, but not for a long enough time to be reported. reportDefect — A transient state during which the defect is reported. defectReported — A defect is present, and some defect has been reported. defectClearing — No defect is present, but the ResetTime timer has not yet expired.
• **SMAC**	This MEP's MAC address.
• **Defects**	**Highest** Highest priority defect that has been present since the MEP's fault notification generator state machine was last in the reset state. **Defects** : A MEP can detect and report a number of defects, and multiple defects can be present at the same time. This is indicated the following letter code.

<table>
<tr><td></td><td>
<table>
<tr><td>Code</td><td>Defect</td><td>Description</td></tr>
<tr><td>-</td><td>Defect not present</td><td>Defect not present</td></tr>
<tr><td>R</td><td>someRDIdefect</td><td>RDI received from at least one remote MEP</td></tr>
<tr><td>M</td><td>someMACstatusDefect</td><td>Received Port Status TLV != psUp or Interface Status TLV != isUp</td></tr>
<tr><td>C</td><td>someRMEPCCMdefect</td><td>Valid CCM is not received within 3.5 times CCM interval from at least one remote MEP</td></tr>
<tr><td>E</td><td>errorCCMdefect</td><td>Received CCM from an unknown remote MEP-ID or CCM interval mismatch</td></tr>
<tr><td>X</td><td>xconCCMdefect</td><td>Received CCM with an MD/MEG level smaller than configured or wrong MAID/MEGID (cross-connect)</td></tr>
</table>
</td></tr>
<tr><td>• CCM Rx</td><td>Valid: Total number of CCMs that hit this MEP and passed the validation test.
Invalid: Total number of CCMs that hit this MEP and didn't pass the validation test.
Errors: Total number of out-of-sequence errors seen from RMEPs.</td></tr>
<tr><td>• CCM Tx</td><td>Total number of CCM PDUs transmitted by this MEP.</td></tr>
</table>

Buttons

Refresh: Click to update values.

4.3.19 sFlow

4.3.19.1 sFlow Configuration

This page allows for configuring sFlow. The configuration is divided into two parts: Configuration of the sFlow receiver (a.k.a. sFlow collector) and configuration of per-port flow and counter samplers.

sFlow configuration is not persisted to non-volatile memory, which means that a reboot will disable sFlow sampling.

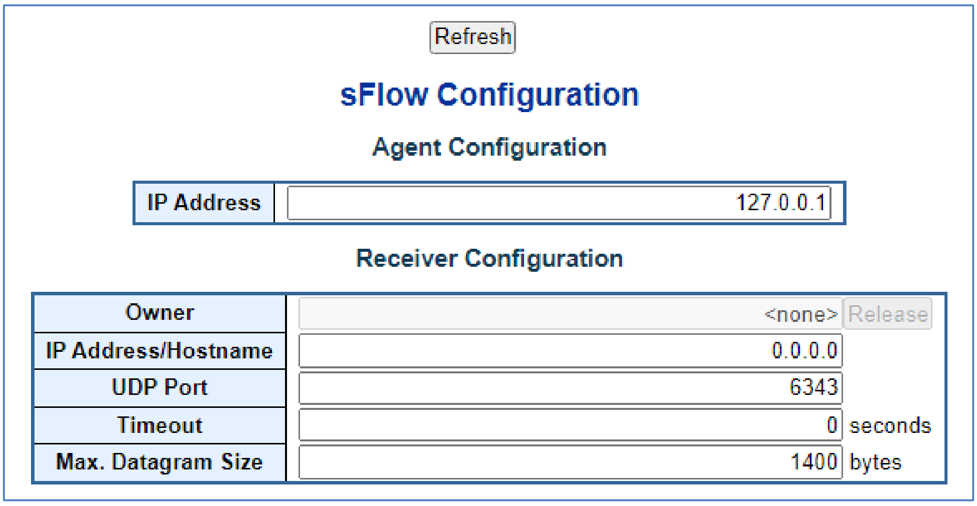


Figure 4-3-88: sFlow Configuration Page Screenshot

The displayed settings are:

Object	Description
• **IP Address**	The IP address used as Agent IP address in sFlow datagrams. It serves as a unique key that will identify this agent over extended periods of time. Both IPv4 and IPv6 addresses are supported.
• **Owner**	Basically, sFlow can be configured in two ways: Through local management using the Web or CLI interface or through SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows: • If sFlow is currently unconfigured/unclaimed, Owner contains <none>. • If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>. • If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver. If sFlow is configured through SNMP, all controls - except for the Release-button - are disabled to avoid inadvertent reconfiguration. The button allows for releasing the current owner and disable sFlow sampling. The button is disabled if sFlow is currently unclaimed. If configured through SNMP, the release must be confirmed (a confirmation request will appear).

• **IP Address**/Hostname	The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.
• **UDP Port**	The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.
• **Timeout**	The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh-button. If locally managed, the timeout can be changed on the fly without affecting any other settings. Valid range is 0 to 2147483647 seconds.
• **Max. Datagram Size**	The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 to 1468 bytes with default being 1400 bytes.

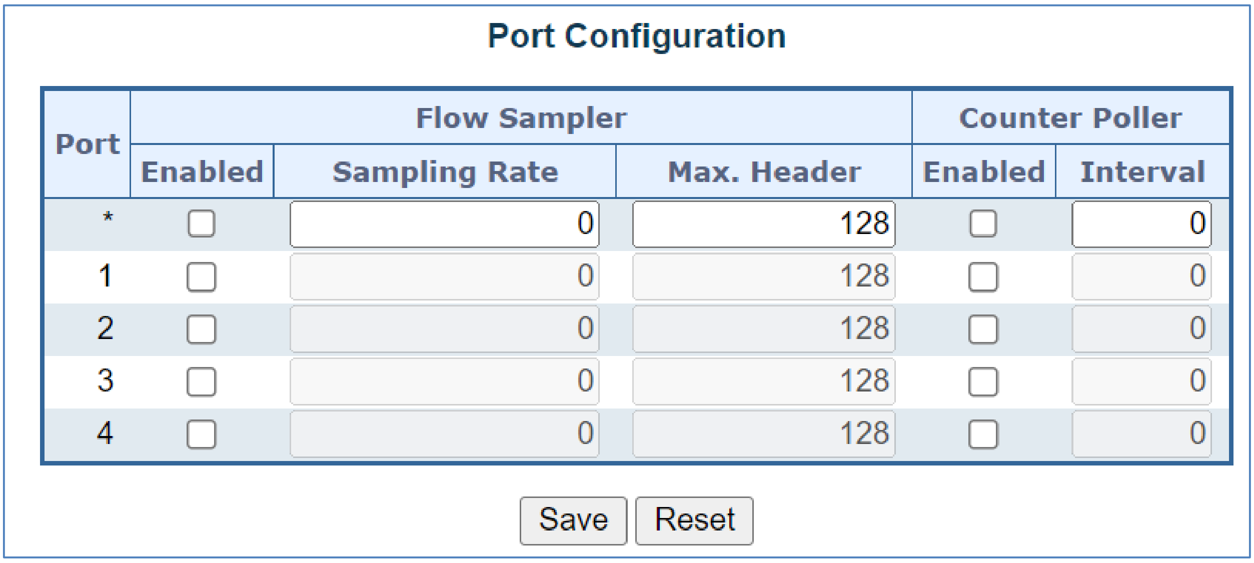


Figure 4-3-89: Port Configuration Page Screenshot

The displayed settings are:

Object	Description
• **Port**	The port number for which the configuration below applies.
• **Flow Sampler Enabled**	Enables/disables flow sampling on this port.
• **Flow Sampler Sampling Rate**	The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port. Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field. Valid range is 1 to 32767.
• **Flow Sampler Max. Header**	The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. Valid range is 14 to 200 bytes with default being 128 bytes. To have room for any frame, the maximum datagram size should be roughly 100

	bytes larger than the maximum header size. If the maximum datagram size does not take into account the maximum header size, samples may be dropped.
• **Counter Poller Enabled**	Enables/disables counter polling on this port.
• **Counter Poller Interval**	With counter polling enabled, this specifies the interval - in seconds - between counter poller samples. Valid range is 1 to 3600 seconds.

Buttons

Release: See description under Owner.

Refresh: Click to refresh the page. Note that unsaved changes will be lost.

Apply: Click to apply changes. Note that sFlow configuration is not persisted to non-volatile memory.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.19.2 sFlow Statistics

This page shows receiver and per-port sFlow statistics.

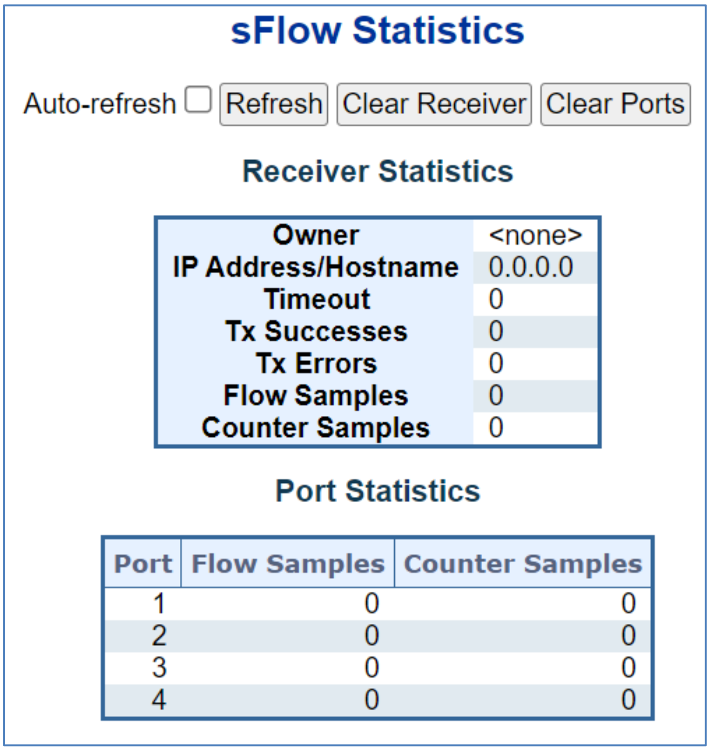


Figure 4-3-90: sFlow Statistics

Receiver Statistics

Object	Description
• **Owner**	This field shows the current owner of the sFlow configuration. It assumes one of three values as follows: • If sFlow is currently unconfigured/unclaimed, Owner contains **<none>**. • If sFlow is currently configured through Web or CLI, Owner contains **<Configured through local management>**. • If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.
• **IP Address/Hostname**	The IP address or hostname of the sFlow receiver.
• **Timeout**	The number of seconds remaining before sampling stops and the current sFlow owner is released.
• **Tx Successes**	The number of UDP datagrams successfully sent to the sFlow receiver.
• **Tx Errors**	The number of UDP datagrams that has failed transmission. The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping Web page (Diagnostics → Ping/Ping6).
• **Flow Samples**	The total number of flow samples sent to the sFlow receiver.
• **Counter Samples**	The total number of counter samples sent to the sFlow receiver.

Port Statistics

Object	Description
• **Port**	The port number for which the following statistics applies.
• **Flow Samples**	The number of flow samples sent to the sFlow receiver originating from this port.
• **Counter Samples**	The total number of counter samples sent to the sFlow receiver originating from this port.

Buttons

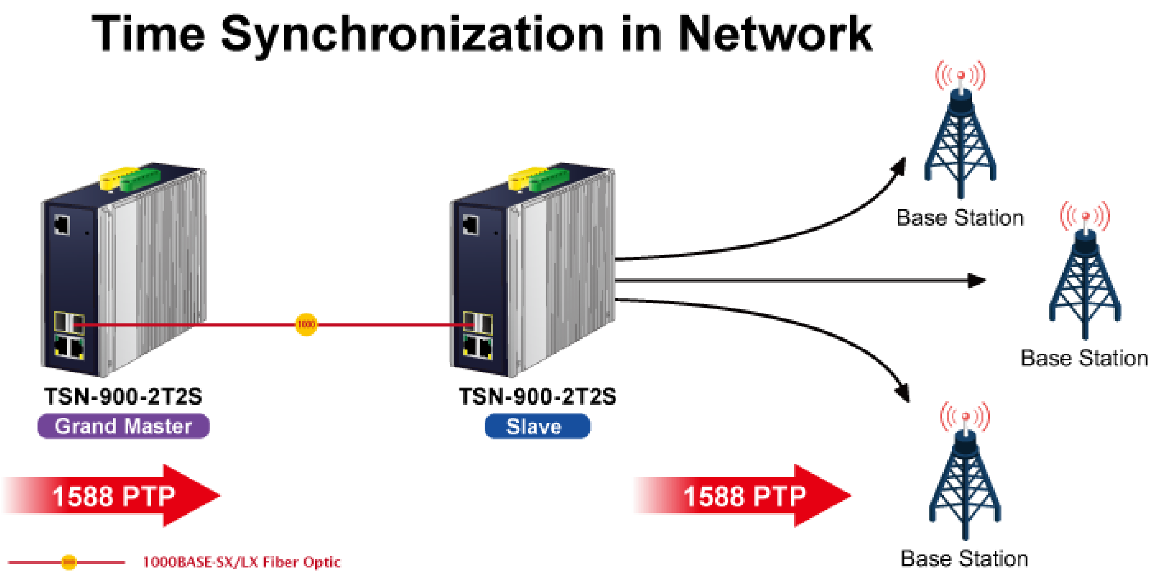
Auto-refresh ☐:Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Clear Receiver : Clears the sFlow receiver counters.

Clear Ports : Clears the per-port counters.

4.3.20 PTP

The **Precision Time Protocol** (**PTP**) is a protocol used to synchronize clocks throughout a computer network. On a local area network, it achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control systems.



PTP was originally defined in the **IEEE 1588-2002** standard, officially entitled *"Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems"* and published in 2002. In 2008 a revised standard, **IEEE 588-2008** was released. This new version, also known as PTP Version 2, improves accuracy, precision and robustness but is not backwards compatible with the original 2002 version.

"IEEE 1588 is designed to fill a niche not well served by either of the two dominant protocols, **NTP** and **GPS**. IEEE 1588 is designed for local systems requiring accuracies beyond those attainable using NTP. It is also designed for applications that cannot bear the cost of a GPS receiver at each node, or for which GPS signals are inaccessible"

4.3.20.1 PTP Configuration

This page allows the user to configure and inspect the current PTP clock settings as shown below:.

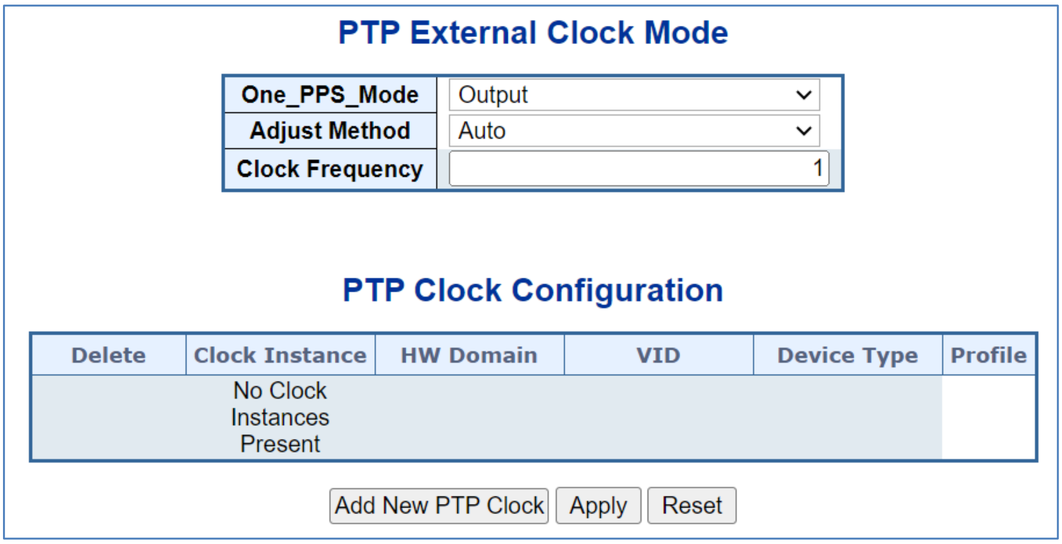


Figure 4-3-91: PTP Configuration Page Screenshot

Object	Description
• **One_PPS_Mode**	This Selection box will allow you to select the One_pps_mode configuration. The following values are possible: 1. Output : Enable the 1 pps clock output 2. Disable : Disable the 1 pps clock output
• **Adjust Method**	This Selection box will allow you to configure the Frequency adjustment configuration. 1. LTC : Select Local Time Counter (LTC) frequency control 2. Single : Select SyncE DPLL frequency control, if allowed by SyncE 3. Independent : Select an oscillator independent of SyncE for frequency control, if supported by the HW 4. Common : Select second DPLL for PTP, Both DPLL have the same (SyncE recovered) clock. 5. Auto : AUTO Select clock control, based on PTP profile and available HW resources.
• **Clock Frequency**	This will allow to set the Clock Frequency. The possible range of values are 1 - 25000000 (1 - 25MHz).
• **Delete**	Check this box and click on 'Save' to delete the clock instance.
• **Clock Instance**	Indicates the Instance 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.
• **VID**	VLAN Identifier used for tagging the VLAN packets.

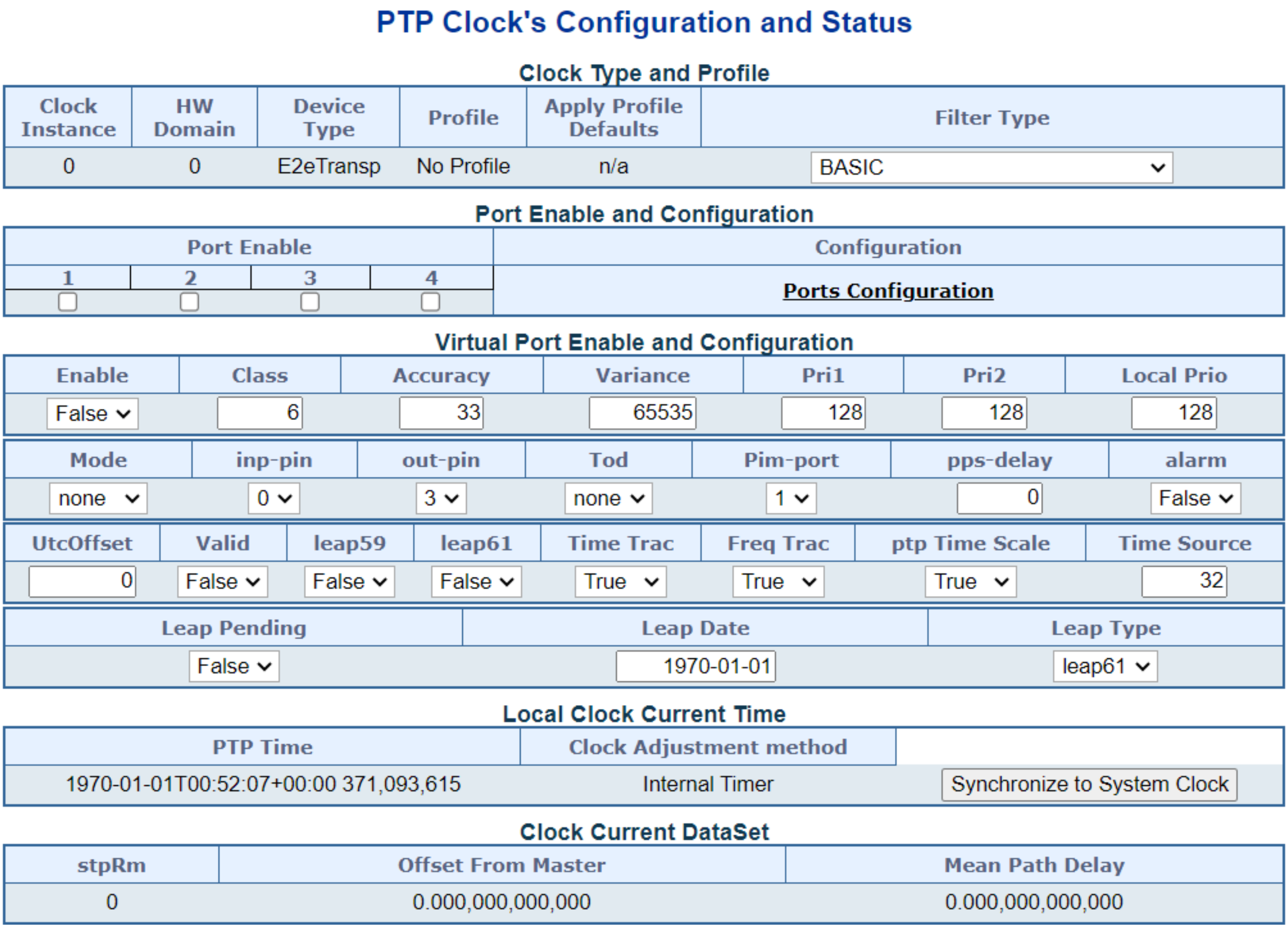
• **Device Type**	Indicates the Type of the Clock Instance. There are six Device Types. 1. Ord-Bound - clock's Device Type is Ordinary-Boundary Clock. 2. P2p Transp - clock's Device Type is Peer to Peer Transparent Clock. 3.E2e Transp - clock's Device Type is End to End Transparent Clock. 4. Master Only - clock's Device Type is Master Only. 5. Slave Only - clock's Device Type is Slave Only. 6. BC-frontend - clock's Device Type is Boundary Clock frontend.
• **Profile**	Indicates the profile used by the clock.

Buttons

Add New PTP Clock : Click to create a new clock instance

Apply : Click to save the page immediately.

Reset : Click to reset the the page immediately.



Clock Parent DataSet

Parent Port ID	port	PStat	Var	Rate	GrandMaster ID	GrandMaster Clock Quality	Pri1	Pri2
a8:f7:e0:ff:fe:43:25:67	0	False	0	0	a8:f7:e0:ff:fe:43:25:67	Cl:248 Ac:Unknwn Va:65535	128	128

Clock Default DataSet

Device Type	One-Way	2 Step Flag	Ports	Clock Identity	Dom	Clock Quality
E2eTransp	False	False	4	a8:f7:e0:ff:fe:43:25:67	0	Cl:248 Ac:Unknwn Va:65535

Pri1	Pri2	Local Prio	Protocol	PCP	DSCP
128	128	128	Ethernet	0	0

Clock Time Properties DataSet

UtcOffset	Valid	leap59	leap61	Time Trac	Freq Trac	ptp Time Scale	Time Source
0	False	False	False	False	False	True	160

Leap Pending	Leap Date	Leap Type
False	1970-01-01	leap61

Basic Filter Parameters

Delay Filter	Period	Dist
0	10	0

Basic Servo Parameters

Display	P-enable	I-enable	D-enable	'P' constant	'I' constant	'D' constant	Gain constant
False	True	False	False	1	30	40	1

Apply Reset

The page includes the following fields:

Clock Type and Profile

Clock Type and Profile

Clock Instance	HW Domain	Device Type	Profile	Apply Profile Defaults	Filter Type
0	0	E2eTransp	1588	Apply	ACI_BASIC_PHASE_LOW

Object	Description
• **Clock Instance**	Indicates the instance number of a particular Clock Instance [0..3].
• **HW Domain**	Indicates the HW clock domain used by the clock.
• **Device Type**	Indicates the Type of the Clock Instance. There are two Device Types. 1. P2p Transp - clock's Device Type is Peer to Peer Transparent Clock. 2. E2e Transp - clock's Device Type is End to End Transparent Clock.
• **Profile**	Indicates the profile used by the clock.
• **Apply Profile Defaults**	If the clock has been configured to use a profile, clicking the 'Apply' button will reset configured values to profile defaults.
• **Filter Type**	The PTP filter type determines should match the operating conditions of the network and the PTP profile.

	Filter Types

PTP Profile	SyncE enabled(hybrid)	Filter type	Description
1588	No	ACI_BASIC_PHASE	Requires PTP Sync and Delay_req frame rate of 16 fps or higher.
1588	Yes	ACI_BASIC_PHASE_SYNCE	Requires PTP Sync and Delay_req frame rate of 16 fps or higher.
1588	No	ACI_BASIC_PHASE_LOW	Use when the PTP Sync and Delay_req frame rate is between 1 fps to 16 fps.
1588	Yes	ACI_BASIC_PHASE_LOW_SYNCE	Use when the PTP Sync and Delay_req frame rate is between 1 fps to 16 fps.
None	No	ACI_BC_FULL_ON_PATH_FREQ	Used for Syntonized TC with basic filter.

Port Enable and Configuration

Port Enable and Configuration

Port Enable				Configuration
1	2	3	4	Ports Configuration
☐	☐	☐	☐	

Object	Description
• **Port Enable**	Set check mark for each port configured for this Clock Instance.
• **Configuration**	Click **'Ports Configuration**' to edit the port data set for the ports assigned to this clock instance.

Port Data Set

The port data set is defined in the IEEE 1588 Standard. It holds three groups of data: the static members, the dynamic members, and configurable members which can be set here.

PTP Clock's Port Data Set Configuration

Port	Stat	MDR	PeerMeanPathDel	Anv	ATo	Syv	Dlm	MPR	Delay Asymmetry	Ingress Latency	Egress Latency	Version	Mcast Addr	Not Slave	Local Prio	2 Step Flag	Not Master

Apply Reset

Object	Description
• **Port**	Static member port Identity : Port number [1..max port no]
• **Stat**	Dynamic member portState: Current state of the port.
• **MDR**	Dynamic member log Min Delay Req Interval: The delay request interval announced by the master.
• **Peer Mean Path Del**	The path delay measured by the port in P2P mode. In E2E mode this value is 0
• **Anv**	The interval for issuing announce messages in master state. Range is -3 to 4.
• **ATo**	The timeout for receiving announce messages on the port. Range is 1 to 10.
• **Syv**	The interval for issuing sync messages in master. Range is -7 to 4.

• **Dlm**	Configurable member delayMechanism: The delay mechanism used for the port: e2e End to end delay measurement p2p Peer to peer delay measurement. Can be defined per port in an Ordinary/Boundary clock. In a transparent clock all ports use the same delay mechanism, determined by the clock type.
• **MPR**	The interval for issuing Delay_Req messages for the port in **E2e** mode. This value is announced from the master to the slave in an announce message. The value is reflected in the MDR field in the Slave The interval for issuing Pdelay_Req messages for the port in P2P mode Range is -7 to 5. **Note:** The interpretation of this parameter has changed from release 2.40. In earlier versions the value was interpreted relative to the Sync interval, this was a violation of the standard, so now the value is interpreted as an interval. i.e. MPR=0 => 1 Delay_Req pr sec, independent of the Sync rate.
• **Delay Asymmetry**	If the transmission delay for a link in not symmetric, the asymmetry can be configured here, see IEEE 1588 Section 7.4.2 Communication path asymmetry Range is -100000 to 100000. Version The current implementation only supports PTP version 2
• **Ingress latency**	Ingress latency measured in ns, as defined in IEEE 1588 Section 7.3.4.2. Range is -100000 to 100000.
• **Egress Latency**	Egress latency measured in ns, as defined in IEEE 1588 Section 7.3.4.2. Range is -100000 to 100000.
• **Version**	PTP version used by this port
• **Mcast Addr**	Configured destinaton address for multicast packets (PTP default or LinkLocal)
• **Not Slave**	TRUE indicates that this interface cannot enter slave mode
• **Local Prio**	1-255, priority used in the 8275.1 BMCA
• **2 Step Flag**	Option to override the 2-step option on port level */ // **IEEE 802.1AS** specific parameters are only available when the 802.1AS profile is selected
• **Not Master**	TRUE indicates that this interface cannot enter master mode

Virtual Port Enable and Configuration

Virtual Port Enable and Configuration

Enable	Class	Accuracy	Variance	Pri1	Pri2	Local Prio
False	6	33	65535	128	128	128

Mode	inp-pin	out-pin	Tod	Pim-port	pps-delay	alarm
none	0	3	none	1	0	False

UtcOffset	Valid	leap59	leap61	Time Trac	Freq Trac	ptp Time Scale	Time Source
0	False	False	False	True	True	True	32

Leap Pending	Leap Date	Leap Type
False	1970-01-01	leap61

Object	Description
• **Enable**	Disabled or Enabled.
• **Class**	Clock class value for clock as defined in IEEE Std 1588. The valid range is from 0 to 255.
• **Accuracy**	Clock accuracy value as defined in IEEE Std 1588. The valid range is 0 to 255.
• **Variance**	offsetScaledLogVariance for clock as defined in IEEE Std 1588. The valid range is 0 to 65535.
• **Pri1**	Clock priority 1 [0..255] used by the BMC master select algorithm.
• **Pri2**	Clock priority 2 [0..255] used by the BMC master select algorithm.
• **Local Prio**	Priority [1..255]used in the 8275.1 BMCA.
• **Mode**	Virtual-port mode :Main-auto | Main-man | Sub | PPS-out | PPS-in | freq-out | disabled. The first three are based on the PTP Time Interface, which combines 1PPS with a serial channel. The next three uses a raw io pin. Fields inp-pin and out-pin are only relevant in the PPS-out, PPS-in or freq-out modes. The value range depends on the board design.In the main-auto, main-man or sub modes, the boards supports one set of io pins, therefore external_io_pin is not configurable in these modes. Some of the boards like the caracal platform type do not support virtual port.
• **inp-pin**	The external IO pin that can be used for Mode: PPS-in
• **out-pin**	The external IO pin that can be used for Mode: PPS-out/freq-out
• **Tod**	The 1PPS can be combined with either a serial channel, sending/receiving timeofday information in one of a number of standard formats, or an Ethernet port transferring timeofday information in a proprietary format (PIM). None | Serial | PIM None: No TOD information is provided. Serial: Different serial protocols are implemented: polyt, rmc, zda. It depends on the board design which IO pin that can be combined with a serial communication.

• **Pim-port**	Port number that is used to transfer time of day information when PIM protocol is used
• **pps-delay**	Delay compensation for the 1pps signal when it is received at the sub device.
• **alarm**	Alarms are used to notify possible traceability issues in time and frequency at the sender. This field is introduced to emulate GNSS status messages.
• **UtcOffset**	It is the offset between TAI and UTC. GNSS servers on virtual port use UTC.
• **Valid**	When true, the value of currentUtcOffset is valid
• **leap59**	When true, this field indicates that last minute of the current UTC day has only 59 seconds.
• **leap61**	When true, this field indicates that last minute of the current UTC day has 61 seconds.
• **Time Trac**	True if the timescale and the value of currentUtcOffset are traceable to a primary reference.
• **Freq Trac**	True if the frequency determining the timescale is traceable to a primary reference.
• **ptp Time Scale**	True if the clock timescale of the grandmaster clock and false otherwise.
• **Time Source**	The source of time used by the grandmaster clock.
• **Leap Pending**	When true, there is a leap event pending at the date defined by leapDate.
• **Leap Date**	The date for which the leap will occur at the end of its last minute. Date is represented as the number of days after 1970-01-01 (the latter represented as 0).
• **Leap Type**	The type of leap event i.e. leap59 or leap61.

Local Clock Current Time

Local Clock Current Time

PTP Time	Clock Adjustment method	Synchronize to System Clock
1970-01-01 Thu 03:41:03+00:00 806,497,060	Internal Timer	Synchronize to System Clock

Object	Description
• **PTP Time**	Shows the actual PTP time with nanosecond resolution.
• **Clock Adjustment Method**	Shows the actual clock adjustment method. The method depends on the available hardware.
• **Synchronize to System Clock**	Activate this button to synchronize the System Clock to PTP Time.

Clock current DataSet

Clock Current DataSet

stpRm	Offset From Master	Mean Path Delay
0	0.000,000,000	0.000,000,000

Object	Description
• **stpRm**	Steps Removed : It is the number of PTP clocks traversed from the grandmaster to the local slave clock.
• **Offset from master**	Time difference between the **master clock** and the **local slave clock**, measured in **ns**.
• **Mean Path Delay**	The mean propagation time for the link between the **master** and the **local slave**

Clock Parent DataSet

The clock parent data set is defined in the IEEE 1588 standard. The parent data set is dynamic.

Clock Parent DataSet

Parent Port ID	port	PStat	Var	Rate	GrandMaster ID	GrandMaster Clock Quality	Pri1	Pri2
a8:f7:00:ff:fe:00:12:34	0	False	0	0	a8:f7:00:ff:fe:00:12:34	Cl:248 Ac:Unknwn Va:65535	128	128

Object	Description
• **Parent Port Identity**	Clock identity for the parent clock, if the local clock is not a slave, the value is the clocks own id.
• **Port**	Port Id for the parent master port
• **P Stat**	Parents Stats (always false).
• **Var**	It is observed parent offset scaled log variance
• **Rate**	Observed Parent Clock Phase Change Rate. i.e. the slave clocks rate offset compared to the master. (unit = ns per s).
• **Grand Master ID**	Clock identity for the grand master clock, if the local clock is not a slave, the value is the clocks own id.
• **Grand Master Clock Quality**	The clock quality announced by the grand master (See description of Clock Default Data Set: Clock Quality)
• **Pri1**	Clock priority 1 announced by the grand master
• **Pri2**	Clock priority 2 announced by the grand master

Clock Default DataSet

The clock default data set is defined in the IEEE 1588 Standard. It holds three groups of data: the static members defined at clock creation time, the Dynamic members defined by the system, and the configurable members which can be set here.

Clock Default DataSet

Device Type	One-Way	2 Step Flag	Ports	Clock Identity	Dom	Clock Quality
E2eTransp	False	False	4	a8:f7:e0:ff:fe:43:25:67	0	Cl:248 Ac:Unknwn Va:65535

Pri1	Pri2	Local Prio	Protocol	PCP	DSCP
128	128	128	Ethernet	0	0

Object	Description
• **Device Type**	Indicates the Type of the Clock Instance. There are five Device Types. ■ **P2p Transp** - clock's Device Type is Peer to Peer Transparent Clock. ■ **E2e Transp** - clock's Device Type is End to End Transparent Clock.
• **One-Way**	If true, one way measurements are used. This parameter applies only to a slave. In one-way mode no delay measurements are performed, i.e. this is applicable only if frequency synchronization is needed. The master always responds to delay requests.
• **2 Step Flag**	Static member: defined by the system, true if two-step Sync events and Pdelay_Resp events are used
• **Ports**	The total number of physical ports in the node
• **Clock Identity**	It shows unique clock identifier
• **Dom**	Clock domain [0..127].
• **Clock Quality**	The clock quality is determined by the system, and holds 3 parts: **Clock Class**, **Clock Accuracy** and **OffsetScaledLog Variance** as defined in IEEE1588. The Clock Accuracy values are defined in IEEE1588 table 6 (Currently the clock Accuracy is set to 'Unknown' as default).
• **Pri1**	Clock priority 1 [0..255] used by the BMC master select algorithm.
• **Pri2**	Clock priority 2 [0..255] used by the BMC master select algorithm.
• **Local Prio**	Priority [1..255] used in the 8275.1 BMCA.
• **Protocol**	Transport protocol used by the PTP protocol engine ■ **Ethernet** PTP over Ethernet multicast ■ **EthernetMixed** PTP using a combination of Ethernet multicast and unicast ■ **IPv4Multi** PTP over IPv4 multicast ■ **IPv4Mixed** PTP using a combination of IPv4 multicast and unicast ■ **IPv4Uni** PTP over IPv4 unicast
• **PCP**	Priority Code Point value used for PTP frames.
• **DSCP**	DSCP value used when transmitting IPv4 encapsulated packets

Clock Time Properties DataSet

The clock time properties data set is defined in the IEEE 1588 Standard. The data set is both configurable and dynamic, i.e. the parameters can be configured for a grandmaster. In a slave clock the parameters are overwritten by the grandmasters timing properties. The parameters are not used in the current PTP implementation.

The valid values for the Time Source parameter are:

- 16 (0x10) ATOMIC_CLOCK
- 32 (0x20) GPS
- 48 (0x30) TERRESTRIAL_RADIO
- 64 (0x40) PTP
- 80 (0x50) NTP
- 96 (0x60) HAND_SET
- 144 (0x90) OTHER
- 160 (0xA0) INTERNAL_OSCILLATOR

Clock Time Properties DataSet

UtcOffset	Valid	leap59	leap61	Time Trac	Freq Trac	ptp Time Scale	Time Source
0	False	False	False	False	False	True	160

Leap Pending	Leap Date	Leap Type
False	1970-01-01	leap61

Object	Description
• **UtcOffset**	In systems whose epoch is UTC, it is the offset between TAI and UTC
• **Valid**	When true, the value of currentUtcOffset is valid
• **leap59**	When true, this field indicates that last minute of the current UTC day has only 59 seconds.
• **leap61**	When true, this field indicates that last minute of the current UTC day has 61 seconds.
• **Time Trac**	True if the timescale and the value of currentUtcOffset are traceable to a primary reference.
• **Freq Trac**	True if the frequency determining the timescale is traceable to a primary reference.
• **ptp Time Scale**	True if the clock timescale of the grandmaster clock and false otherwise.
• **Time Source**	The source of time used by the grandmaster clock.
• **Leap Pending**	When true, there is a leap event pending at the date defined by leapDate.
• **Leap Date**	The date for which the leap will occur at the end of its last minute. Date is represented as the number of days after 1970-01-01 (the latter represented as 0).
• **Leap Type**	The type of leap event i.e. leap59 or leap61.

Basic Filter Parameters

The default delay filter is a low pass filter, with a time constant of 2*DelayFilter*DelayRequestRate.

Basic Filter Parameters

Delay Filter	Period	Dist
0	10	0

Object	Description
• **Delay Filter**	If the **DelayFilter** parameter is set to 0 or the **Dist** parameter is 0, the delay filter uses the same algorithm as the offset filter. The default offset filter uses a minimum offset or a mean filter method
• **Period**	i.e. The minimum measured offset during **Period** samples is used in the calculation.
• **Dist**	The distance between two calculations is **Dist** periods. Note: In configurations with Timestamp enabled PHYs, the period is automatically increased, if (period*dist < SyncPackets pr sec/4), i.e. max 4 adjustments are made pr sec. If **Dist** is 0 the offset is low pass filtered using **Period** to determine the filter bandwidth. The filter BW is **Period**/100 Hz which provides a resolution of 0.01 Hz, the filter automatically adapts to the packet rate, If **Dist** is 1 the offset is averaged over the **Period**, If **Dist** is >1 the offset is calculated using 'min' offset.

Basic Servo Parameters

The Basic clock servo uses a PID regulator to calculate the current clock rate.

i.e. clockAdjustment = OffsetFromMaster/ P constant + Integral(OffsetFromMaster)/ I constant + Differential OffsetFromMaster)/ D constant

Basic Servo Parameters

Display	P-enable	I-enable	D-enable	'P' constant	'I' constant	'D' constant	Gain constant
False	True	False	False	1	30	40	1

Object	Description
• **Display**	If true then Offset From Master, MeanPathDelay and clockAdjustment are logged on the debug terminal
• **P-enable**	If true the P part of the algorithm is included
• **I-enable**	If true the I part of the algorithm is included
• **D-enable**	If true the D part of the algorithm is included
• **'P' constant**	[1..10000] see above
• **'I' constant**	[1..10000] see above
• **'D' constant**	[1..10000] see above
• **Gain constant**	[1..10000] see above

4.3.20.2 PTP Status

This page allows the user to inspect the current PTP clock settings as shown below:

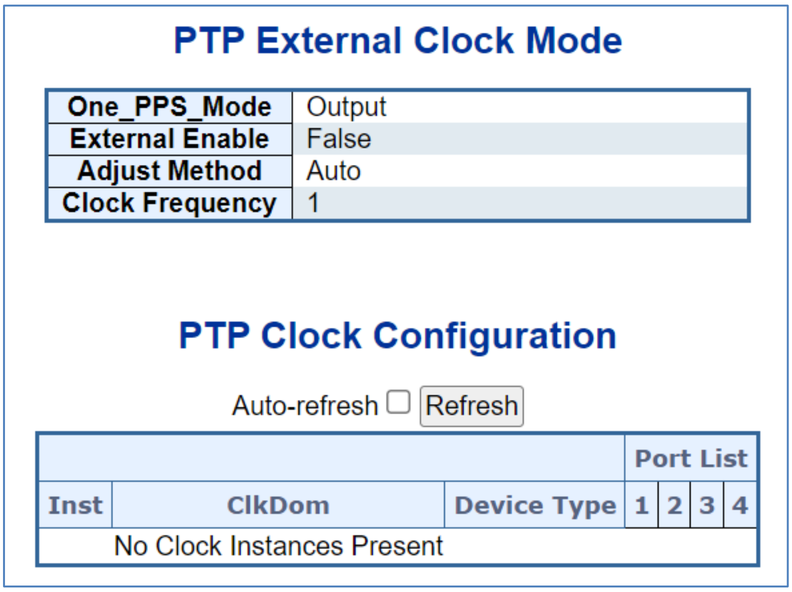


Figure 4-3-92: PTP Clock Monitor Page Screenshot

Object	Description
• **Inst**	Indicates the Instance of a particular Clock Instance [0..3]. Click on the Clock Instance number to monitor the Clock details.
• **ClkDom**	Indicates the Clock domain used by the Instance of a particular Clock Instance [0..3]
• **Device Type**	Indicates the Type of the Clock Instance. There are five Device Types 1. P2p Transp - Clock's Device Type is Peer to Peer Transparent Clock. 2. E2e Transp - Clock's Device Type is End to End Transparent Clock.
• **Port List**	Shows the ports configured for that Clock Instance.

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4.3.20.3 802.1AS Statistics

This page allows the user to inspect the current PTP configurations, and possibly change them as well, as shown below:

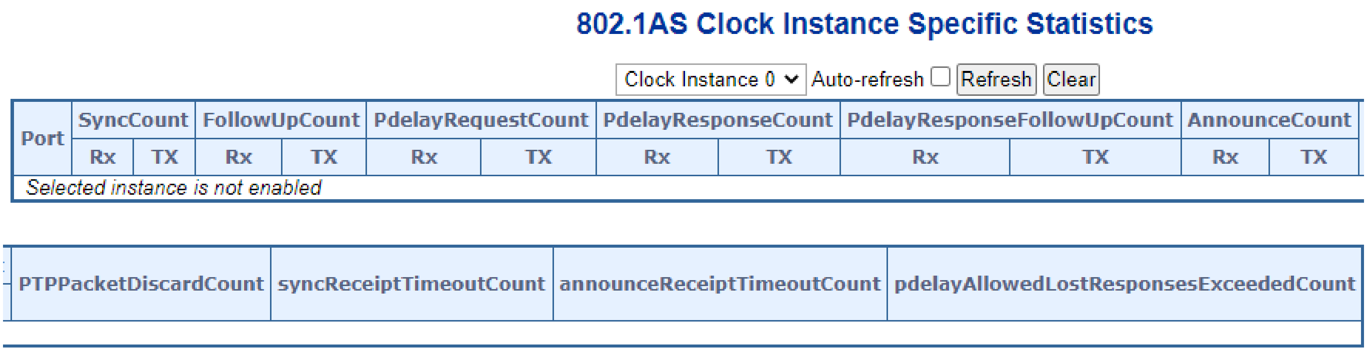


Figure 4-3-93: 802.1AS Statistics Page Screenshot

Object	Description
• **Delete SyncCount**	A counter that increments every time when synchronization information is received.
• **Clock Instance FollowUpCount**	A counter that increments every time when a Follow Up message is received.
• **HW Domain PdelayRequestCount**	A counter that increments every time when a Pdelay_Req message is received.
• **PdelayResponseCount**	A counter that increments every time when a Pdelay_Resp message is received
• **PdelayResponseFollowUpCount**	A counter that increments every time when a Pdelay_Resp_Follow_Up message is received.
• **AnnounceCount**	A counter that increments every time when an Announce message is received
• **PTPPacketDiscardCount**	A counter that increments every time when a PTP message is discarded.
• **syncReceiptTimeoutCount**	A counter that increments every time when sync receipt timeout occurs
• **announceReceiptTimeoutCount**	A counter that increments every time when announce receipt timeout occurs
• **Pdelay Allowed Lost Responses ExceededCount**	A counter that increments everytime the value of the variable lostResponses exceeds the value of the variable allowedLostResponses
• **AnnounceCount**	A counter that increments every time an Announce message is transmitted.

Buttons

Display : Click to Display the configured values.

Clear : Clears the statistics.

4.3.21 TSN

PLANET **Industrial Managed TSN Device** provides real-time, low-latency network communication for industrial automation, 5G NR networks, Industry 4.0, 4K/8K video streaming, and VR/AR gaming industry by using the **Time-sensitive Networking (TSN)** technology and **IEEE 1588 Precision Time Protocol (PTPv2)** for time synchronization on all ports.

The **Industrial Managed TSN Device** supports TSN IEEE standards needed for a complete real-time communication solution. These include

IEEE 802.1AS-REV profile for time synchronization,

IEEE **802.1Qbv** Enhancements for Scheduled Traffic,

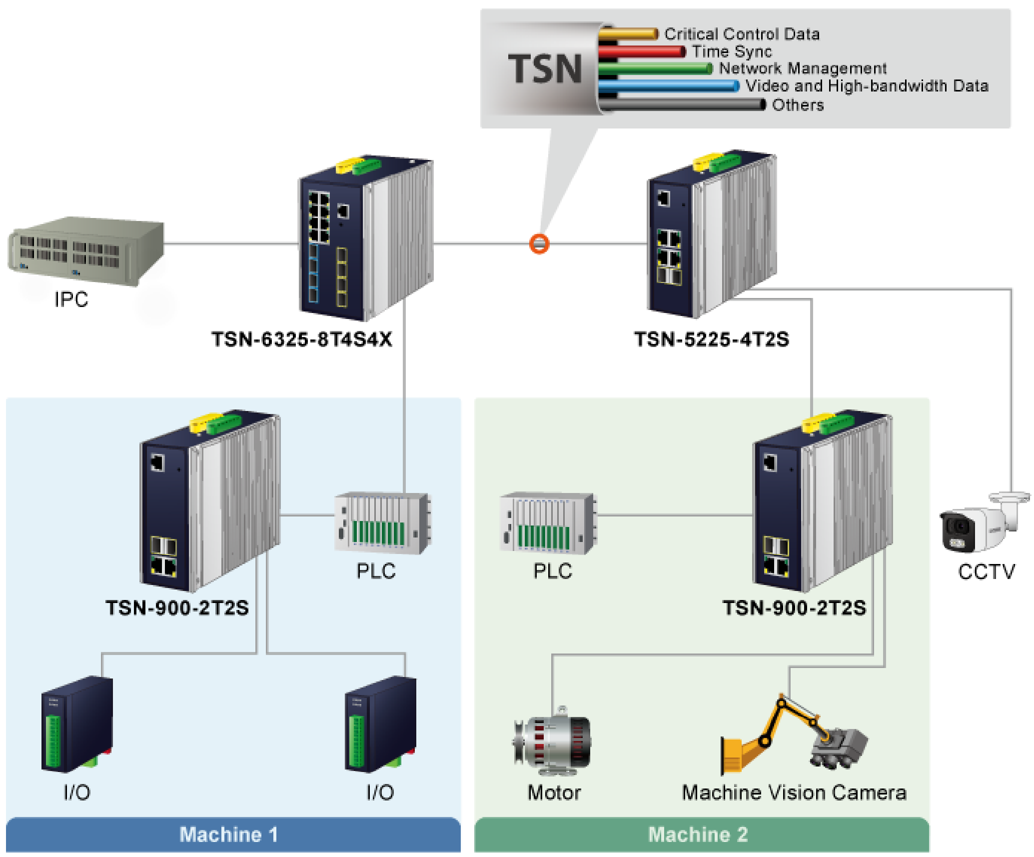
IEEE 802.1Qbu Frame Preemption,

IEEE 802.3br Interspersing Express Traffic (IET),

IEEE **802.1Qci** for per-stream filtering and policing (**PSFP**) and

IEEE **802.1CB** frame replication and elimination for reliability (**FRER**) for seamless redundancy.

The **Industrial Managed TSN Device** eliminates the need for separating information technology (IT) and operational technology (OT) Ethernet networks, providing a more ubiquitous approach to synchronization and precision timing for today's industrial automation systems.



4.3.21.1 Streams

This page gives an overview of the configured streams, and it allows for deleting and editing existing streams as well as adding new. Please refer to the following Figure 4-3-94.

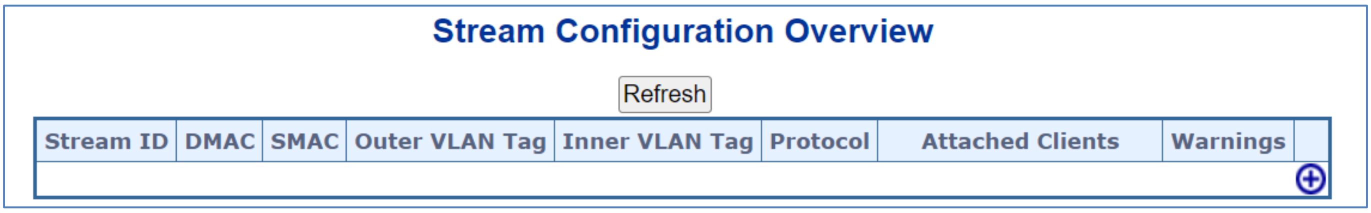


Figure 4-3-94: Stream Configuration Page Screenshot

Object	Description
• **Stream ID**	The ID of the stream. The lower the ID, the higher precedence when matching. For example, if Stream #1 matches all frames with a multicast DMAC and Stream #2 matches a particular multicast DMAC, Stream #2 will never be hit.
• **DMAC**	Indicates which types of destination MAC addresses are matched.
• **SMAC**	Indicates whether a particular source MAC address (with an optional mask) or any source MAC address is matched.
• **Outer VLAN Tag**	Indicates the required presence of an outer VLAN tag.
• **Inner VLAN Tag**	Indicates the required presence of an inner VLAN tag.
• **Protocol**	Indicates layer 3 and 4 matching options.
• **Attached Clients**	Streams don't do anything by themselves. They are utilized by PSFP and FRER for matching particular flows. This field indicates which of those two protocols - if any - are utilizing a particular stream. The number in parenthesis shows the PSFP or FRER instance the stream is used on.
• **Warnings**	Configuration of a stream may result in configurational warnings. If it is yellow, at least one configurational warning is detected. Hover the mouse over the image to see a list of the warnings. If it is green, no configurational warnings are detected. For a description of the possible configurational warnings, refer to Stream Configuration Help.

Configuration Buttons

On the right hand side of each stream, you find two buttons:

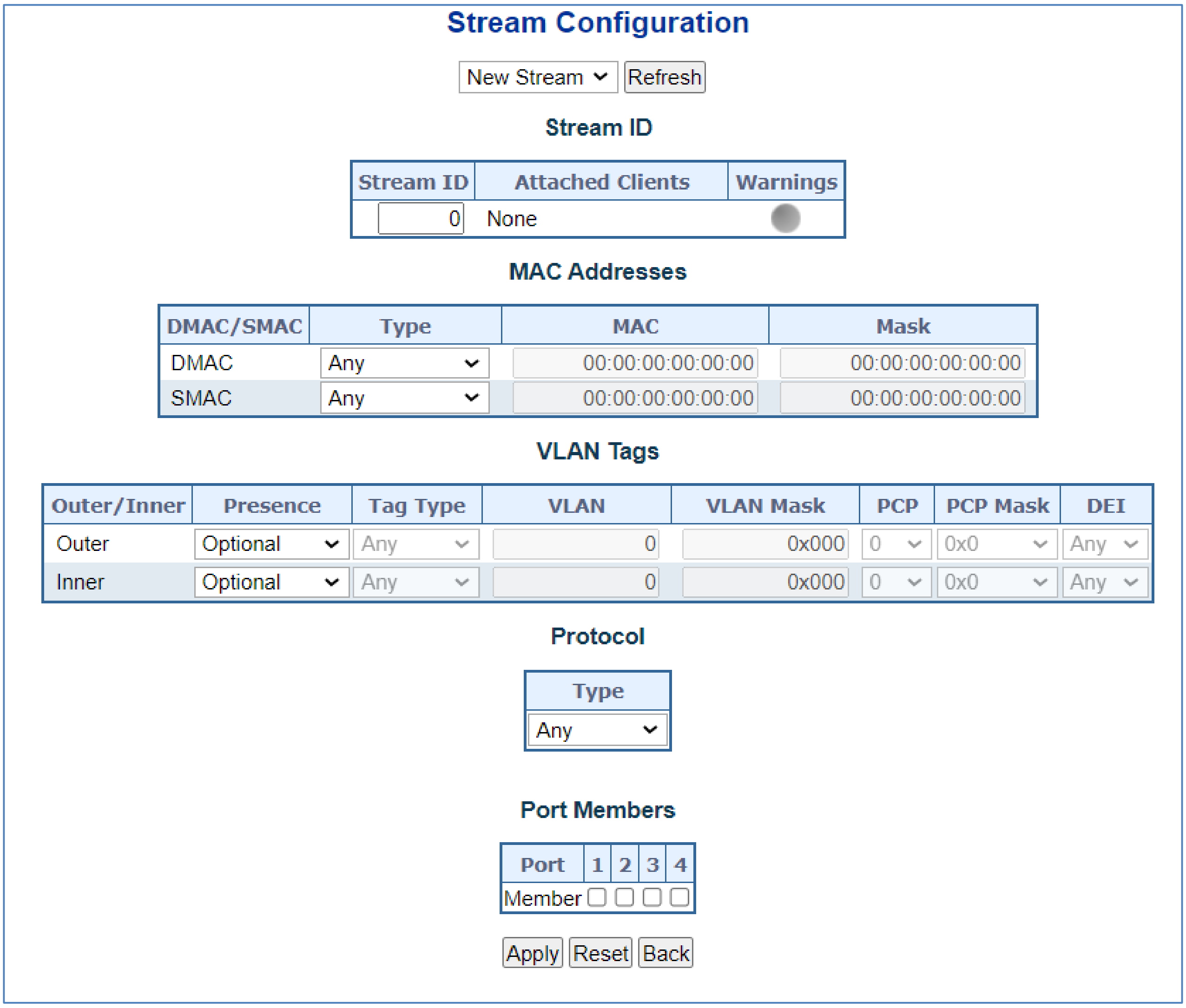
: Click to edit this stream.

: Click to delete this stream (happens immediately without confirmation).

The very last row in the table also contains a button:

: Click to create a new stream.

: Click to refresh the page immediately. This is useful if the stream configuration has been changed from e.g. CLI.



This page allows for editing existing or new streams.

At the top right corner, the page offers a drop-down list, where any of the existing streams can be selected. Notice that if you have changed contents of a stream without saving and then change to another stream, the changes with be lost without confirmation.

Besides all the existing streams, the selector has one last item, which allows for creating a new stream.

The page is divided into sections corresponding to fields in a frame, starting with Layer 2 fields (MAC addresses, possible VLAN tags, and EtherType) and followed by Layer 3 and Layer 4 fields.

Stream ID

Object	Description
• **Stream ID**	The ID of the stream. The lower the ID, the higher precedence when matching. For example, if Stream #1 matches all frames with a multicast DMAC and Stream #2 matches a particular multicast DMAC, Stream #2 will never be hit.
• **Attached Clients**	Streams don't do anything by themselves. They are utilized by PSFP and

	FRER for matching particular flows. This field indicates which of those two protocols - if any - are utilizing a particular stream. The number in parenthesis shows the PSFP or FRER instance the stream is used on.
• **Warnings**	Configuration of a stream may result in configurational warnings. For instance, if a stream is not instantiated on any ports, it is not of any use, and a warning will appear. A color indicates the warning state as follows: • : The stream is not yet created • : The stream has no configurational warnings • : The stream has configurational warnings When yellow, hover the mouse over the image to see a list of configurational warnings. The possible warnings are as follows: • The stream does not have any member ports • No clients attached. Rule not installed in hardware It is important to note that not all configurational errors are detected. An example of configurational errors that are not detected includes the case described under Stream ID, where stream #2 cannot be hit.

MAC Addresses

Besides the heading row, this table holds one row for Destination MAC (DMAC) address matching and another for Source MAC (SMAC) address matching.

Object	Description
• **DMAC/SMAC**	Indicates whether this row in the table is for DMAC or SMAC matching.
• **Type**	The drop-down list for the DMAC offers the following options: • Any: Match on any DMAC (default) • Multicast: Match on multicast (but not broadcast) frames • Broadcast: Match on broadcast frames • Unicast: Match on unicast frames • Not Broadcast: Match on unicast and multicast frames • Not Unicast: Match on multicast and broadcast frames • MAC/Mask: Match on a particular DMAC address with mask. The 'MAC' and 'Mask' fields will become available for editing when this is selected

	The drop-down list for the SMAC offers only the following options: • Any: Match on any SMAC (default) • MAC/Mask: Match on a particular SMAC address with mask. The 'MAC' and 'Mask' fields will become available for editing when this is selected
• **MAC**	This field is only available when Type is set to 'MAC/Mask'. MAC address used in the matching along with the mask. See 'Mask' below for a description.
• **Mask**	This field is only available when Type is set to 'MAC/Mask'. Mask to be used in the matching along with the MAC address. This cannot be all-zeros. Suppose you want to match on a particular OUI (the three most significant bytes of a MAC address), and suppose the OUI is `00:01:C1`. In that case, you will set 'MAC' to `00:01:C1:00:00:00` and 'Mask' to `FF:FF:FF:00:00:00`. When the configuration gets saved, bits in the 'MAC' address where the corresponding 'Mask' bits are zero will be cleared automatically.

VLAN Tags

Besides the heading row, this table holds one row for outer VLAN tag matching and another for inner VLAN tag matching.

Object	Description
• **Outer/Inner**	Indicates whether this row in the table is for outer or inner VLAN tag matching.
• **Presence**	This drop-down list controls whether the VLAN tag must be present ('Required'), must not be present ('Not Allowed'), or it doesn't matter whether the frame is VLAN tagged or not ('Optional'). If the Outer VLAN Tag's presence is set to 'Not Allowed', it is not possible to set the Inner VLAN Tag's presence to 'Required', because that doesn't make sense. Only when 'Presence' is set to 'Required' will the remaining fields of the row become available.
• **Tag Type**	This field is only available when Presence is set to 'Required'. If set to 'C-tag', only frames with EtherType (TPID) 0x8100 are matched. If set to 'S-tag', only frames with EtherTYpe (TPID) 0x88a8 are matched. If set to 'Any', both frames with EtherType (TPID) 0x8100 and 0x88a8 are matched.

• **VLAN**	This field is only available when Presence is set to 'Required'. VLAN ID used in the matching along with the VLAN mask. See 'VLAN Mask' below for a description. Valid values are in the range [0-4095].
• **VLAN Mask**	This field is only available when Presence is set to 'Required'. Mask to be used in the matching along with the VLAN ID. This is shown in hexadecimal notation but both hexadecimal and decimal values can be used when editing it. A mask of all-zeros means that any VLAN ID is matched. A mask of all-ones means that only the specified VLAN ID is matched. Any mask value in the range [0x000-0xFFF] is accepted. When the configuration gets saved, bits in the 'VLAN' where the corresponding 'VLAN Mask' bits are zero will be cleared automatically.
• **PCP**	This field is only available when Presence is set to 'Required'. PCP value used in the matching along with the PCP mask. See 'PCP Mask' below for a description.
• **PCP Mask**	This field is only available when Presence is set to 'Required'. Mask to be used in the matching along with the PCP value. A mask of all-zeros means that any PCP value is matched. A mask of all-ones (0x7) means that only the specified PCP value is matched. When the configuration gets saved, bits in 'PCP' where the corresponding 'PCP Mask' bits are zero will be cleared automatically.
• **DEI**	This field is only available when Presence is set to 'Required'. If set to '0', only frames with DEI = 0 are matched. If set to '1', only frames with DEI = 1 are matched. If set to 'Any', the frame's DEI value is not used in the matching.

Protocol

This section allows for configuring properties in frames beyond VLAN tags.

Use the Type drop-down list to select what properties to configure. The following are supported:

- Any: Don't use properties beyond VLAN tags for matching
- EtherType: Match on the frame's EtherType
- LLC: Match on LLC frames
- SNAP: Match on SNAP frames
- IPv4: Match on IPv4 frames
- IPv6: Match on IPv6 frames

Each of these types (except Any) have associated configurable parametrs. These are outlined below per type.

Object	Description
• **EtherType**	A hexadecimal (or decimal) value ranging from 0x600 to 0xffff indicating the frame's EtherType, e.g. 0x800 for IPv4 (notice that IP has better matching properties than just the EtherType, so this was just an example).
• **LLC**	LLC (Logical Link Control) frames are frames with an EtherType/TypeLength field < 0x600. The LLC header carries two mandatory fields: DSAP and SSAP, whose values are used in the matching.
• **DSAP**	The one-byte Destination Service Access Point to match.
• **SSAP**	The one-byte Source Service Access Point to match.
• **SNAP**	SNAP frames are LLC frames with DSAP = 0xAA, SSAP = 0xAA and control field = 0x03. The LLC fields are implicitly matched, while the SNAP protocol fields must be explicitly configured.
• **SNAP Type**	This drop-down list holds the following selections: • RFC1042. If selected, the OUI will be set to 00:00:00 • 802.1H. If selected, the OUI will be set to 00:00:F8 • Custom. If selected, the OUI can be specified directly in the OUI field The primary purpose of providing this list of options is that people tend to forget often-used protocol OUIs. One may also simply select Custom and type e.g. the 802.1H OUI directly into the OUI field. But notice, that once this gets saved, the SNAP Type will change to 802.1H.
• **OUI**	Only when the SNAP Type is set to Custom, will this field be editable. Type the OUI you with to match on as six hexadecimal digits, but omit the colon. All six characters must be specified.
• **Protocol ID**	The SNAP header's Protocol ID (a.k.a. PID) is a 16-bit integer that can be entered as both a decimal and hexadecimal value. If SNAP Type is RFC1042, the Protocol ID must be an EtherType, that is, a value >= 0x600.
• **IPv4**	IPv4 frames are identified by hardware by having an EtherType of 0x800. With the IPv4 type, any IPv4 frame can be matched or one or more fields from the IPv4 header and (in case of UDP/TCP frames), also the UDP/TCP destination port can be matched.
• **Source IP Address**	Specify an IPv4 address in dotted decimal format to match aginst the frames' IPv4 header's SIP field.

	Only if the Source IP Prefix Length is non-zero, will the frame be matched against a source IP address.
• **Source IP Prefix Length**	Sets the number of bits in the Source IP address to match. If set to 0, no source IP matching will occur. If set to 32, all bits in the Source IP Address will be used. Otherwise, only the N first bits will be used in the matching, and the remaining bits will be cleared. The latter rule means that if you e.g. set the Source IP address to 1.2.3.4 and the Prefix Length to 16 and hit the Save button, the ".3.4" part will be cleared, so that the IP address will be shown as 1.2.0.0. Many tend to forget to set the prefix length after having specified an IP address. Therefore, if the prefix length is zero while the IP address is non-zero, a confirmation dialog will be shown asking whether this is really what the user wants.
• **Destination IP Address**	This is where you will specify the IPv4 header's DIP to match again. See Source IP Address above for details.
• **Destination IP Prefix Length**	Sets the number of bits in the Destination IP address to match. See Source IP Prefix Length for details.
• **DSCP Match**	One can choose to match on either any DSCP value, a given DSCP value, or a range of DSCP values. Which selection is chosen determines the editability of the following two inputs.
• **DSCP Minimum**	If DSCP Match is set to Value, this input determines the DSCP value to use in the matching. If DSCP Match is set to Range, this input determines the lower value in the range used in the matching. Valid values are 0-63. If DSCP Match is set to Any, this input cannot be modified.
• **DSCP Maximum**	If DSCP Match is set to Range, this input determines the higher value in the range used in the matching. Valid values are 0-63. If DSCP Match is set to Any or Value, this input cannot be modified.
• **Fragment**	If the IPv4 headers MF (More Fragments) bit is set, or the Fragment Offset is non-zero, the IPv4 frame is considered a fragment. Set this drop-down list to Any to not using the fragment info for anything in the matching Set it to No to match IPv4 frames not considered fragments. Set it to Yes to match IPv4 frames considered fragments.
• **Protocol Type**	The IPv4 header contains a one-byte Protocol field, which can be matched upon with this section. Set the drop-down list to Any to match any protocol field value.

	Set it to TCP to match on protocol field value 6. Set it to UDP to match on protocol field value 17. Set it to Custom to match on a custom protocol field value, which is input in the next field.
• **Protocol Value**	If the Protocol Type is set to Custom, this one-byte field is used to input the protocol fiel value to match against. This may also be set to the value of TCP (6) or UDP (17). Doing so and saving, causes the Protocol Type to change to the relevant value.
• **TCP/UDP Destination Port Match**	In case the Protocol Type is set to UDP or TCP, it is also possible to match on these two protocols' 16-bit destination port fields. Set the drop-down list value to Any to match all destination ports Set it to Value to match a particular destination port. Set it to Range to match a range of destination ports.
• **TCP/UDP Destination Port Minimum**	If TCP/UDP Destination Port Match is set to Value, this input determines the destination port value to use in the matching. in the matching. If it is set to Range, this input determines the lower value in the range used in the matching. Valid values are 0-65535. If The Match drop-down list is set to Any, this input cannot be modified.
• **TCP/UDP Destination Port Maximum**	If TCP/UDP Destination Port Match is set to Range, this input determines the higher value in the range used in the matching. Valid values are 0-65535. If The Match drop-down list is set to Any or Value, this input cannot be modified.
• **IPv6**	IPv6 frames are identified by hardware by having an EtherType of 0x86dd. With the IPv6 type, any IPv6 frame can be matched or one or more fields from the IPv6 header and (in case of UDP/TCP frames), also the UDP/TCP destination port can be matched.
• **Source IP Address**	Specify an IPv6 address in standard IPv6 representation notations to match aginst the frames' IPv6 header's SIP field. Only if the Source IP Prefix Length is non-zero, will the frame be matched against a source IP address.
• **Source IP Prefix Length**	Sets the number of bits in the Source IP address to match. If set to 0, no source IP matching will occur. If set to 128, all bits in the Source IP Address will be used. Otherwise, only the N first bits will be used in the matching, and the remaining bits will be cleared.The latter rule means that if you e.g. set the Source IP address to 2001:db8::1 and the Prefix Length to 64 and hit the Save button, the ::1 part will be cleared, so that the IP address will be shown as 2001:db8::

	Many tend to forget to set the prefix length after having specified an IP address. Therefore, if the prefix length is zero while the IP address is non-zero, a confirmation dialog will be shown asking whether this is really what the user wants.
• **Destination IP Address**	This is where you will specify the IPv6 header's DIP to match again. See Source IP Address above for details.
• **Destination IP Prefix Length**	Sets the number of bits in the Destination IP address to match. See Source IP Prefix Length for details.
• **DSCP Match**	One can choose to match on either any DSCP value, a given DSCP value, or a range of DSCP values. Which selection is chosen determines the editability of the following two inputs.
• **DSCP Minimum**	If DSCP Match is set to Value, this input determines the DSCP value to use in the matching. If DSCP Match is set to Range, this input determines the lower value in the range used in the matching. Valid values are 0-63. If DSCP Match is set to Any, this input cannot be modified.
• **DSCP Maximum**	If DSCP Match is set to Range, this input determines the higher value in the range used in the matching. Valid values are 0-63. If DSCP Match is set to Any or Value, this input cannot be modified.
• **Protocol Type**	The IPv6 header contains a one-byte Protocol field, which can be matched upon with this section. Set the drop-down list to Any to match any protocol field value. Set it to TCP to match on protocol field value 6. Set it to UDP to match on protocol field value 17. Set it to Custom to match on a custom protocol field value, which is input in the next field.
• **Protocol Value**	If the Protocol Type is set to Custom, this one-byte field is used to input the protocol fiel value to match against. This may also be set to the value of TCP (6) or UDP (17). Doing so and saving, causes the Protocol Type to change to the relevant value.
• **TCP/UDP Destination Port Match**	In case the Protocol Type is set to UDP or TCP, it is also possible to match on these two protocols' 16-bit destination port fields. Set the drop-down list value to Any to match all destination ports Set it to Value to match a particular destination port. Set it to Range to match a range of destination ports.
• **TCP/UDP Destination Port Minimum**	If TCP/UDP Destination Port Match is set to Value, this input determines the destination port value to use in the matching. in the matching. If it is set to Range, this input determines the lower value in the range used

	in the matching. Valid values are 0-65535. If The Match drop-down list is set to Any, this input cannot be modified.
• **TCP/UDP Destination Port Maximum**	If TCP/UDP Destination Port Match is set to Range, this input determines the higher value in the range used in the matching. Valid values are 0-65535. If The Match drop-down list is set to Any or Value, this input cannot be modified.

Port Members

Check the ports on which this stream must be instantiated. By default, no ports are included.

Hover the mouse over a given port number of checkbox to see the port number as an interface name.

Buttons

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

Back: Return to the previous page. Any changes made locally will be undone.

Refresh: Click to refresh the page immediately. Any changes made locally will be lost. This is useful if the stream configuration has been changed from e.g. CLI.

4.3.21.2 TSN Configuration

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.

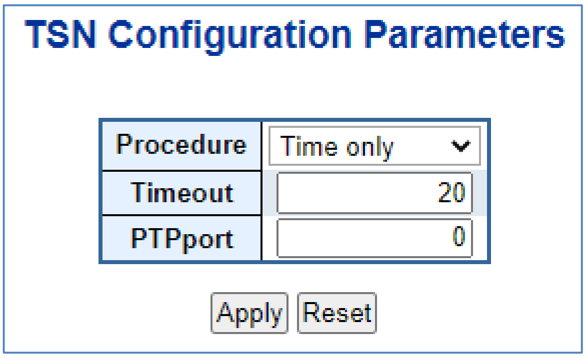


Figure 4-3-95: TSN Configuration Parameters Page Screenshot

The displayed settings are:

Object	Description
• **Procedure**	Select how to ensure PTP state
• **Timeout**	Specify the maximal number of seconds to wait before config_change is issued.
• **PTPport**	Specify the PTP port to use for sensing PTP status

Buttons

: Click to apply changes.

: Click to undo any changes made locally and revert to previously saved values.

4.3.21.3 Frame Preemption

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

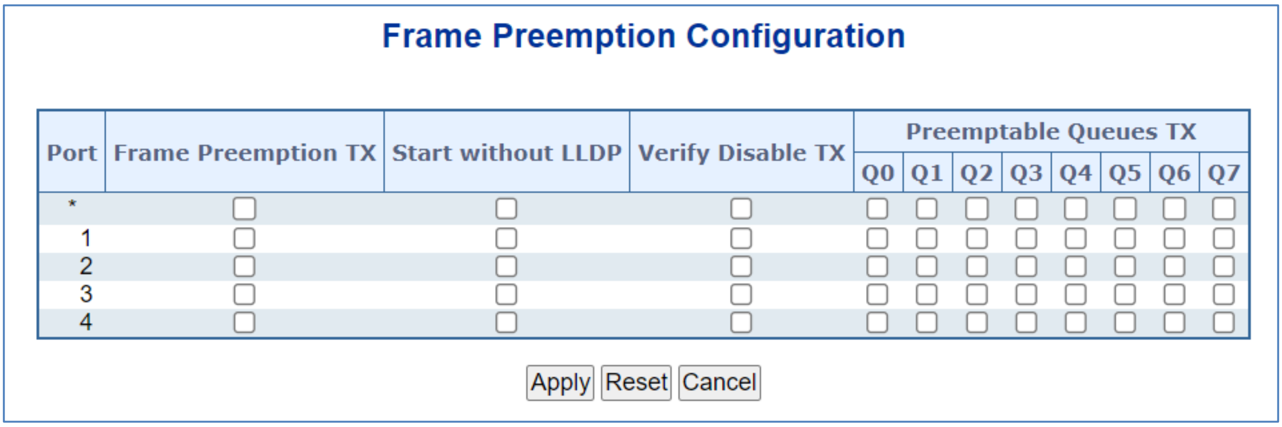


Figure 4-3-96: Frame Preemption Configuration Page Screenshot

The displayed settings are:

Object	Description
• **Port**	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**	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**	When this field is checked, Frame Preemption will be active when Frame Preemption TX is checked
• **Verify Disable TX**	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**	This parameter is the administrative value of the preemption 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.

4.3.21.4 Frame Preemption Status

This page provides an overview of TSN Egress Port Frame Preemption Status on all switch ports.

TSN Egress Port Frame Preemption Status

Auto-refresh ☐ Refresh

Port	Hold Advance	Release Advance	Preemption Active	Hold Request	Status Verify	LocPreemptsupport	LocPreemptEnabled	LocPreemptActive	LocAddFragSize
1	0	0	✗	✗	disabled	✓	✗	✓	0
2	0	0	✗	✗	indeterminate	✓	✗	✓	0
3	0	0	✗	✗	disabled	✓	✗	✓	0
4	0	0	✗	✗	disabled	✓	✗	✓	0

Figure 4-3-96: Frame Preemption Configuration Page Screenshot

The displayed settings are:

Object	Description
• **Port**	The logical port for the settings contained in the same row.
• **Hold Advance**	The value of the holdAdvance parameter for the Port in nanoseconds. There is no default value; the holdAdvance is a property of the underlying MAC.
• **Release Advance**	The value of the releaseAdvance parameter for the Port in nanoseconds. There is no default value; the releaseAdvance is a property of the underlying MAC.
• **Preemption Active**	The value is active (TRUE) when preemption is operationally active for the Port, and idle (FALSE) otherwise.
• **Hold Request**	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. The value of this object is release (FALSE) on system initialization.
• **Status Verify**	The status of the MAC Merge sublayer verification for the given device
• **LocPreemptsupport**	The value is TRUE when preemption is supported on the port, and FALSE otherwise.
• **LocPreemptEnabled**	The value is TRUE when preemption is enabled on the port, and FALSE otherwise.
• **LocPreemptActive**	The value is TRUE when preemption is operationally active on the port, and FALSE otherwise
• **LocAddFragSize**	The value of the 802.3br LocAddFragSize parameter for the port. The minimum size of non-final fragments supported by the receiver on the local port. This value is expressed in units of 64 octets of additional fragment length. The minimum non-final fragment size is: (LocAddFragSize + 1) * 64 octets.

4.3.22 TAS

4.3.22.1 Ports

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.

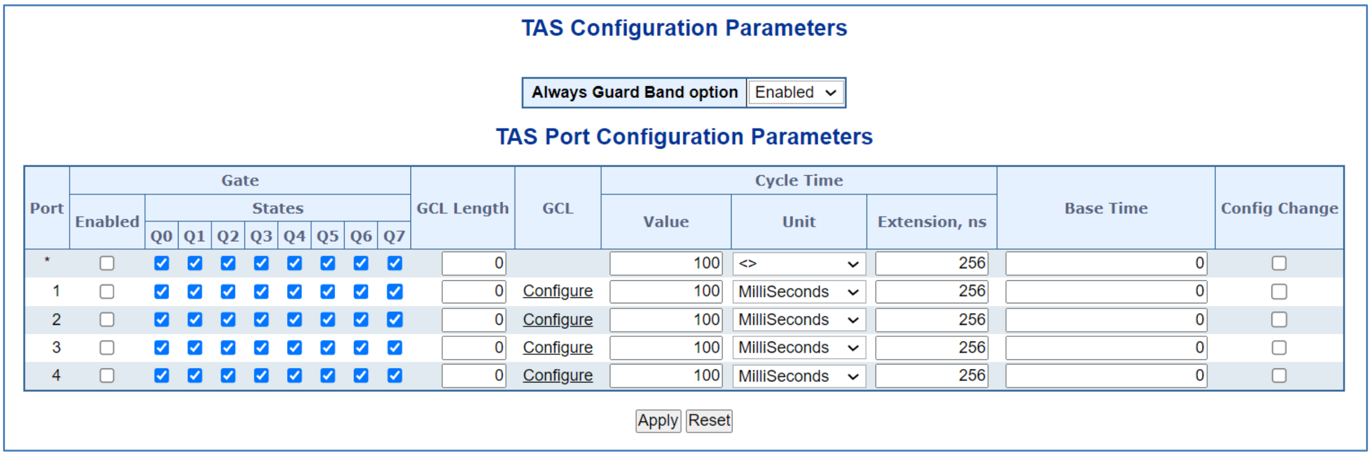


Figure 4-3-97: TAS Configuration Parameters Page Screenshot

The displayed settings are:

Object	Description
• **Always Guard Band**	The Always Guard Band option defines how the guard band values are calculated. If a Gate Control List do not contain SetAndHold and/or SetAndRelease operations the Always Guard Band option has no effect. If a Gate Control List do 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**	Port number of the switch.
• **Gate Enabled**	The Enabled parameter determines whether traffic scheduling is active (true) or inactive (false).

• **Gate States**	The initial value of the port open states that is used when no Gate Control List is active on the Port.
• **GCL Length**	The Admin Gate Control List length parameter for the Port. Valid range is 0-256. The integer value indicates the number of entries Gate Control Elements in the Gate Control List. If you change the value, press the Save button before configuring the Gate Control List by pressing the GCL link.
• **GCL**	A link to the Gate Control List parameter configuration.
• **Cycle Time**	The Admin value of the gating cycle for the Port. The Admin Cycle Time variable is a rational number of seconds, defined by value and a unit.
• **Cycle Time Value**	The Admin Cycle Time is defined by this number of units defined in the Unit field. The Admin Cycle Time is a value in the range 1-999999999, and combined with the Cycle Time Unit the value shall be in the range 256-999999999 nanoseconds. The default value is 100 milliseconds.
• **Cycle Time Unit**	The Admin Cycle Time unit. May be milliseconds, microseconds or nanoseconds.
• **Cycle Time Extension**	An integer number of nanoseconds in the range 256-999999999, 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**	The Admin value of base time, expressed as an IEEE 1588 precision time protocol (PTP) timescale.
• **Config Change**	The Configuration Change parameter signals the start of a configuration change. After a successfull 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. If Base Time is in the past, the configuration change will be executed as soon as possible. In practice it will be within approx 2 seconds, at a time which is an integral number of Cycle Time ahead of the configured value of Base Time. This way, the synchronisation between schedules in elements across a sceduled network can be maintained.

Buttons

Apply: Click to apply changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.22.2 Max SDU

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

TAS SDU Configuration

Port	Max SDU Size							
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
*	1536	1536	1536	1536	1536	1536	1536	1536
1	1536	1536	1536	1536	1536	1536	1536	1536
2	1536	1536	1536	1536	1536	1536	1536	1536
3	1536	1536	1536	1536	1536	1536	1536	1536
4	1536	1536	1536	1536	1536	1536	1536	1536

Apply Reset

Figure 4-3-98: TAS SDU Configuration Page Screenshot

The displayed settings are:

Object	Description
• **Port**	Port number of the switch.
• **Maximum SDU**	The value of the Maximum SDU size parameter for the traffic class supported by the port. This value is represented as an unsigned integer in the range 0-10240. 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.

Buttons

Apply: Click to apply changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.22.3 TAS Status

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

TAS Status Parameters

Auto-refresh ☐ Refresh

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	849	0	0	1	false	0	Status
2	✗	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	849	0	0	1	false	0	Status
3	✗	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	849	0	0	1	false	0	Status
4	✗	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	849	0	0	1	false	0	Status

Figure 4-3-99: TAS Status Parameters Page Screenshot

The displayed settings are:

Object	Description
• **Port**	Port number of the switch.
• **Oper Gate Enabled**	The Enabled parameter shows whether traffic scheduling is active (true) or inactive (false).
• **Oper Gate States**	The current state of the gate associated with each queue for the Port.
• **Cycle Time Value**	The operational value of the gating cycle for the Port. The Cycle Time variable is a rational number of seconds, defined by value and a unit.
• **Cycle Time Unit**	The operational Cycle Time unit. May be milliseconds, microseconds or nanoseconds.
• **Cycle Time Extension**	An 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**	The operational value of base time, expressed as an IEEE 1588 precision time protocol (PTP) timescale.
• **Current Time**	The current time, 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. Only the seconds are displayed.
• **Config Change Time**	The PTPtime at which the next config change is scheduled to occur. 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 Error**	A 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**	The granularity of the cycle time clock, represented as an unsigned number of tenths of nanoseconds.
• **Config Pending**	The value of the ConfigPending state machine variable. The value is TRUE if a

	configuration change is in progress but has not yet completed.
• **GCL Length**	The operational value of the gate control list length parameter for the Port. The integer value indicates the number of entries (TLVs) in the operational gate control list.
• **GCL**	A link to the GCL parameter status.

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every? seconds.

Refresh: Click to refresh the page immediately.

4.3.23 PSFP

4.3.23.1 Flow Meter

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

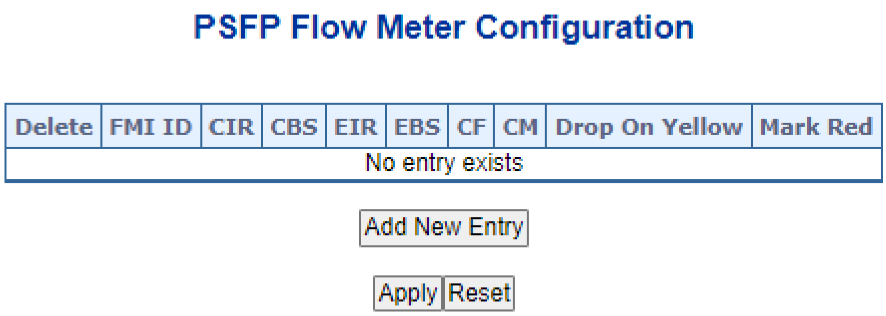


Figure 4-3-100: PSFP Flow Meter Configuration Page Screenshot

The displayed settings are:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save
• **FMI ID**	The FlowMeterInstance parameter is an index into the FlowMeterTable.
• **CIR**	The FlowMeterCIR parameter contains an integer value that represents the CIR value for the flow meter, in bit/s.
• **CBS**	The FlowMeterCBS parameter contains an integer value that represents the CBS value for the flow meter, in octets.
• **Mark RED Enable**	The FlowMeterMarkAllFramesRedEnable parameter contains a Boolean value that indicates whether the MarkAllFramesRed function is enabled (TRUE) or disabled (FALSE).
• **Mark RED**	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).

Buttons

: Click to add Flow Meter entry.

: Click to apply changes.

: Click to undo any changes made locally and revert to previously saved values.

4.3.23.2 Stream Filter

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

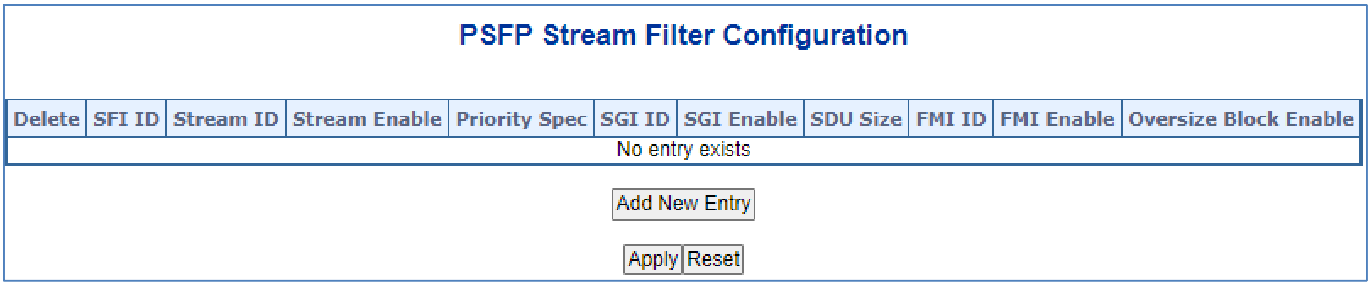


Figure 4-3-101: PSFP Stream Filter Configuration Page Screenshot

The displayed settings are:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **SFI ID**	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.
• **Priority Spec**	The Priority Spec parameter contains a priority specification value. A value of -1 denotes the wild card value; zero or positive values denote priority values.
• **Interface Spec**	The InterfaceSpec parameter contains an interface specification value. A value of VTSS_IFINDEX_NONE denotes the wild card value.
• **SGI ID**	The Stream Gate Instance parameter contains the index of an entry in the Stream Gate Table.
• **SDU Size**	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**	The FlowMeterInstanceID parameter contains the index 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.
• **Block Oversize Enable**	The StreamBlockedDueToOversizeFrameEnable object contains a Boolean value that indicates whether the StreamBlockedDueToOversizeFrame function is enabled (TRUE) or disabled (FALSE).
• **Block Oversize**	The StreamBlockedDueToOversizeFrame object contains a Boolean value that indicates whether, if the StreamBlockedDueToOversizeFrame function is enabled, all frames are to be discarded (TRUE) or not (FALSE).

Buttons

Add New Entry: Click to add Flow Meter entry.

Apply: Click to apply changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.23.3 Stream Gate

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

PSFP SGI Configuration

Delete	SGI ID	Gate		Cycle Time			Base Time	Admin IPV	GCL Length	GCL Configuration	Enable Gate-closed-due-to		Config Change
		Enabled	States	value	unit	extension					invalid-rx	octets-exceeded	
No entry exists													

Add New Entry

Apply Reset

Figure 4-3-102: PSFP SGI Configuration Page Screenshot

The displayed settings are:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **SGI ID**	The Stream Gate Instance parameter is an index into the Stream Gate Table.
• **Gate Enabled**	The Gate Enabled parameter determines whether the stream gate is active (true) or inactive (false).
• **Gate States**	The administrative value of the GateStates parameter for the stream gate. The open value indicates that the gate is open, the closed value indicates that the gate is closed.
• **Cycle Time Value**	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**	The unit used for specifying the administrative cycle time. possible values are ns, us or ms.
• **Cycle Time Extension**	The administrative value of the CycleTimeExtension parameter for the gate. The value is an unsigned integer number of nanoseconds.
• **Base Time**	The administrative value of the BaseTime parameter for the gate. The value is 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**	The administrative value of the IPV parameter for the gate. A value of -1 denotes the null value.
• **GCL Length**	The number of entries in the Gate Control List.
• **GCL Configuration**	Configuration of the Gate Control List.
• **Enable Gate-closed-due-to invalid-rx**	A Boolean value that indicates whether to close the gate if invalid data is received.
• **Enable Gate-closed-due-to octets-exceeded**	A Boolean value that indicates 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.

Buttons

Add New Entry: Click to add Flow Meter entry.

Apply: Click to apply changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.23.4 Global Parameters

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

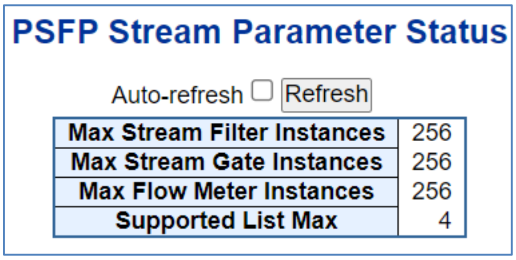


Figure 4-3-103: PSFP Stream Parameter Status Page Screenshot

The displayed settings are:

Object	Description
• **Max Stream Filter Instances**	The MaxStreamFilterInstances parameter defines the maximum number of stream filter instances that are supported by this Bridge component.
• **Max Stream Gate Instances**	The MaxStreamGateInstances parameter defines the maximum number of stream gate instances that are supported by this Bridge component.
• **Max Flow Meter Instances**	The MaxFlowMeterInstances parameter defines the maximum number of flow meter instances that are supported by this Bridge component.
• **Supported List Max**	The SupportedListMax parameter defines the The maximum value supported by this Bridge component of the AdminControlListLength and OperControlListLength parameters.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4.3.23.5 Stream Filter Status

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

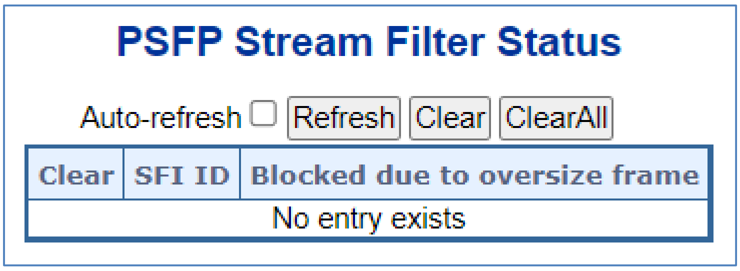


Figure 4-3-104: PSFP Stream Filter Status Page Screenshot

The displayed settings are:

Object	Description
• **Clear**	This box is used to mark an entry for clearance in next Clear operation.
• **SFI ID**	The id of the stream filter instance.
• **Blocked due to oversize frame**	True if the filter has been blocked due to an oversize frame, otherwise false

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every? seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the blocked flag for selected entries.

Clear All: Clears the blocked flag for all entries.

4.3.23.6 Stream Filter Statistics

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

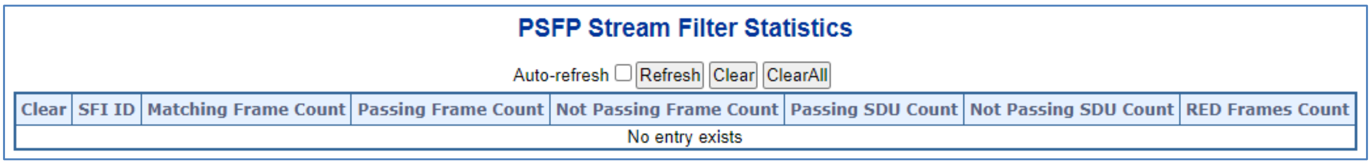


Figure 4-3-105: PSFP Stream Filter Statistics Page Screenshot

The displayed settings are:

Object	Description
• **Clear**	This box is used to mark an entry for clearance in next Clear operation.
• **SFI ID**	The MaxStreamFilterInstances parameter defines the maximum number of stream filter instances that are supported by this Bridge component.
• **Matching Frame Count**	The MatchingFramesCount counter counts received frames that match this stream filter.
• **Passing Frame Count**	The PassingFramesCount counter counts received frames that pass the gate associated with this stream filter.
• **Not Passing Frame Count**	The NotPassingFramesCount counter counts received frames that do not pass the gate associated with this stream filter.
• **Passing SDU Count**	The PassingSDUCount counter counts received frames that pass the SDU size filter specification associated with this stream filter.
• **Not Passing SDU Count**	The NotPassingSDUCount counter counts received frames that do not pass the SDU size filter specification associated with this stream filter.
• **RED Frames Count**	The REDFramesCount counter counts received random early detection (RED) frames associated with this stream filter.

Buttons

Auto-refresh ☐:: Check this box to refresh the page automatically. Automatic refresh occurs every? seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the blocked flag for selected entries.

Clear All: Clears the blocked flag for all entries.

4.3.23.7 Stream Gate Status

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

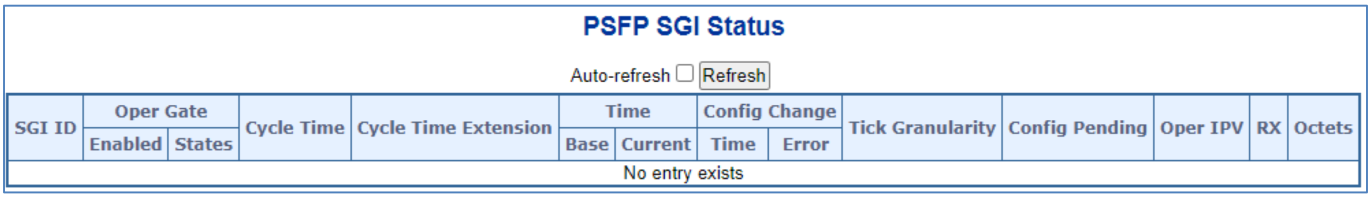


Figure 4-3-106: PSFP SGI Status Page Screenshot

The displayed settings are:

Object	Description
• **SGI ID**	The Stream Gate Instance parameter is an index into the Stream Gate Table.
• **Oper Gate Enabled**	The Gate Enabled parameter determines whether the stream gate is active (true) or inactive (false).
• **Oper Gate States**	The operational value of the GateStates parameter for the stream gate. The open value indicates that the gate is open, the closed value indicates that the gate is closed.
• **Cycle Time Numerator**	The operational value of the numerator of the CycleTime parameter for the gate. The numerator and denominator together represent the cycle time as a rational number of seconds.
• **Cycle Time Denominator**	The operational value of the denominator of the CycleTime parameter for the gate. The numerator and denominator together represent the cycle time as a rational number of seconds.
• **Cycle Time Extension**	The operational value of the CycleTimeExtension parameter for the gate. The value is an unsigned integer number of nanoseconds.
• **Base Time**	The operational value of the BaseTime parameter for the gate. 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**	The current time, 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. Only the seconds are displayed.
• **Config Change Time**	The PTPtime at which the next config change is scheduled to occur. 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 Error**	A 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**	The granularity of the cycle time clock, represented as an unsigned number of

	tenths of nanoseconds.
• **Config Pending**	The value of the ConfigPending state machine variable. The value is TRUE if a configuration change is in progress but has not yet completed.
• **Oper IPV**	The operational value of the IPV parameter for the gate. A value of -1 denotes the null value.
• **GCL Length**	The operational value of the ListMax parameter for the gate. The integer value indicates the number of entries (TLVs) in the operControlList.
• **GCL Status**	A link to the GCL parameter status.

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every? seconds.

Refresh: Click to refresh the page immediately.

4.3.23.8 Frame Preemption

This page provides an overview of TSN Egress Port Frame Preemption Status on all switch ports.

TSN Egress Port Frame Preemption Status

Auto-refresh ☐ Refresh

Port	Hold Advance	Release Advance	Preemption Active	Hold Request	Status Verify	LocPreemptsupport	LocPreemptEnabled	LocPreemptActive	LocAddFragSize
1	0	0	✗	✗	indeterminate	✓	✗	✓	0
2	0	0	✗	✗	indeterminate	✓	✗	✓	0
3	0	0	✗	✗	disabled	✓	✗	✓	0
4	0	0	✗	✗	disabled	✓	✗	✓	0

Figure 4-3-107: TSN Egress Port Frame Preemption Status Page Screenshot

The displayed settings are:

Object	Description
• **Port**	The logical port for the settings contained in the same row.
• **Hold Advance**	The value of the holdAdvance parameter for the Port in nanoseconds. There is no default value; the holdAdvance is a property of the underlying MAC.
• **Release Advance**	The value of the releaseAdvance parameter for the Port in nanoseconds. There is no default value; the releaseAdvance is a property of the underlying MAC.
• **Preemption Active**	The value is active (TRUE) when preemption is operationally active for the Port, and idle (FALSE) otherwise.
• **Hold Request**	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. The value of this object is release (FALSE) on system initialization.
• **Status Verify**	The status of the MAC Merge sublayer verification for the given device.
• **LocPreemptsupport**	The value is TRUE when preemption is supported on the port, and FALSE otherwise.
• **LocPreemptEnabled**	The value is TRUE when preemption is enabled on the port, and FALSE otherwise.
• **LocPreemptActive**	The value is TRUE when preemption is operationally active on the port, and FALSE otherwise.
• **LocAddFragSize**	The value of the 802.3br LocAddFragSize parameter for the port. The minimum size of non-final fragments supported by the receiver on the local port. This value is expressed in units of 64 octets of additional fragment length. The minimum non-final fragment size is: (LocAddFragSize + 1) * 64 octets.

4.3.24 FRER

4.3.24.1 FRER Configuration

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

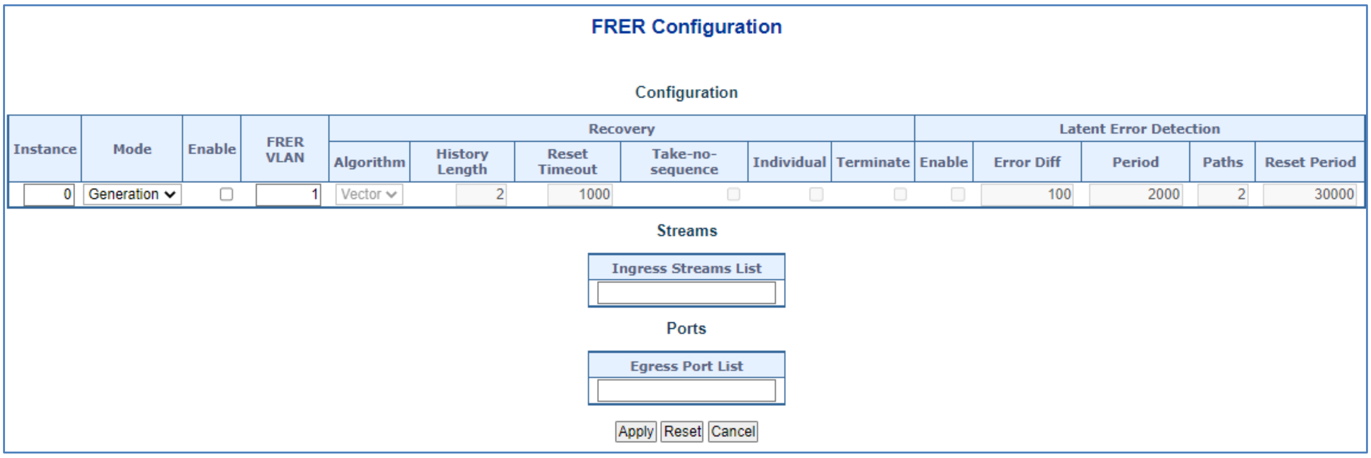


Figure 4-3-108: FRER Configuration Page Screenshot

The displayed settings are:

Object	Description
• **Mode**	Decides if this FRER instance shall run in generation or recovery mode. Default is generation.
• **Enable**	Enable or disable a FRER instance.
• **FRER VLAN**	Select the VLAN ID that ingress flows get classified to.
• **Algorithm**	IEEE 802.1CB-2017 requires implementations to provide two different recovery function algorithms, match and vector. match is the simplest algorithm: It basically says: Discard all packets with a sequence number equal to the last sequence number seen. Accept all others. The algorithm also comes with a reset timer that - when it expires - causes the algorithm to accept any sequence number - even the same as the previous. The reset timer is restarted every time a packet is accepted. The match algorithm counts the number of times the reset timer has expired and the number of passed, discarded, and out-of-order packets. Out-of-order happens when the sequence number of a given packet is not one higher than the previous (and the timer has not expired). vector is somewhat more complicated. When a packet with a given sequence number arrives, it must be within the previous accepted packets sequence number +/- a configurable history length, or it will be discarded. If the packet is

	already seen (within the history length window), it is also discarded. Also this algorithm comes with a reset timer that - when it expires - causes the algorithm to accept any sequence number next time a packet arrives. The reset timer is restarted every time a packet is accepted. The vector algorithm counts the number of times the reset timer has expired and the number of passed, discarded, out-of-order, and so-called rogue packets. Out-of-order happens when the sequence number of a given packet is "older" than a previous packets (taking wrap-around into account), and the packet has not been accepted before. Out-of-order packets are accepted. Rogue packets are packets with a sequence number beyond the history length window. Rogue packets are also counted as discarded. Furthermore, the vector algorithm counts lost packets, that is, the number of unreceived sequence numbers when the history window moves. Both algorithms also counts the number of packets arriving without an R-tag. This is done with the tagless counter. By default, such packets will be discarded. A per-FRER instance parameter recovery take-no-sequence, however, allows such frames to pass through. Notice: The 802.1CB standard utilizes the frerSeqRcvyTakeNoSequence only in the vector algorithm, but the switches that the present guide is meant for also utilizes it in the match algorithm. Notice: This feature should only be used on terminating switches, because such tagless packets will be R-tagged (with sequence number 0) on their way out on non-terminating switches. The selected algorithm on a given FRER instance will be used in both compound and individual recovery functions. Default is the vector algorithm.
• **History Length**	Configure the recvery functions history length. Valid range is 2-32 and default is 2.
• **Reset Timeout**	Configure recovery function's reset timeout in milliseconds. Valid range is 1-4095 and default is 1000.
• **Take-no-sequence**	Select this option to accept all frames whether they are R-tagged or not.
• **Individual**	Individual recovery means that a member stream undergoes recovery before it reaches the compound recovery function. The compound recovery function sits on each and every egress port in the FRER instance. The one and only thing that individual recovery can do that compound recovery can not is to filter out member streams that keep presenting the same R-tag sequence number because of a defect transmitter. It goes like this:

	Suppose the transmitter of member stream 1 is working perfectly. It will send out frames with an increasing sequence number and wrap back to 0 after 65535 frames. Suppose the transmitter of member stream 2 is sending out the same frame with the same sequence number, X, over and over again. If we only had a compound recovery function, that function would at times be presented with frames with sequence number X from stream 1 and sequence number X from stream 2, and the first of these two frames would be sent to the egress port. So - depending on timing - sometimes the frame with sequence number X would come from stream 1 and sometimes it would come from the erroneous stream 2. The effect of enabling individual recovery is to have the individual recovery function for stream 2 filter out all identically numbered frames before they are presented to the compound recovery function. This is a very unlikely situation, and most network administrators will not need individual recovery. Moreover, individual recovery is very expensive in terms of hardware resources: Every ingress stream needs an individual recovery function per egress port. So if a FRER instance defines 8 ingress streams and 8 egress ports, the switch needs 64 individual recovery instances - just for this one FRER instance.
• **Terminate**	Select this option to strip an R-Tag from a frame before presenting it on egress.

• **Latent Error Detection**	The purpose of latent error detection is to raise a flag if the number of discarded packets is "relatively few" compared to the number of passed packets. The algorithm relies on four user inputs:
	
	Period, Reset period, Paths, Error difference.
	
	The reset function algorithm is as follows: Every Reset period milliseconds, read number of passed and discarded packet counters, and set a per-FRER instance variable, CurDiff, as follows:
	
	CurDiff = passed_packets * (paths - 1) - discarded_packets;
	
	The test function algorithm is as follows: Every timeout milliseconds, read the discarded and passed packet counters, and perform the following:
	
	diff = Abs(CurDiff - (passed_packets * (paths - 1) - discarded_packets));
	
	if (diff > difference) {
	raise_flag();

	} Basically, it says: If you expect N member streams to ingress this FRER instance, N-1 of these member streams are expected to be discarded, and only one is expected to pass. To allow for some slack due to random packet losses and the fact that counters are not neccessarily read simultaneously, set the difference to account for that. The reset function makes sure that CurDiff is updated to avoid that occassional packet losses do not accumulate forever.
• **Latent Error Detection, Enable**	Enable/disable Latent error detection.
• **Latent Error Detection, Error Diff**	The number of packets "allowed" to be in difference without raising the flag. Valid range is 0-10000000 and default is 100.
• **Latent Error Detection, Period**	The number of milliseconds between invoking the test function. Valid range is 1000-86400000 and default is 2000.
• **Latent Error Detection, Paths**	The number of member streams expected to ingress this FRER instance. Valid range is 2-8 and default is 2.
• **Latent Error Detection, Reset period**	The number of milliseconds between invoking the reset function. Valid range is 1000-86400000 and default is 30000.
• **Ingress streams list**	Select the ingress streams that should map to this FRER instance. Only one stream ID can be specified in generator mode. There is a maximum limit of 8 ingress streams.
• **Egress port list**	Select egress ports that this FRER instance will hit. There is a maximum of 8 egress ports pr. FRER instance.

Buttons

Apply: Click to apply changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Cancel: Return to the previous page; any changes made locally will be undone.

4.3.24.2 FRER Status

This page allows the user to inspect the current FRER status, and possibly reset/clear them as well.

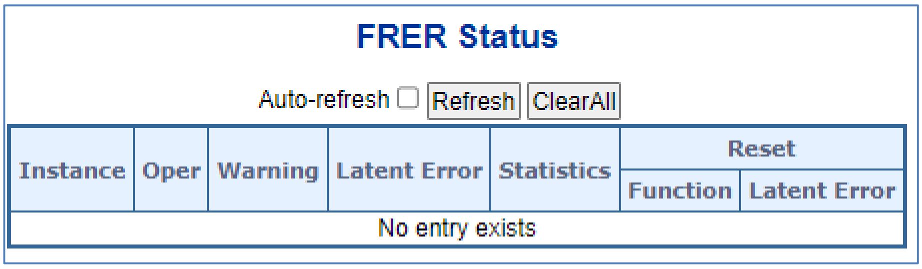


Figure 4-3-109: FRER Status Page Screenshot

The displayed settings are:

Object	Description
• **Instance**	The id of the FRER instance.
• **Oper**	The operational state of FRER instance. : Active. : Disabled or Internal error.
• **Warning**	Operational warnings of FRER instance. : No warnings. : There are warnings, use tooltip to see.
• **Latent Error**	: No errors. : There are latent errors.
• **Statistics**	Check to reset statistics counters.
• **Reset Function**	Click to perform function reset. 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**	Clich to clear a sticky latent error.

Buttons

Auto-refresh :: Check this box to refresh the page automatically. Automatic refresh occurs every? seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the blocked flag for selected entries.

Clear All: Clears the blocked flag for all entries.

4.3.24.3 FRER Statistics

This page allows the user to inspect the current FRER statistics counters, and possibly clear them as well.

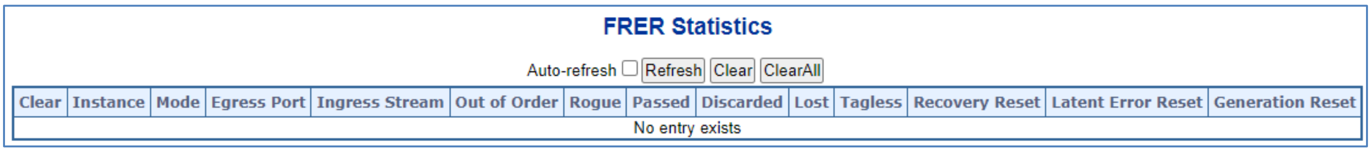


Figure 4-3-110: FRER Statistics Page Screenshot

The displayed settings are:

Object	Description
• **Clear**	This box is used to mark an entry for clearance in next Clear operation.
• **Instance**	The FRER instance id.
• **Mode**	Mode of operation. Generation or Recovery.
• **Egress Port**	List of egress port numbers.
• **Ingress Stream**	List of Ingress stream Ids.
• **Out of order**	IEEE 802.1CB-2017: frerCpsSeqRcvyOutOfOrderPackets.
• **Rogue**	IEEE 802.1CB-2017: frerCpsSeqRcvyRoguePackets.
• **Passed**	IEEE 802.1CB-2017: frerCpsSeqRcvyPassedPackets.
• **Discarded**	IEEE 802.1CB-2017: frerCpsSeqRcvyDiscardedPackets.
• **Lost**	IEEE 802.1CB-2017: frerCpsSeqRcvyLostPackets.
• **Tagless**	IEEE 802.1CB-2017: frerCpsSeqRcvyTaglessPackets.
• **Recovery resets**	IEEE 802.1CB-2017: frerCpsSeqRcvyResets.
• **Latent error resets**	IEEE 802.1CB-2017: frerCpsSeqRcvyLatentErrorResets.
• **Generation resets**	IEEE 802.1CB-2017: frerCpsSeqGenResets.

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically.

Refresh: Click to refresh the page immediately.

Clear: Clears the blocked flag for selected entries.

Clear All: Clears the blocked flag for all entries.

4.3.25 SyncE

4.3.25.1 SyncE Configuration

This page allows the user to inspect and configure the current SyncE port settings. For each possible clock source the following can be configured.

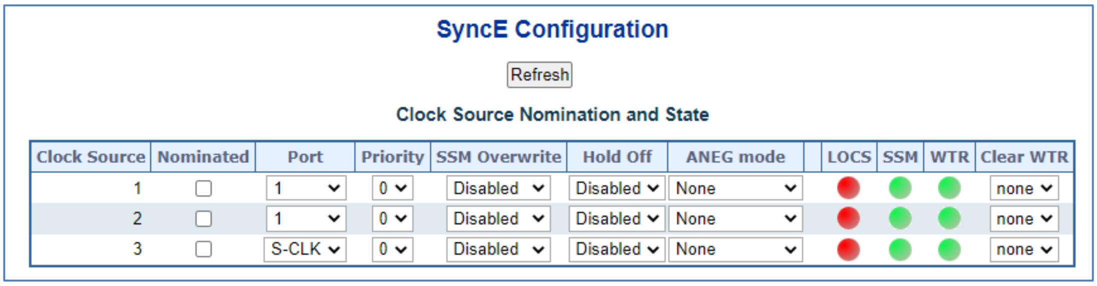


Figure 4-3-111: SyncE Configuration Page Screenshot

The displayed settings are:

Object	Description
• **Clock Source**	This is the instance number of the clock source. This has to be referenced when selecting 'Manual' Mode
• **Nominated**	When a clock source is nominated, the clock output from the related PHY (Port) is enabled against the clock controller. This makes it available as a possible source in the clock selection process. If it is supported by the actual HW configuration, The Station clock input can be nominated as a Clock Source.
• **Port**	In this drop down box, the ports that are possible to select for this clock source, is presented. The PCB104 Synce module supports 10MHz station clock input. The station clock input is indicated by a port name = 'S-CLK'. The serval1 has a limitation that chip port 1 cannot be nominated as source 1. On the Vitesse boards this is port 7 (interface gi 1/7). Serval2 NID board limitations: Port 5-12 can be configured for 100M, 1G or 2.5G speed. In 2.5G speed mode the SyncE hardware is not able to lock, because the recovered clock output frequency does not match the SyncE hardware's frequency options.
• **Priority**	The priority for this clock source. Lowest number (0) is the highest priority. If two clock sources has the same priority, the lowest clock source number gets the highest priority in the clock selection process.
• **SSM Overwrite**	A selectable clock source Quality Level (QL) to overwrite any QL received in a SSM. If QL is not Received in a SSM (SSM is not enabled on this port), the SSM Overwrite QL is used as if received. The SSM Overwrite can be set to QL_NONE, indicating that the clock source is without any know quality (Lowest compared to clock source with known quality)

• **Hold Off**	The Hold Off timer value. Active loss of clock Source will be delayed the selected amount of time. The clock selector will not change clock source if the loss of clock condition is cleared within this time
• **ANEG Mode**	This is relevant for 1000BaseT ports only. In order to recover clock from port it must be negotiated to 'Slave' mode. In order to distribute clock the port must be negotiated to 'Master' mode. This different ANEG modes can be activated on a Clock Source port: Prefer Slave: The Port will be negotiated to 'Slave' mode if possible. Prefer Master: The Port will be negotiated to 'Master' mode if possible. Forced Slave: The Port will be forced to 'Slave' mode. The selected port in 'Locked' state will always be negotiated to 'Slave' if possible.
• **LOCS**	Signal is lost on this clock source.
• **SSM**	If SSM is enabled and not received properly. Type of SSM fail will be indicated in the 'Rx SSM' field
• **WTR**	Wait To Restore timer is active.
• **Clear WTR**	Clears the WTR timer and makes this clock source available to the clock selection process.

The Clock Selector is only in one instance - the one who selects between the nominated clock sources.

Clock Selection Mode and State

Mode	Source	WTR Time	SSM Hold Over	SSM Free Run	EEC Option		State	Clock Source	LOL	DHOLD
Auto Revertive	1	5M	Disabled	Disabled	1		Free Run			

The displayed settings are:

Object	Description
• **Mode**	The definition of the 'best' clock source is firstly the one with the highest (QL) and secondly (the ones with equal QL) the highest priority. Clock Selector can be in different modes: Manual: Clock selector will select the clock source stated in Source (see below). If this manually selected clock source is failing, the clock selector will go into holdover state. Manual To Selected: Same as Manual mode where the pt. selected clock source will become Source.

	Auto NonRevertive: Clock Selection of the best clock source is only done when the selected clock fails. Auto Revertive: Clock Selection of the best clock source is constantly done. Force Hold Over: Clock Selector is forced to Hold Over State. Force Free Run: Clock Selector is forced to Free Run State.
• **Source**	Only relevant if Manual mode is selected (see above).
• **WTR Time**	WTR is the Wait To Restore timer value in minutes. The WTR time is activated on the falling edge of a clock source failure (in Revertive mode). This means that the clock source is first available for clock selection after WTR Time (can be cleared).
• **SSM Hold Over**	This is the transmitted SSM QL value when clock selector is in Hold Over State.
• **SSM Free Run**	This is the transmitted SSM QL value when clock selector is in Free Run State.
• **EEC Option**	The ZL30xxx based Synce modules support both EEC1 and EEC2 option. The difference is: EEC1=> DPLL bandwidth=3,5 Hz, EEC2=> DPLL bandwidth = 0,1 Hz.
• **State**	This is indicating the state of the clock selector. Possible states are:. Free Run: There is no external clock sources to lock to (unlocked state). The Clock Selector has never been locked to a clock source long enough to calculate the hold over frequency offset to local oscillator. The frequency of this node is the frequency of the local oscillator. Hold Over: There is no external clock sources to lock to (unlocked state). The Clock Selector has calculate the holdover frequency offset to local oscillator. The frequency of this node is hold to the frequency of the clock source previous locked to. Locked: Clock selector is locked to the clock source indicated (See next). Top: Clock selector is locked to Time over packets, e.g. PTP (See next).
• **Clock Source**	The clock source locked to when clock selector is in locked state.
• **LOL**	Clock selector has raised the Los Of Lock alarm.
• **DHOLD**	Clock selector has not yet calculated the holdover frequency offset to local oscillator. This becomes active for about 10 s. when a new clock source is selected

The Synce module may have a Station Clock hardware.

Station Clock hardware

Clock hardware id	Clock F/W version
ZL 30772	1770

Apply Reset

For each possible port on switch.

SyncE Ports

Port	SSM Enable	Tx SSM	Rx SSM	1000BaseT Mode
*	☐			
1	☐			Slave
2	☐			Slave
3	☐			Slave
4	☐			Master

PTP Ports (8265.1)

Instance	Rx SSM	PTSF
1	QL NONE	None
2	QL NONE	None
3	QL NONE	None

The displayed settings are:

Object	Description
• **Port**	The port number to configure.
• **SSM Enable**	Enable and disable of SSM functionality on this port.
• **Tx SSM**	Monitoring of the transmitted SSM QL on this port. Transmitted QL should be the Quality Level of the clock generated by this node. This means the QL of the clock source this node is locked to
• **Rx SSM**	Monitoring of the received SSM QL on this port. If link is down on port, QL_LINK is indicated. If no SSM is received, QL_FAIL is indicated
• **1000BaseT Mode**	If PHY is in 1000BaseT Mode then this is monitoring the master/slave mode. In order to receive clock on a port, it has to be in slave mode. In order to transmit clock on a port, it has to be in master mode

Buttons

Refresh: Click to refresh the page immediately.

Apply: Click to apply changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.4 QoS

4.4.1 General

Quality of Service (QoS) is an advanced traffic prioritization feature that allows you to establish control over network traffic. QoS enables you to assign various grades of network service to different types of traffic, such as multi-media, video, protocol-specific, time critical, and file-backup traffic.

QoS reduces bandwidth limitations, delay, loss, and jitter. It also provides increased reliability for delivery of your data and allows you to prioritize certain applications across your network. You can define exactly how you want the switch to treat selected applications and types of traffic. You can use QoS on your system to:

- Control a wide variety of network traffic by:
- Classifying traffic based on packet attributes.
- Assigning priorities to traffic (for example, to set higher priorities to time-critical or business-critical applications).
- Applying security policy through traffic filtering.
- Provide predictable throughput for multimedia applications such as video conferencing or voice over IP by minimizing delay and jitter.
- Improve performance for specific types of traffic and preserve performance as the amount of traffic grows.
- Reduce the need to constantly add bandwidth to the network.
- Manage network congestion.

QoS Terminology

- **Classifier**—classifies the traffic on the network. Traffic classifications are determined by protocol, application, source, destination, and so on. You can create and modify classifications. The Switch then groups classified traffic in order to schedule them with the appropriate service level.
- **DiffServ Code Point (DSCP)** — is the traffic prioritization bits within an IP header that are encoded by certain applications and/or devices to indicate the level of service required by the packet across a network.
- **Service Level**—defines the priority that will be given to a set of classified traffic. You can create and modify service levels.
- **Policy**—comprises a set of "rules" that are applied to a network so that a network meets the needs of the business. That is, traffic can be prioritized across a network according to its importance to that particular business type.
- **QoS Profile**—consists of multiple sets of rules (classifier plus service level combinations). The QoS profile is assigned to a port(s).
- **Rules**—comprises a service level and a classifier to define how the Switch will treat certain types of traffic. Rules are associated with a QoS Profile (see above).

To implement QoS on your network, you need to carry out the following actions:

1. Define a service level to determine the priority that will be applied to traffic.
2. Apply a classifier to determine how the incoming traffic will be classified and thus treated by the Switch.
3. Create a QoS profile which associates a service level and a classifier.
4. Apply a QoS profile to a port(s).

4.4.1.1 Port Classification

This page allows you to configure the basic QoS Classification settings for all switch ports. The Port classification screen in Figure 4-4-1 appears.

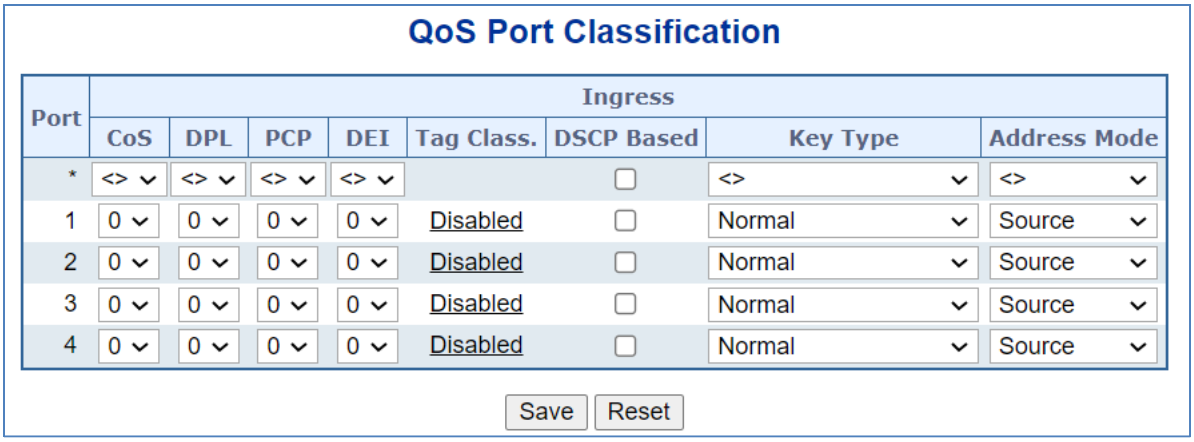


Figure 4-4-1: QoS Ingress Port Policers Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The port number for which the configuration below applies.
• **CoS**	Controls 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. The classified CoS can be overruled by a QCL entry. **Note:** If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.
• **DPL**	Controls the default DPL value. All frames are classified to a Drop Precedence Level. The classified DPL can be overruled by a QCL entry.
• **PCP**	Controls 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**	Controls 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.
• **Tag Class.**	Shows the classification mode for tagged frames on this port. **Disabled**: Use default CoS and DPL for tagged frames. **Enabled**: Use mapped versions of PCP and DEI for tagged frames. Click on the mode in order to configure the mode and/or mapping. **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 DSCP Based QoS Ingress Port Classification.
• **Key Type**	The key type specifying the key generated for frames received on the port. The allowed values are: `Normal`: Half key, match outer tag, SIP/DIP and SMAC/DMAC. `Double Tag`: Quarter key, match inner and outer tag. `IP Address`: Half key, match inner and outer tag, SIP and DIP. For non-IP frames, match outer tag only. `MAC and IP Address`: Full key, match inner and outer tag, SMAC, DMAC, SIP and DIP. Filtering on DMAC type (unicast/multicast/broadcast) is supported for any key type.
• **Address Mode**	The IP/MAC address mode specifying whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. This parameter is only used when the key type is `Normal`. The allowed values are: `Source`: Enable SMAC/SIP matching. `Destination`: Enable DMAC/DIP matching.

Buttons

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.4.1.2 Queue Policing

This page allows you to configure the Queue Policer settings for all switch ports.. The Queue Policing screen in Figure 4-4-2 appears.

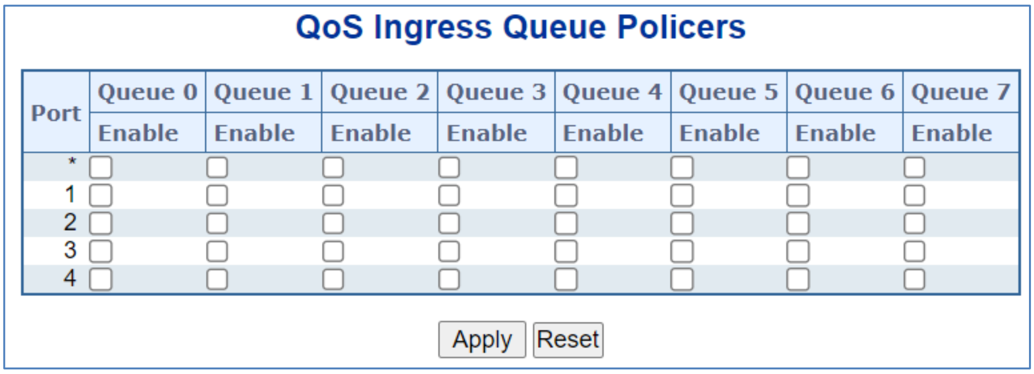


Figure 4-4-2 : QoS Ingress Port Classification Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The port number for which the configuration below applies.
• **Enable (E)**	Enable or disable the queue policer for this switch port.
• **Rate**	Controls the rate for the queue policer. This value is restricted to 25-13128147 when "Unit" is kbps, and 1-13128 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue policer. This field is only shown if at least one of the queue policers are enabled.
• **Unit**	Controls the unit of measure for the queue policer rate as kbps or Mbps. This field is only shown if at least one of the queue policers are enabled.

Buttons

: Click to apply changes

: Click to undo any changes made locally and revert to previously saved values.

4.4.1.3 Port Tag Remarking

This page provides an overview of QoS Egress Port Tag Remarking for all switch ports. The Port tag remarking screen in Figure 4-4-3 appears.

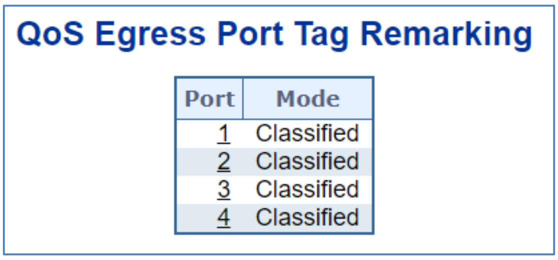


Figure 4-4-3: Port Tag Remarking Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	he logical port for the settings contained in the same row. Click on the port number in order 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.

4.4.1.4 WERD

This page allows you to configure the Random Early Detection (RED) settings.. The Port Shaper screen in Figure 4-4-4 appears.

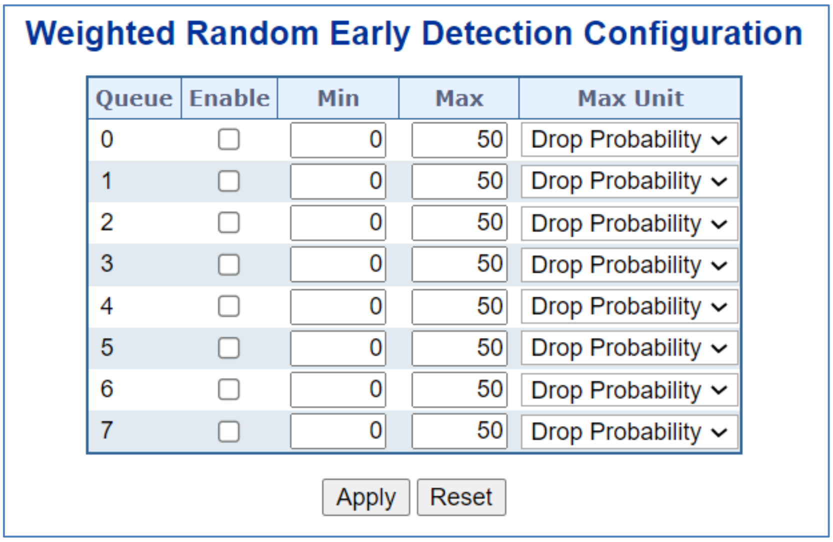


Figure 4-4-4: QoS Egress Port Shapers Page Screenshot

The page includes the following fields:

Object	Description
• **Queue**	The queue number (CoS) for which the configuration below applies.
• **Enable**	Controls whether RED is enabled for this entry.
• **Min**	Controls the lower RED fill level threshold. If the queue filling level is below this threshold, the drop probability is zero. This value is restricted to 0-100%.
• **Max**	Controls the upper RED drop probability or fill level threshold for frames marked with Drop Precedence Level > 0 (yellow frames). This value is restricted to 1-100%.
• **Max Unit**	Selects the unit for Max. Possible values are: **Drop Probability**: Max controls the drop probability just below 100% fill level. **Fill Level**: Max controls the fill level where drop probability reaches 100%..

Buttons

: Click to apply changes

: Click to undo any changes made locally and revert to previously saved values.

4.4.1.5 Statistics

This page provides statistics for the different queues for all switch ports. The statistice screen in Figure 4-4-5 appears.

Queuing Counters

Auto-refresh ☐ Refresh Clear

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	332983	6304	0	0	0	0	0	0	0	0	0	0	0	0	0	6694
4	6991	280741	0	0	0	0	0	0	0	0	0	0	0	0	0	36765

Figure 4-4-5: QoS statistics Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The logical port for the settings contained in the same row.
• **Qn**	There are 8 QoS queues per port. Q0 is the lowest priority queue.
• **Rx/Tx**	The number of received and transmitted packets per queue.

Buttons

Refresh : Click to refresh the page immediately.

Clear :Clears the counters for all ports

4.4.2 Bandwidth Control

4.4.2.1 Port Policing

This page allows you to configure the Policer settings for all switch ports. The Port Policing screen in Figure 4-4-6 appears.

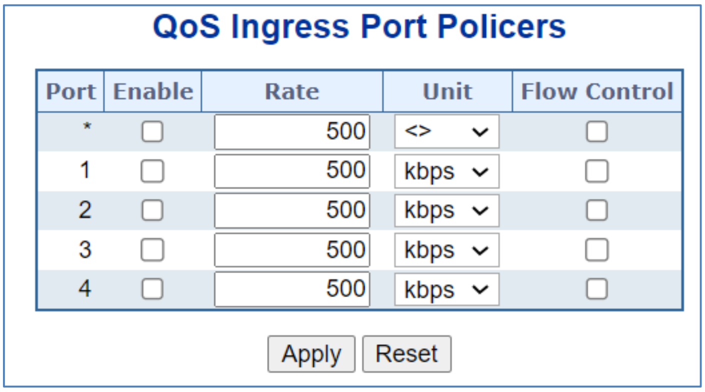


Figure 4-4-6: QoS Ingress Port Policers Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The port number for which the configuration below applies.
• **Enable**	Controls whether the policer is enabled on this switch port.
• **Rate**	Controls the rate for the policer. This value is restricted to 100-1000000 when the "Unit" is "**kbps**" or "**fps**", and it is restricted to 1-3300 when the "Unit" is "**Mbps**" or "**kfps**". The default value is **500**.
• **Unit**	Controls the unit of measure for the policer rate as **kbps**, **Mbps**, **fps** or **kfps** . The default value is "**kbps**".
• **Flow Control**	If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

Buttons

: Click to apply changes

: Click to undo any changes made locally and revert to previously saved values.

4.4.2.2 Port Scheduler

The Port Scheduler and Shapers for a specific port are configured on this page. The QoS Egress Port Schedule and Shaper screen in Figure 4-4-7 appears.

QoS Egress Port Schedulers

Port	Mode	Weight							
		Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
1	Strict Priority	-	-	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-	-	-

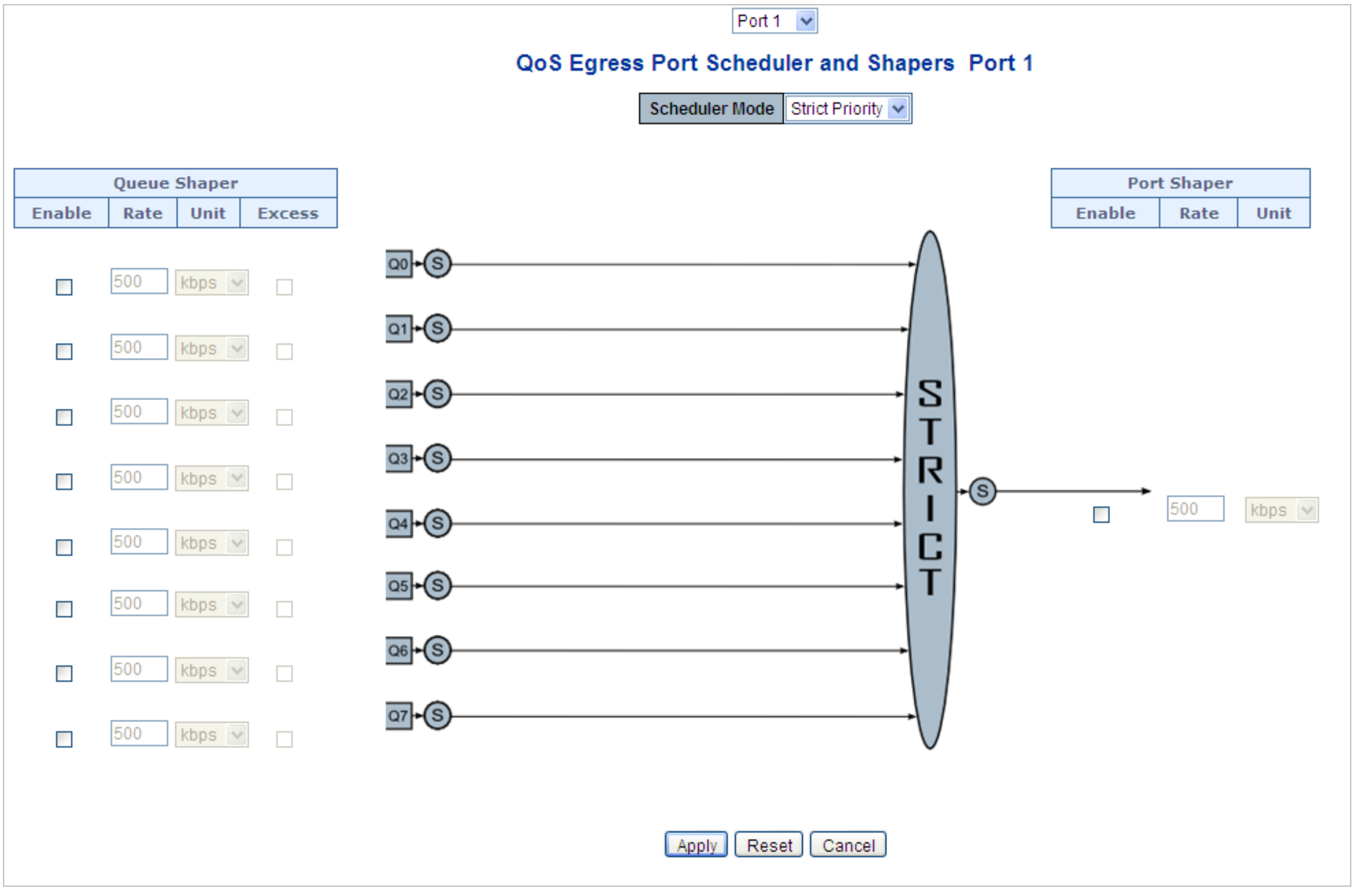


Figure 4-4-7: QoS Egress Port Schedule and Shapers Page Screenshot

The page includes the following fields:

Object	Description
• **Schedule Mode**	Controls whether the scheduler mode is "**Strict Priority**" or "**Weighted**" on this switch port.
• **Queue Shaper Enable**	Controls whether the queue shaper is enabled for this queue on this switch port.
• **Queue Shaper Rate**	Controls the rate for the queue shaper. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps". The default value is **500**.
• **Queue Shaper Unit**	Controls the unit of measure for the queue shaper rate as "**kbps**" or "**Mbps**". The default value is "kbps".
• **Queue Shaper Excess**	Controls whether the queue is allowed to use excess bandwidth.
• **Queue Scheduler Weight**	Controls the weight for this queue. This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "**Weighted**". The default value is "**17**".
• **Queue Scheduler Percent**	Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".
• **Port Shaper Enable**	Controls whether the port shaper is enabled for this switch port.
• **Port Shaper Rate**	Controls the rate for the port shaper. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps". The default value is 500.
• **Port Shaper Unit**	Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

Buttons

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

Cancel: Click to undo any changes made locally and return to the previous page.

4.4.2.3 Port Shaping

This page provides an overview of QoS Egress Port Shapers for all switch ports.. The Port shaping screen in Figure 4-4-8 appears.

QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-

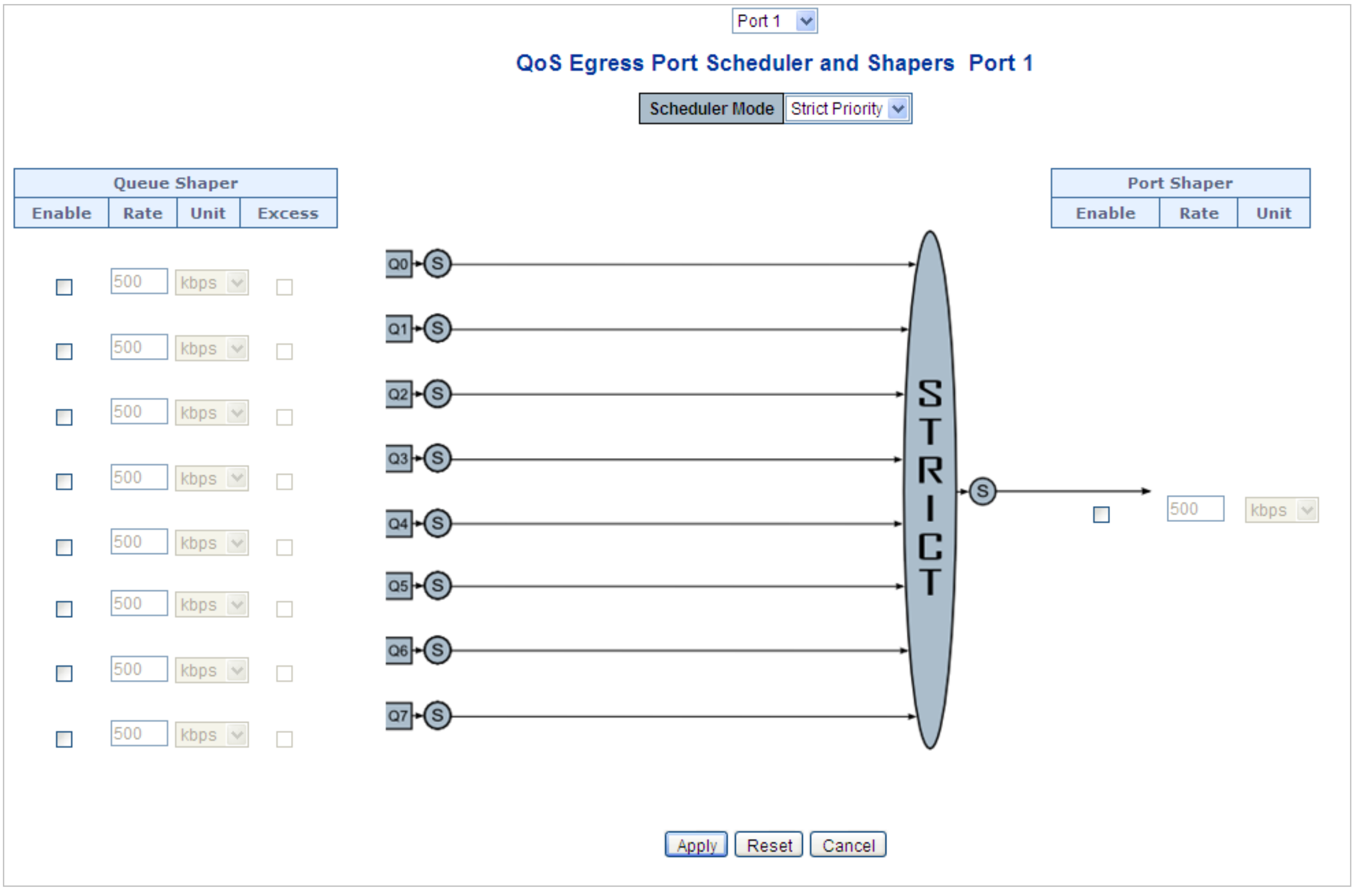


Figure 4-4-8: QoS Egress Port Schedule and Shapers Page Screenshot

The page includes the following fields:

Object	Description
• **Schedule Mode**	Controls whether the scheduler mode is "**Strict Priority**" or "**Weighted**" on this switch port.
• **Queue Shaper Enable**	Controls whether the queue shaper is enabled for this queue on this switch port.
• **Queue Shaper Rate**	Controls the rate for the queue shaper. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps". The default value is **500**.
• **Queue Shaper Unit**	Controls the unit of measure for the queue shaper rate as "**kbps**" or "**Mbps**". The default value is "kbps".
• **Queue Shaper Excess**	Controls whether the queue is allowed to use excess bandwidth.
• **Queue Scheduler Weight**	Controls the weight for this queue. This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "**Weighted**". The default value is "**17**".
• **Queue Scheduler Percent**	Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".
• **Port Shaper Enable**	Controls whether the port shaper is enabled for this switch port.
• **Port Shaper Rate**	Controls the rate for the port shaper. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps". The default value is 500.
• **Port Shaper Unit**	Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

Buttons

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

Cancel: Click to undo any changes made locally and return to the previous page.

4.4.3 Storm Control

4.4.3.1 Storm Policing

Global storm policers for the switch are configured on this page.

There is a unicast storm policer, multicast storm policer, and a broadcast storm policer.
These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present in the MAC Address table.

The displayed settings are:

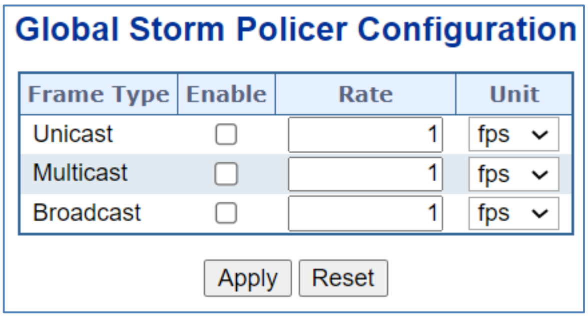


Figure 4-4-9: Global Storm Policer Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Frame Type**	The frame type for which the configuration below applies.
• **Enable**	Enable or disable the global storm policer for the given frame type.
• **Rate**	Controls the rate for the global storm policer. This value is restricted to 10-13128147 when "Unit" is fps or kbps, and 1-13128 when "Unit" is kfps or Mbps. The rate is internally rounded up to the nearest value supported by the global storm policer. Supported rates are divisible by 10 fps or 25 kbps.
• **Unit**	Controls the unit of measure for the global storm policer rate as fps, kfps, kbps or Mbps.

Buttons

: Click to apply changes

: Click to undo any changes made locally and revert to previously saved values.

4.4.4 Differentiated Service

4.4.4.1 Port DSCP

This page allows you to configure the basic QoS Port DSCP Configuration settings for all switch ports. The Port DSCP screen in Figure 4-4-10 appears.

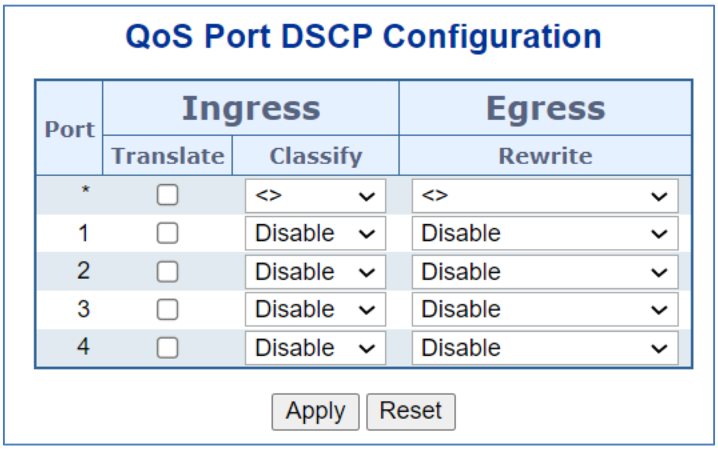


Figure 4-4-10: QoS Port DSCP Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The Port column shows the list of ports for which you can configure dscp ingress and egress settings.
• **Ingress**	In Ingress settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress: ■ **Translate** ■ **Classify**
• **Translate**	To Enable the Ingress Translation click the checkbox.
• **Classify**	Classification for a port have 4 different values. ■ **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**	Port Egress Rewriting can be one of - ■ **Disable**: No Egress rewrite. ■ **Enable**: Rewrite enable without remapped. ■ **Remap DP Unaware**: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation->Egress Remap DP0' table. ■ **Remap DP Aware**: DSCP from analyzer is remapped and frame is

	remarked with remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the 'DSCP Translation->Egress Remap DP0' table or from the 'DSCP Translation->Egress Remap DP1' table.

Buttons

: Click to apply changes

: Click to undo any changes made locally and revert to previously saved values.

4.4.4.2 DSCP-based QoS

This page allows you to configure the basic QoS DSCP-based QoS Ingress Classification settings for all switches. The DSCP-based QoS screen in Figure 4-4-11 appears.

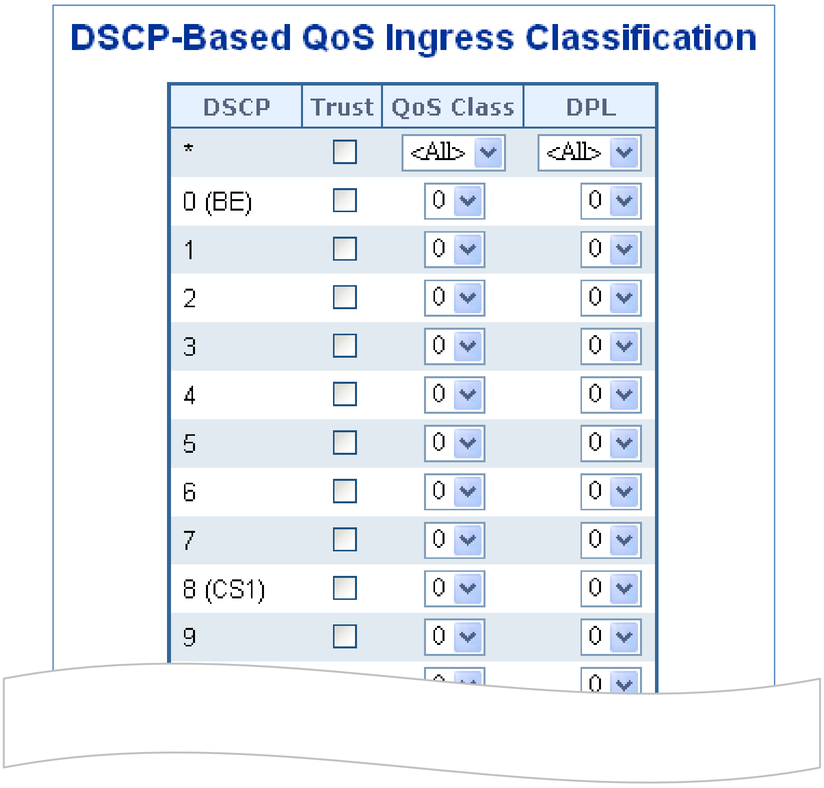


Figure 4-4-11: DSCP-based QoS Ingress Classification Page Screenshot

The page includes the following fields:

Object	Description
• **DSCP**	Maximum number of supported DSCP values are 64.
• **Trust**	Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.
• **QoS Class**	QoS Class value can be any of (0-7)
• **DPL**	Drop Precedence Level (0-1)

4.4.4.3 DSCP Translation

This page allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress. The DSCP Translation screen in Figure 4-4-12 appears.

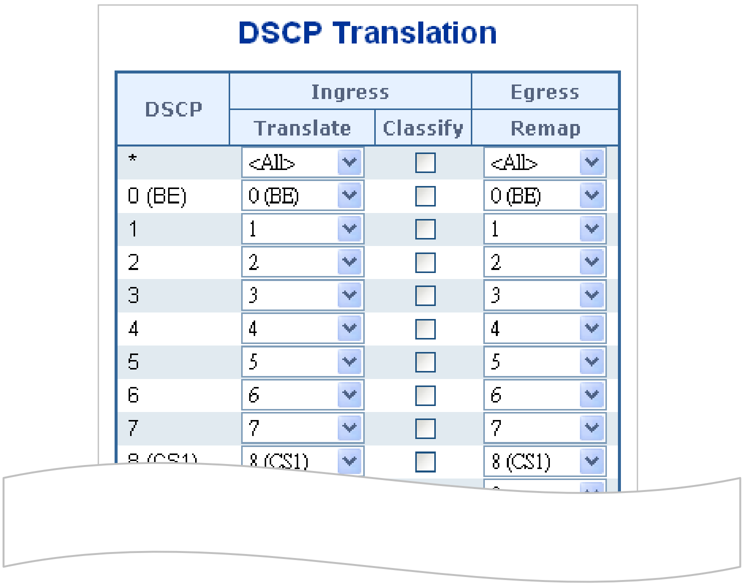


Figure 4-4-12: DSCP Translation Page Screenshot

The page includes the following fields:

Object	Description
• **DSCP**	Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.
• **Ingress**	Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. There are two configuration parameters for DSCP Translation – ■ **Translate** ■ **Classify**
• **Translate**	DSCP at Ingress side can be translated to any of (0-63) DSCP values.
• **Classify**	Click to enable Classification at Ingress side.
• **Egress**	There is following configurable parameter for Egress side - ■ **Remap**
• **Remap DP**	Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.

Buttons

: Click to apply changes

: Click to undo any changes made locally and revert to previously saved values.

4.4.4.4 DSCP Classification

This page allows you to map DSCP value to a QoS Class and DPL value. The DSCP Classification screen in Figure 4-4-13 appears.

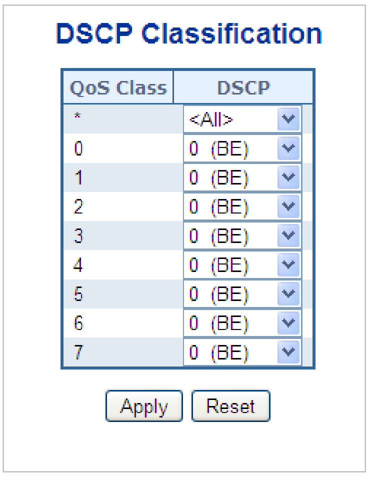


Figure 4-4-13: DSCP Classification Page Screenshot

The page includes the following fields:

Object	Description
• **QoS Class**	Available QoS Class value ranges from 0 to 7. QoS Class (0-7) can be mapped to followed parameters.
• **DPL**	Actual Drop Precedence Level.
• **DSCP**	Select DSCP value (0-63) from DSCP menu to map DSCP to corresponding QoS Class and DPL value

Buttons

: Click to apply changes

: Click to undo any changes made locally and revert to previously saved values.

4.4.5 QCL

4.4.5.1 QoS Control List

This page shows the QoS Control List(QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is **256** on each switch.

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

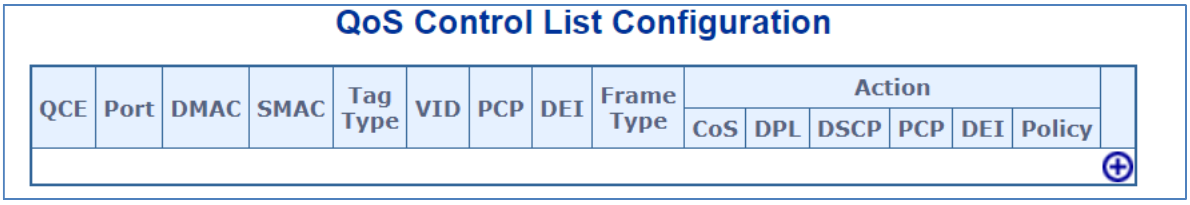


Figure 4-4-14: QoS Control List Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **QCE**	Indicates the index of QCE.
• **Port**	Indicates the list of ports configured with the QCE.
• **DMAC**	Specify the type of Destination MAC addresses for incoming frame. Possible values are: ■ **Any**: All types of Destination MAC addresses are allowed. ■ **Unicast**: Only Unicast MAC addresses are allowed. ■ **Multicast**: Only Multicast MAC addresses are allowed. ■ **Broadcast**: Only Broadcast MAC addresses are allowed. The default value is 'Any'.
• **SMAC**	Displays the OUI field of Source MAC address, i.e. first three octet (byte) of MAC address.
• **Tag Type**	Indicates tag type. Possible values are: ■ **Any**: Match tagged and untagged frames. ■ **Untagged**: Match untagged frames. ■ **Tagged**: Match tagged frames. The default value is 'Any'
• **VID**	Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'
• **PCP**	Priority Code Point: Valid value PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.
• **DEI**	Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any'.

• **Frame Type**	Indicates the type of frame to look for incoming frames. Possible frame types are: ■ **Any**: The QCE will match all frame type. ■ **Ethernet**: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed. ■ **LLC**: Only (LLC) frames are allowed. ■ **SNAP**: Only (SNAP) frames are allowed. ■ **IPv4**: The QCE will match only IPV4 frames. ■ **IPv6**: The QCE will match only 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.
• **Modification Buttons**	You can modify each QCE in the table using the following buttons: ⊕: Inserts a new QCE before the current row. ⓔ: Edits the QCE. ⓘ: Moves the QCE up the list. ⓘ: Moves the QCE down the list. ⊗: Deletes the QCE. ⊕: The lowest plus sign adds a new entry at the bottom of the list of QCL.

4.4.5.2 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. The maximum number of QCEs is **256** on each switch. The QoS Control List Status screen in Figure 4-4-15 appears.

Figure 4-4-15: QoS Control List Status Page Screenshot

The page includes the following fields:

Object	Description
• **User**	Indicates the QCL user.
• **QCE**	Indicates the index of QCE.
• **Port**	Indicates the list of ports configured with the QCE.
• **Frame Type**	Indicates the type of frame to look for incoming frames. Possible frame types are: ■ **Any**: The QCE will match all frame types. ■ **Ethernet**: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed. ■ **LLC**: Only (LLC) frames are allowed. ■ **SNAP**: Only (SNAP) frames are allowed. ■ **IPv4**: The QCE will match only IPV4 frames. ■ **IPv6**: The QCE will match only 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.
• **Conflict**	Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is

	always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.

Buttons

Combined: Select the QCL status from this drop down list.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Resolve Conflict: Click to release the resources required to add QCL entry, in case the conflict status for any QCL entry is 'yes'.

Refresh: Click to refresh the page.

4.4.6 Voice VLAN

4.4.6.1 Voice VLAN Configuration

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice, one for data.

Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI. The Voice VLAN Configuration screen in Figure 4-4-16 appears.

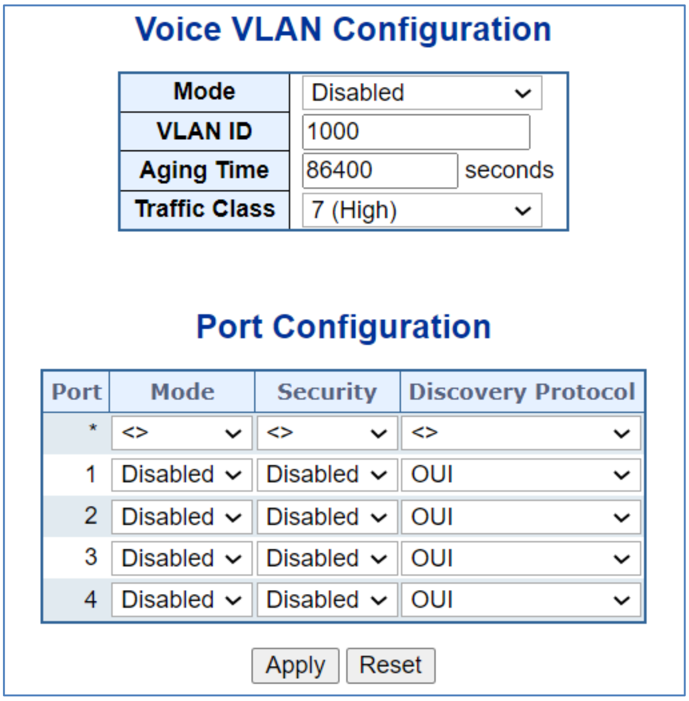


Figure 4-4-16: Voice VLAN Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filter. Possible modes are: ■ **Enabled**: Enable Voice VLAN mode operation. ■ **Disabled**: Disable Voice VLAN mode operation.
• **VLAN ID**	Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is conflict configuration if the value equal management VID, MVR VID, PVID etc. The allowed range is 1 to 4095.
• **Aging Time**	Indicates the Voice VLAN secure learning age time. The allowed range is 10 to 10000000 seconds. It used when security mode or auto detect mode is enabled.

	In other cases, it will based hardware age time. The actual age time will be situated in the [age_time; 2 * age_time] interval.
• **Traffic Class**	Indicates the Voice VLAN traffic class. All traffic on Voice VLAN will apply this class.
• **Mode**	Indicates the Voice VLAN port mode. Possible port modes are: ■ **Disabled**: Disjoin from Voice VLAN. ■ **Auto**: Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically. ■ **Forced**: Force join to Voice VLAN.
• **Port Security**	Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephone MAC address in Voice VLAN will be blocked 10 seconds. Possible port modes are: ■ **Enabled**: Enable Voice VLAN security mode operation. ■ **Disabled**: Disable Voice VLAN security mode operation.
• **Port Discovery Protocol**	Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart auto detect process. Possible discovery protocols are: ■ **OUI**: Detect telephony device by OUI address. ■ **LLDP**: Detect telephony device by LLDP. ■ **Both**: Both OUI and LLDP.

4.4.6.2 Voice VLAN OUI

Configure VOICE VLAN OUI table on this page. The maximum entry number is 16. Modifying the OUI table will restart auto detection of OUI process. The Voice VLAN OUI Table screen in Figure 4-4-17 appears.

Figure 4-4-17: Voice VLAN OUI Table Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Telephony OUI**	An telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).
• **Description**	The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.

Buttons

: Click to add a new access management entry.

: Click to apply changes

: Click to undo any changes made locally and revert to previously saved values.

4.5 Security

4.5.1 Access Security

4.5.1.1 Authentication Method

The authentication section allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces. The table has one row for each client type and a number of columns. The Authentication Method screen in Figure 4-5-1 appears.

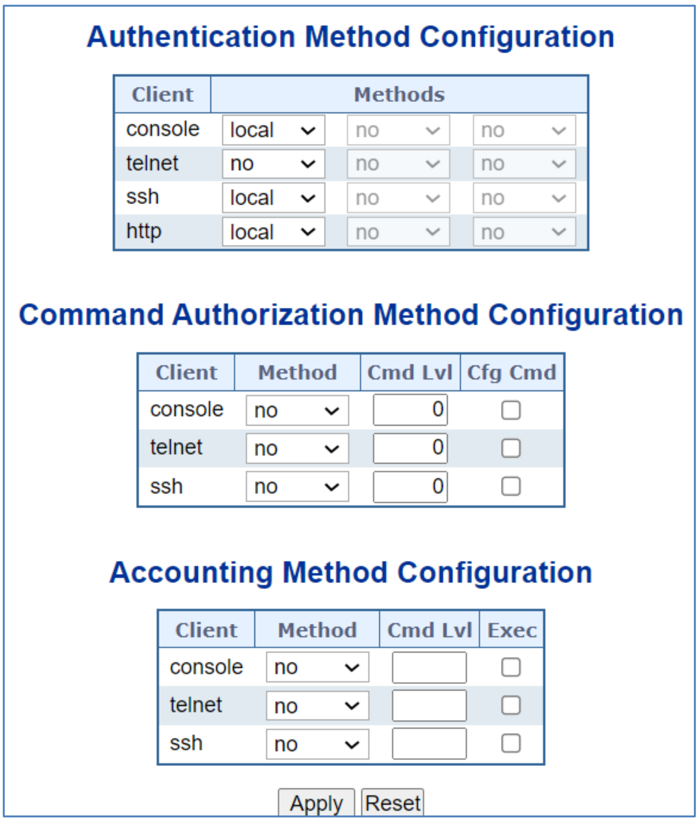


Figure 4-5-1: Authentication Method Configuration Overview Page Screenshot

The page includes the following fields:

Object	Description
• **Client**	The management client for which the configuration below applies.
• **Methods**	Method can be set to one of the following values: • no: Authentication is disabled and login is not possible. • local: Use the local user database on the switch for authentication. • radius: Use remote RADIUS server(s) for authentication. • tacacs: Use remote TACACS+ server(s) for authentication. Methods that involves remote servers are timed out if the remote servers are

	offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive.
• **Command Authorization Method Configuration**	The command authorization section allows you to limit the CLI commands available to a user.
• **Client**	The management client for which the configuration below applies.
• **Method**	Method can be set to one of the following values: • no: Command authorization is disabled. User is granted access to CLI commands according to his privilege level. • tacacs: Use remote TACACS+ server(s) for command authorization. If all remote servers are offline, the user is granted access to CLI commands according to his privilege level.
• **Cmd Lvl**	Authorize all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15.
• **Cfg Cmd**	Also authorize configuration commands.
• **Accounting Method Configuration**	The accounting section allows you to configure command and exec (login) accounting.
• **Client**	The management client for which the configuration below applies.
• **Method**	Method can be set to one of the following values: • no: Command authorization is disabled. User is granted access to CLI commands according to his privilege level. • tacacs: Use remote TACACS+ server(s) for command authorization. If all remote servers are offline, the user is granted access to CLI commands according to his privilege level.
• **Cmd Lvl**	Enable accounting of all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15. Leave the field empty to disable command accounting.
• **Cfg Cmd**	Enable exec (login) accounting.

Buttons

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.5.1.2 Access Management

Configure access management table on this page. The maximum entry number is 16. If the application's type match any one of the access management entries, it will allow access to the switch. The Access Management Configuration screen in Figure 4-5-2 appears.

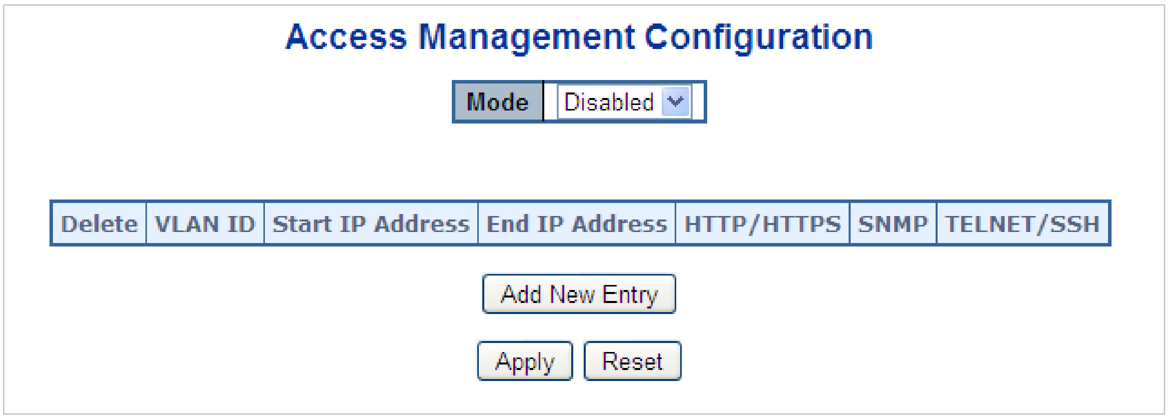


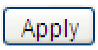
Figure 4-5-2: Access Management Configuration Overview Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	Indicates the access management mode operation. Possible modes are: **Enabled**: Enable access management mode operation. **Disabled**: Disable access management mode operation.
• **Delete**	Check to delete the entry. It will be deleted during the next apply .
• **VLAN ID**	Indicates the VLAN ID for the access management entry.
• **Start IP address**	Indicates the start IP address for the access management entry.
• **End IP address**	Indicates the end IP address for the access management entry.
• **HTTP/HTTPS**	Indicates the host can access the switch from HTTP/HTTPS interface that the host IP address matched the entry.
• **SNMP**	Indicates the host can access the switch from SNMP interface that the host IP address matched the entry.
• **Telnet/SSH**	Indicates the host can access the switch from TELNET/SSH interface that the host IP address matched the entry.

Buttons

: Click to add a new access management entry.

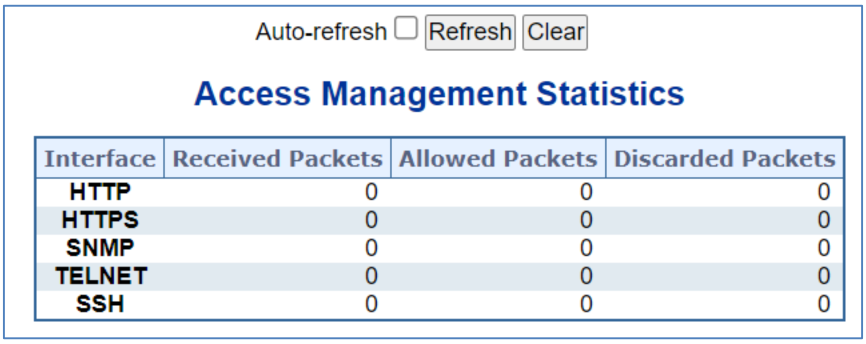


: Click to apply changes

: Click to undo any changes made locally and revert to previously saved values.

4.5.1.3 Access Management Statistics

This page provides statistics for access management. The Access Management Statistics screen in Figure 4-5-3 appears.



Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

Figure 4-5-3: Access Management Statistics Overview Page Screenshot

The page includes the following fields:

Object	Description
• **Interface**	The interface that allowed remote host can access the switch.
• **Receive Packets**	The received packets number from the interface under access management mode is enabled.
• **Allow Packets**	The allowed packets number from the interface under access management mode is enabled.
• **Discard Packets**	The discarded packets number from the interface under access management mode is enabled.

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears all statistics.

4.5.1.4 SSH

Configure SSH on this page. This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

The status page is divided into two sections - one with a legend of user modules and one with the actual port status. The SSH Configuration screen in Figure 4-5-4 appears.

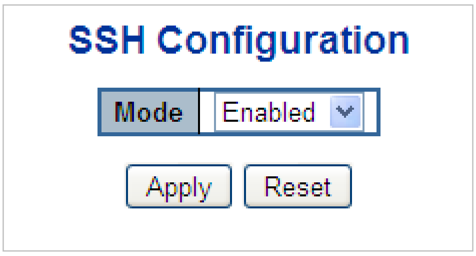


Figure 4-5-4: SSH Configuration Screen Page Screenshot

The page includes the following fields:

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

Buttons

: Click to apply changes

: Click to undo any changes made locally and revert to previously saved values.

4.5.1.5 HTTPs

Configure HTTPS on this page. The HTTPS Configuration screen in Figure 4-5-5 appears.

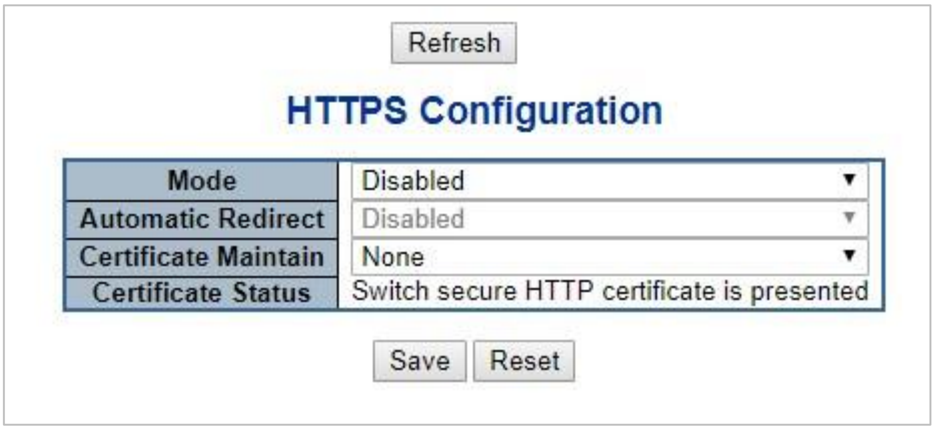


Figure 4-5-5: HTTPS Configuration Screen Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	Indicates the HTTPS mode operation. When the current connection is HTTPS, to apply HTTPS disabled mode operation will automatically redirect web browser to an HTTP connection. Possible modes are: ■ **Enabled**: Enable HTTPS mode operation. ■ **Disabled**: Disable HTTPS mode operation.
• **Automatic Redirect**	Indicates the HTTPS redirect mode operation. It only significant if HTTPS mode "Enabled" is selected. Automatically redirects web browser to an HTTPS connection when both HTTPS mode and Automatic Redirect are enabled or redirects web browser to an HTTP connection when both are disabled. 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. The URL format is <protocol>://[<username>[:<password>]@]<host>[:<port>][/<path>]/<file_name>. For example, tftp://10.10.10.10/new_image_path/new_image.dat, http://username:password@10.10.10.10:80/new_image_path/new_image.dat. A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), under score(_). The maximum length is 63 and hyphen must not be first character. The file name content that only contains '.' is not allowed.
• **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 ...**

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Refresh: Click to refresh the page. Any changes made locally will be undone.

4.5.2 AAA

This section is to control the access to the Managed Switch, including the user access and management control.

The Authentication section contains links to the following main topics:

- **User Authentication**
- **IEEE 802.1X Port-based Network Access Control**
- **MAC-based Authentication**

Overview of 802.1X (Port-Based) Authentication

In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The switch acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as **EAPOL (EAP Over LANs)** frames. EAPOL frames encapsulate **EAP PDU**s (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like **MD5-Challenge**, **PEAP**, and **TLS**. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

Overview of MAC-based Authentication

Unlike 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using static entries into the MAC Table. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

The advantage of MAC-based authentication over 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users, equipment whose MAC address is a valid RADIUS user can be used by anyone, and only the MD5-Challenge method is supported.
The 802.1X and MAC-Based Authentication configuration consists of two sections, a system- and a port-wide.

Overview of User Authentication

It is allowed to configure the Managed Switch to authenticate users logging into the system for management access using local or remote authentication methods, such as telnet and Web browser. This Managed Switch provides secure network management access using the following options:

- **Remote Authentication Dial-in User Service (RADIUS)**
- **Terminal Access Controller Access Control System Plus (TACACS+)**
- **Local user name and Privilege Level control**

RADIUS and TACACS+ are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS-aware devices on the network. An **authentication server** contains a database of multiple user name / password pairs with associated privilege levels for each user that requires management access to the Managed Switch.

Understanding IEEE 802.1X Port-based Authentication

The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port before making available any services offered by the switch or the LAN.

Until the client is authenticated, 802.1X access control allows only **Extensible Authentication Protocol over LAN (EAPOL)** traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

This section includes this conceptual information:

- Device Roles
- Authentication Initiation and Message Exchange
- Ports in Authorized and Unauthorized States

■ **Device Roles**

With 802.1X port-based authentication, the devices in the network have specific roles as shown below.

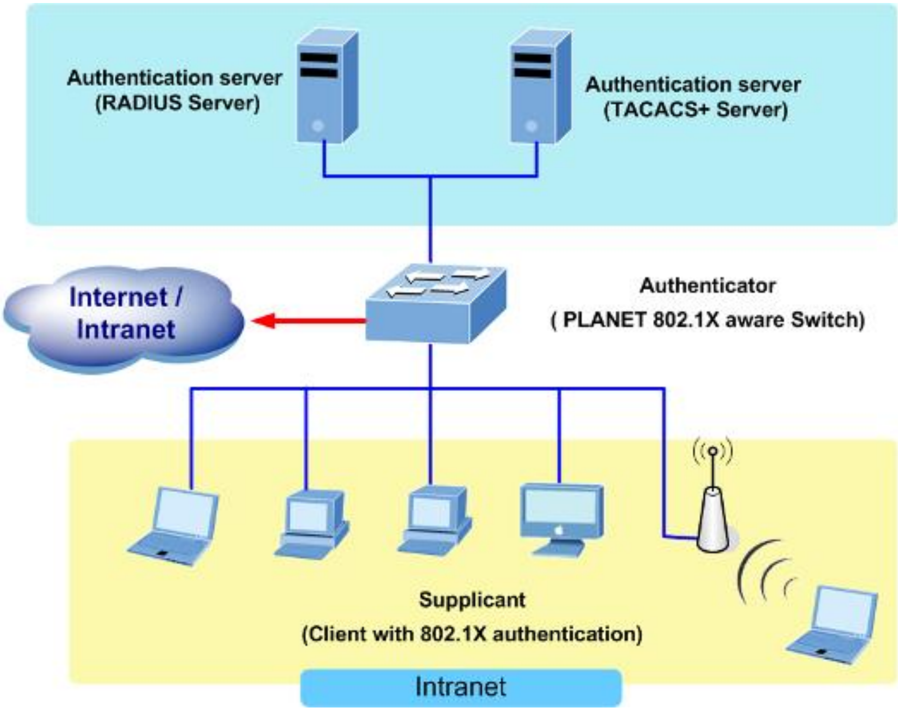


Figure 4-5-6

- ***Client***—the device (workstation) that requests access to the LAN and switch services and responds to requests from the switch. The workstation must be running 802.1X-compliant client software such as that offered in the Microsoft Windows XP operating system. (The client is the *supplicant* in the IEEE 802.1X specification.)

- ***Authentication server***—performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. In this release, the Remote Authentication Dial-In User Service (RADIUS) security system with **Extensible Authentication Protocol (EAP)** extensions is the only supported authentication server; it is available in Cisco Secure Access Control Server version 3.0. RADIUS operates in a client/server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.

- ***Switch* (802.1X device)**—controls the physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client. The switch includes the RADIUS client, which is responsible for encapsulating and decapsulating the Extensible Authentication Protocol (EAP) frames and interacting with the authentication server. When the switch receives EAPOL frames and relays them to the authentication server, the Ethernet header is stripped and the remaining EAP frame is re-encapsulated in the RADIUS format. The EAP frames are not modified or examined during encapsulation, and the authentication server must support EAP within the native frame format. When the switch receives frames from the authentication server, the server's frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the client.

- **Authentication Initiation and Message Exchange**

The switch or the client can initiate authentication. If you enable authentication on a port by using the **dot1x port-control auto** interface configuration command, the switch must initiate authentication when it determines that the port link state transitions from down to up. It then sends an EAP-request/identity frame to the client to request its identity (typically, the switch sends an initial identity/request frame followed by one or more requests for authentication information). Upon receipt of the frame, the client responds with an EAP-response/identity frame.

However, if during bootup, the client does not receive an EAP-request/identity frame from the switch, the client can initiate authentication by sending an EAPOL-start frame, which prompts the switch to request the client's identity

Note

If 802.1X is not enabled or supported on the network access device, any EAPOL frames from the client are dropped. If the client does not receive an EAP-request/identity frame after three attempts to start authentication, the client transmits frames as if the port is in the authorized state. A port in the authorized state effectively means that the client has been successfully authenticated.

When the client supplies its identity, the switch begins its role as the intermediary, passing EAP frames between the client and the authentication server until authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized.

The specific exchange of EAP frames depends on the authentication method being used. "Figure 4-5-7" shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.

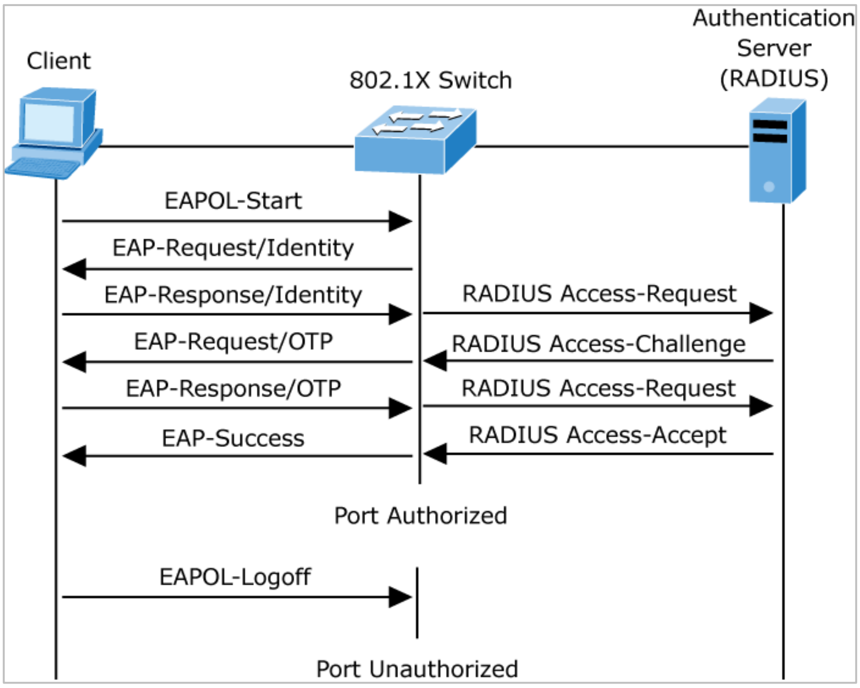


Figure 4-5-7: EAP Message Exchange

- **Ports in Authorized and Unauthorized States**

The switch port state determines whether or not the client is granted access to the network. The port starts in the *unauthorized* state. While in this state, the port disallows all ingress and egress traffic except for 802.1X protocol packets. When a client is successfully authenticated, the port transitions to the *authorized* state, allowing all traffic for the client to flow normally.

If a client that does not support 802.1X is connected to an unauthorized 802.1X port, the switch requests the client's identity. In this situation, the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network.

In contrast, when an 802.1X-enabled client connects to a port that is not running the 802.1X protocol, the client initiates the authentication process by sending the EAPOL-start frame. When no response is received, the client sends the request for a fixed number of times. Because no response is received, the client begins sending frames as if the port is in the authorized state

If the client is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted.

When a client logs off, it sends an EAPOL-logoff message, causing the switch port to transition to the unauthorized state.

If the link state of a port transitions from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

4.5.2.1 RADIUS

This page allows you to configure the RADIUS Servers. The RADIUS Configuration screen in Figure 4-5-8 appears.

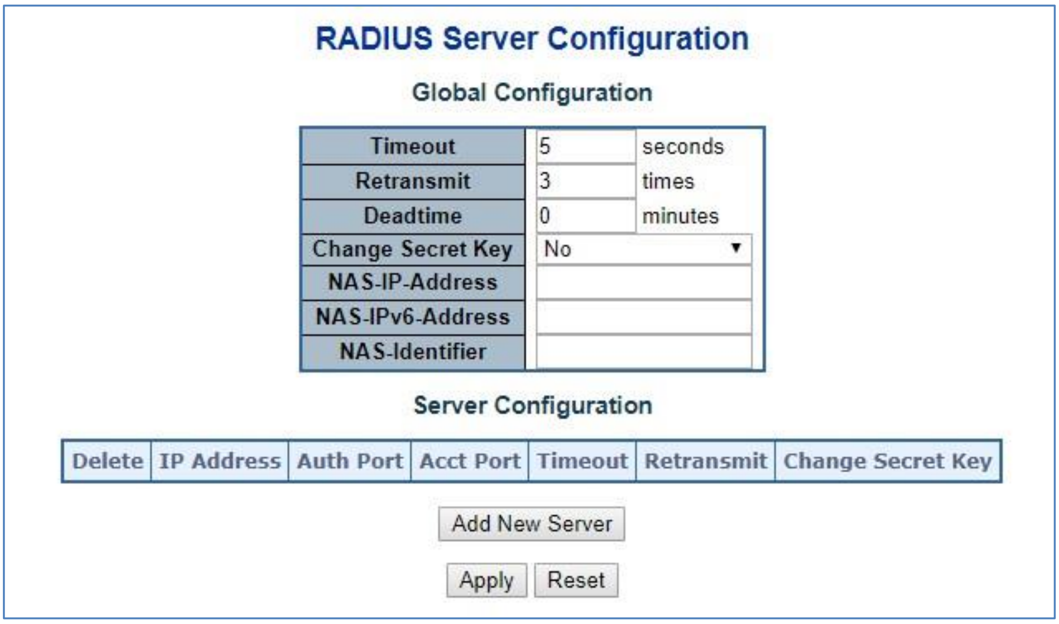


Figure 4-5-8: RADIUS Server Configuration Page Screenshot

The page includes the following fields:

Global Configuration

These setting are common for all of the RADIUS Servers.

Object	Description
• **Timeout**	Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.
• **Retransmit**	Retransmit is the number of times, in the range from 1 to 1000; a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit, it is considered to be dead.
• **Dead Time**	The Dead Time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.
• **Key**	The secret key - up to 63 characters long - shared between the RADIUS server and the switch.
• **NAS-IP-Address**	The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

• **NAS-IPv6-Address**	The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.
• **NAS-Identifier**	The identifier - up to 253 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.

Server Configuration

The table has one row for each RADIUS Server and a number of columns, which are:

Object	Description
• **Delete**	To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.
• **Hostname**	The IP address or hostname of the RADIUS server.
• **Auth Port**	The UDP port to use on the RADIUS server for authentication.
• **Acct Port**	The UDP port to use on the RADIUS server for accounting.
• **Timeout**	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
• **Retransmit**	This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.
• **Key**	This optional setting overrides the global key. Leaving it blank will use the global key.

Buttons

Add New Server: Click to add a new RADIUS server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to 5 servers are supported.

Delete: Click to undo the addition of the new server.

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.5.2.2 TACACS+

This page allows you to configure the TACACS+ Servers. The TACACS+ Configuration screen in Figure 4-5-9 appears.

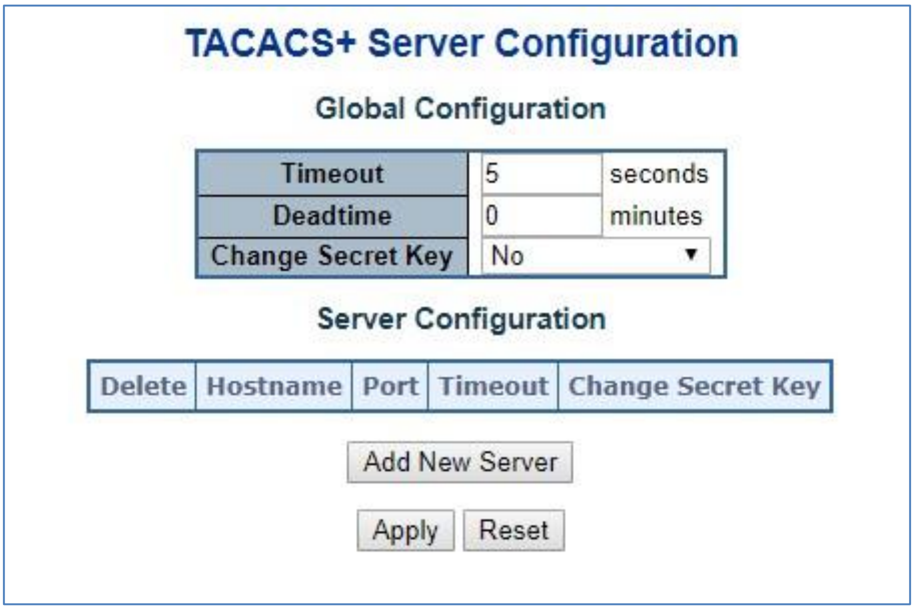


Figure 4-5-9: TACACS+ Server Configuration Page Screenshot

The page includes the following fields:

Global Configuration

These setting are common for all of the TACACS+ Servers.

Object	Description
• **Timeout**	Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a TACACS+ server before it is considered to be dead.
• **Dead Time**	The Dead Time, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.
• **Key**	Specify to change the secret key or not. When "Yes" is selected for the option, you can change the secret key - up to 63 characters long - shared between the TACACS+ server and the switch.

Server Configuration

The table has one row for each TACACS+ server and a number of columns, which are:

Object	Description
• **Delete**	To delete a TACACS+ server entry, check this box. The entry will be deleted during the next Save.
• **Hostname**	The IP address or hostname of the TACACS+ server.
• **Port**	The TCP port to use on the TACACS+ server for authentication.
• **Timeout**	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
• **Key**	This optional setting overrides the global key. Leaving it blank will use the global key.

Buttons

Add New Server: Click to add a new TACACS+ server. An empty row is added to the table, and the TACACS+ server can be configured as needed. Up to 5 servers are supported.

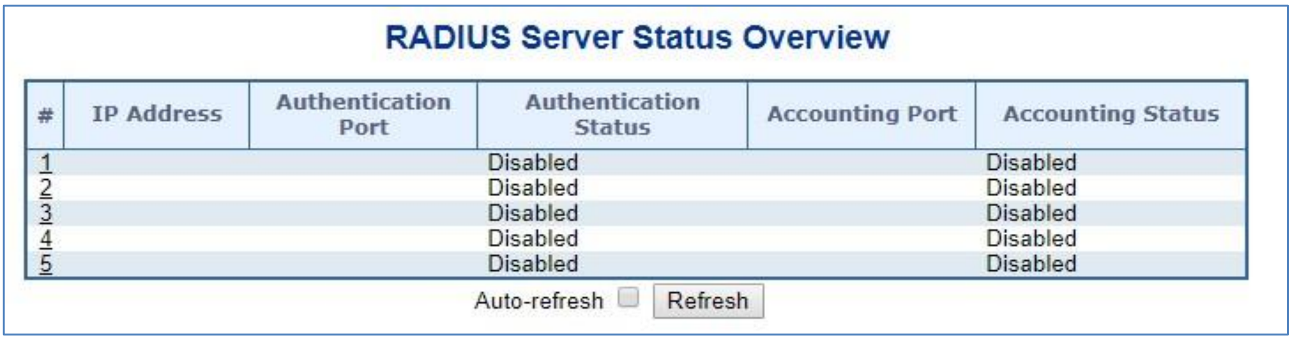
Delete: Click to undo the addition of the new server.

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.5.2.3 RADIUS Overview

This page provides an overview of the status of the RADIUS servers configurable on the authentication configuration page. The RADIUS Authentication/Accounting Server Overview screen in Figure 4-5-10 appears.



RADIUS Server Status Overview

#	IP Address	Authentication Port	Authentication Status	Accounting Port	Accounting Status
1			Disabled		Disabled
2			Disabled		Disabled
3			Disabled		Disabled
4			Disabled		Disabled
5			Disabled		Disabled

Auto-refresh Refresh

Figure 4-5-10: RADIUS Authentication/Accounting Server Overview Page Screenshot

The page includes the following fields:

RADIUS Authentication Server Status Overview

Object	Description
• **#**	The RADIUS server number. Click to navigate to detailed statistics for this server.
• **IP Address**	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
• **Authentication Port**	UDP port number for authentication.
• **Authentication Status**	The current status of the server. This field takes one of the following values: **Disabled**: The server is disabled. **Not Ready**: The server is enabled, but IP communication is not yet up and running. **Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. **Dead (X seconds left)**: Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
• **Accounting Port**	UDP port number for accounting
• **Accounting Status**	The current status of the server. This field takes one of the following values: **Disabled**: The server is disabled. **Not Ready**: The server is enabled, but IP communication is not yet up and running. **Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. **Dead (X seconds left)**: Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

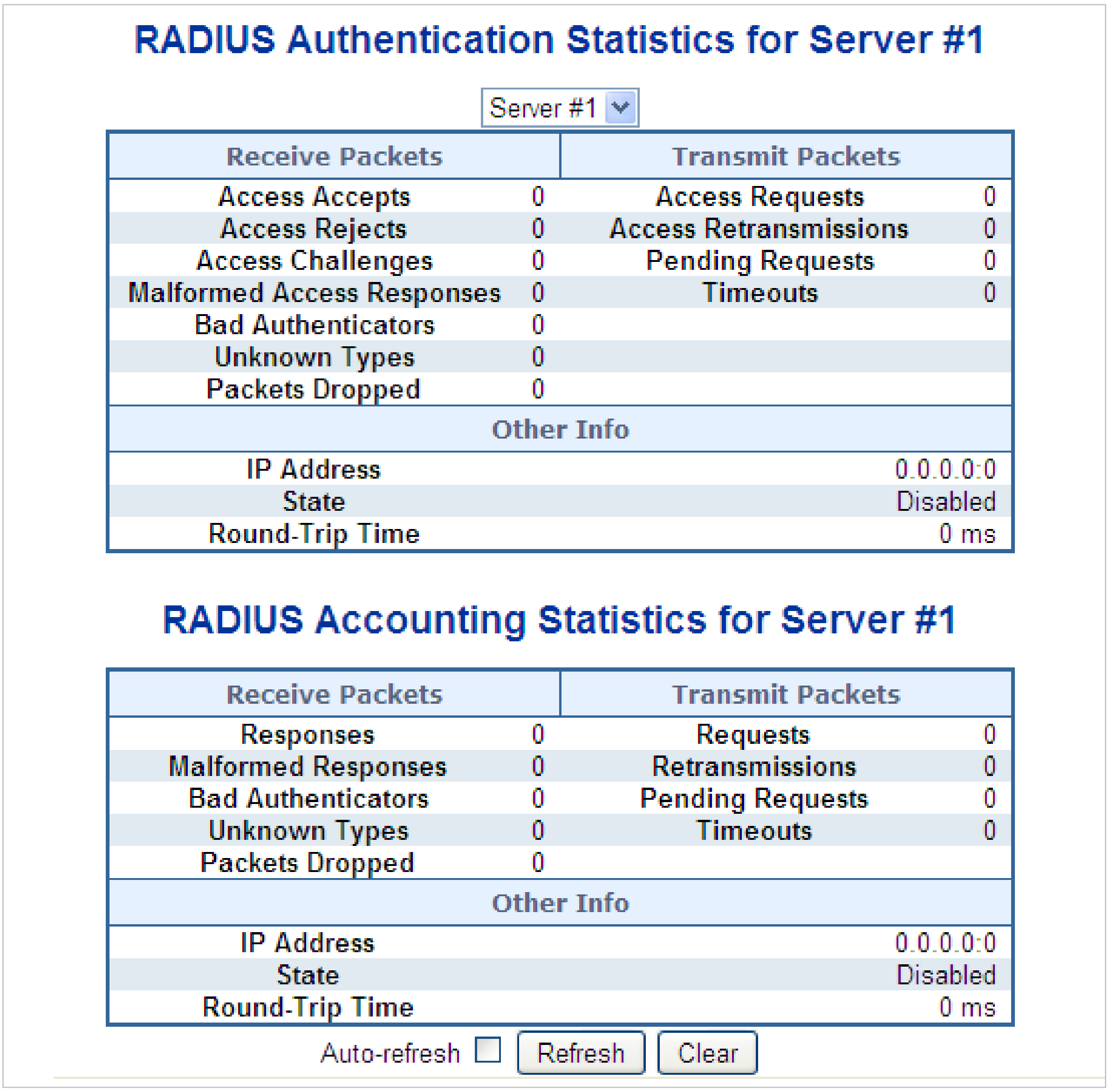
Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4.5.2.4 RADIUS Details

This page provides detailed statistics for a particular RADIUS server. The RADIUS Authentication/Accounting for Server Overview screen in Figure 4-5-11 appears.



RADIUS Authentication Statistics for Server #1

Server #1

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		

Other Info	
IP Address	0.0.0.0:0
State	Disabled
Round-Trip Time	0 ms

RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		

Other Info	
IP Address	0.0.0.0:0
State	Disabled
Round-Trip Time	0 ms

Auto-refresh Refresh Clear

Figure 4-5-11: RADIUS Authentication/Accounting for Server Overview Screenshot

The page includes the following fields:

RADIUS Authentication Statistics

The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB. Use the server select box to switch between the backend servers to show details for.

Object	Description			
• **Packet Counters**	RADIUS authentication server packet counter. There are seven receive and four transmit counters.			
	Direction	**Name**	**RFC4668 Name**	**Description**
	Rx	**Access Accepts**	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
	Rx	**Access Rejects**	radiusAuthClientExtAccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
	Rx	**Access Challenges**	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
	Rx	**Malformed Access Responses**	radiusAuthClientExtMalformedAccessResponses	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.
	Rx	**Bad Authenticators**	radiusAuthClientExtBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.

	Rx	**Unknown Types**	radiusAuthClientExtUnknownTypes	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
	Rx	**Packets Dropped**	radiusAuthClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
	Tx	**Access Requests**	radiusAuthClientExtAccessRequests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
	Tx	**Access Retransmissions**	radiusAuthClientExtAccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
	Tx	**Pending Requests**	radiusAuthClientExtPendingRequests	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.
	Tx	**Timeouts**	radiusAuthClientExtTimeouts	The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is

	counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
• **Other Info**	This section contains information about the state of the server and the latest round-trip time.

Name	RFC4668 Name	Description
IP Address	-	IP address and UDP port for the authentication server in question.
State	-	Shows the state of the server. It takes one of the following values: ■ **Disabled**: The selected server is disabled. ■ **Not Ready**: The server is enabled, but IP communication is not yet up and running. ■ **Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. ■ **Dead (X seconds left)**: Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	radiusAuthClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

RADIUS Accounting Statistics

The statistics map closely to those specified in RFC4670 - RADIUS Accounting Client MIB. Use the server select box to switch between the backend servers to show details for.

Object	Description
• **Packet Counters**	RADIUS accounting server packet counter. There are five receive and four transmit counters.

Direction	Name	RFC4670 Name	Description
Rx	**Responses**	radiusAccClientExtResponses	The number of RADIUS packets (valid or invalid) received from the server.
Rx	**Malformed Responses**	radiusAccClientExtMalformedResponses	The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.
Rx	**Bad Authenticators**	radiusAcctClientExtBadAuthenticators	The number of RADIUS packets containing invalid authenticators received from the server.
Rx	**Unknown Types**	radiusAccClientExtUnknownTypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Rx	**Packets Dropped**	radiusAccClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
Tx	**Requests**	radiusAccClientExtRequests	The number of RADIUS packets sent to the server. This does not include retransmissions.

	Tx	**Retransmissions**	radiusAccClientExt Retransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.
	Tx	**Pending Requests**	radiusAccClientExt PendingRequests	The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.
	Tx	**Timeouts**	radiusAccClientExt Timeouts	The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

- **Other Info**

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4670 Name	Description
IP Address	-	IP address and UDP port for the accounting server in question.
State	-	Shows the state of the server. It takes one of the following values: ■ **Disabled**: The selected server is disabled. ■ **Not Ready**: The server is enabled, but IP communication is not yet up and running. ■ **Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.

			■ **Dead (X seconds left)**: Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
	Round-Trip Time	radiusAccClientExtRoundTripTime	■ The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

4.5.3 Port Authentication

4.5.3.1 Network Access Server Configuration

This page allows you to configure the IEEE 802.1X and MAC-based authentication system and port settings.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the "Configuration→Security→AAA" Page. The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations as shall be explored below.

MAC-based authentication allows for authentication of more than one user on the same port, and doesn't require the user to have special 802.1X supplicant software installed on his system. The switch uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1X authentication. The NAS configuration consists of two sections, a system- and a port-wide. The Network Access Server Configuration screen in Figure 4-5-12 appears.

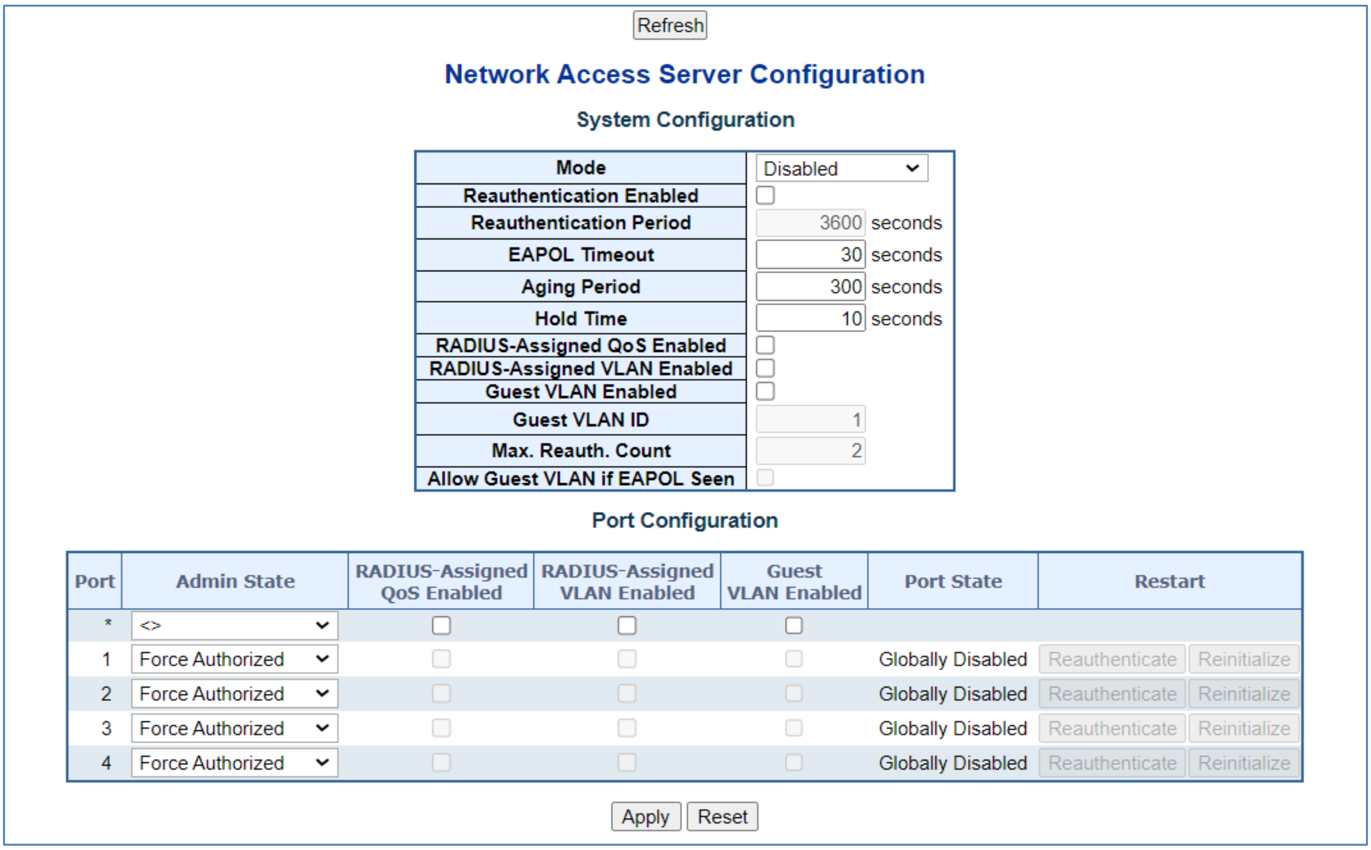


Figure 4-5-12: Network Access Server Configuration Page Screenshot

The page includes the following fields:

System Configuration

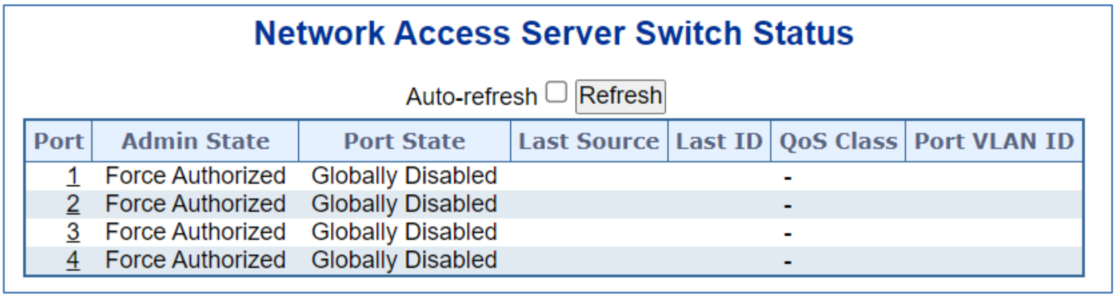
Object	Description
• **Mode**	Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.
• **Reauthentication Enabled**	If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached. For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port.
• **Reauthentication Period**	Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.
• **EAPOL Timeout**	Determines the time for retransmission of Request Identity EAPOL frames. Valid values are in the range 1 to 65535 seconds. This has no effect for MAC-based ports.
• **Aging Period**	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses: ■ **Single 802.1X** ■ **Multi 802.1X** ■ **MAC-Based Auth**. When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds. If reauthentication is enabled and the port is in a 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries. For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether

	the client is still attached or not, and the only way to free any resources is to age the entry.
• **Hold Time**	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses: ■ **Single 802.1X** ■ **Multi 802.1X** ■ **MAC-Based Auth**. If a client is denied access, either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration→Security→AAA" page), the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication. In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time. The Hold Time can be set to a number between 10 and 1000000 seconds.
• **RADIUS-Assigned QoS Enabled**	RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature. The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determines whether RADIUS-assigned QoS Class is enabled for that port. When unchecked, RADIUS-server assigned QoS Class is disabled for all ports.
• **RADIUS-Assigned VLAN Enabled**	RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature. The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determines whether RADIUS-assigned VLAN is enabled for that port. When unchecked, RADIUS-server assigned VLAN is disabled for all ports.
• **Guest VLAN Enabled**	A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined

	timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below. The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled for all ports.
• **Guest VLAN ID**	This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled. Valid values are in the range [1; 4095].
• **Max. Reauth. Count**	The number of times that the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled. Valid values are in the range [1; 255].
• **Allow Guest VLAN if EAPOL Seen**	The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port. The value can only be changed if the Guest VLAN option is globally enabled.

4.5.3.2 Network Access Overview

This page provides an overview of the current NAS port states for the selected switch. The Network Access Overview screen in Figure 4-5-13 appears.



Network Access Server Switch Status

Auto-refresh ☐ Refresh

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled			-	
2	Force Authorized	Globally Disabled			-	
3	Force Authorized	Globally Disabled			-	
4	Force Authorized	Globally Disabled			-	

Figure 4-5-13: Network Access Server Switch Status Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number. Click to navigate to detailed NAS statistics for this port.
• **Admin State**	The port's current administrative state. Refer to NAS Admin State for a description of possible values.
• **Port State**	The current state of the port. Refer to NAS Port State for a description of the individual states.
• **Last Source**	The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.
• **Last ID**	The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.
• **QoS Class**	QoS Class assigned to the port by the RADIUS server if enabled.
• **Port VLAN ID**	The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.5.3.3 Network Access Statistics

This page provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics, only. Use the port select box to select which port details to be displayed. The Network Access Statistics screen in Figure 4-5-14 appears.

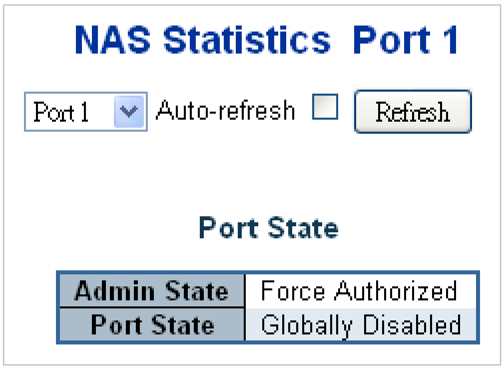


Figure 4-5-14: Network Access Statistics Page Screenshot

The page includes the following fields:

Port State

Object	Description
• **Admin State**	The port's current administrative state. Refer to NAS Admin State for a description of possible values.
• **Port State**	The current state of the port. Refer to NAS Port State for a description of the individual states.
• **QoS Class**	The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.
• **Port VLAN ID**	The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Port Counters

Object	Description
• **EAPOL Counters**	These supplicant frame counters are available for the following administrative states: ■ **Force Authorized** ■ **Force Unauthorized** ■ **Port-based 802.1X** ■ **Single 802.1X** ■ **Multi 802.1X**

Direction	Name	IEEE Name	Description
Rx	**Total**	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.
Rx	**Response ID**	dot1xAuthEapolRespIdFramesRx	The number of valid EAPOL Response Identity frames that have been received by the switch.
Rx	**Responses**	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames (other than Response Identity frames) that have been received by the switch.
Rx	**Start**	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.
Rx	**Logoff**	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL Logoff frames that have been received by the switch.
Rx	**Invalid Type**	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.
Rx	**Invalid Length**	dot1xAuthEapLengthErr	The number of EAPOL

			orFramesRx	frames that have been received by the switch in which the Packet Body Length field is invalid.
	Tx	**Total**	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that have been transmitted by the switch.
	Tx	**Request ID**	dot1xAuthEapolReqIdFramesTx	The number of EAPOL Request Identity frames that have been transmitted by the switch.
	Tx	**Requests**	dot1xAuthEapolReqFramesTx	The number of valid EAPOL Request frames (other than Request Identity frames) that have been transmitted by the switch.

- **Backend Server Counters**

These backend (RADIUS) frame counters are available for the following administrative states:

- **Port-based 802.1X**
- **Single 802.1X**
- **Multi 802.1X**
- **MAC-based Auth**.

Direction	Name	IEEE Name	Description
Rx	**Access Challenges**	dot1xAuthBackendAccessChallenges	**802.1X-based**: Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch. **MAC-based**: Counts all Access Challenges received from the backend server for this port (left-most

			table) or client (right-most table).
Rx	**Other Requests**	dot1xAuthBackendOtherRequestsToSupplicant	**802.1X-based**: Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method. **MAC-based**: Not applicable.
Rx	**Auth. Successes**	dot1xAuthBackendAuthSuccesses	**802.1X- and MAC-based**: Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.
Rx	**Auth. Failures**	dot1xAuthBackendAuthFails	**802.1X- and MAC-based**: Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.
Tx	**Responses**	dot1xAuthBackendResponses	**802.1X-based:** Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted. **MAC-based:** Counts all the backend server packets sent from the switch

<table>
<tr><td></td><td>towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.</td></tr>
<tr><td>• Last Supplicant/Client Info</td><td>Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states:
■ Port-based 802.1X
■ Single 802.1X
■ Multi 802.1X
■ MAC-based Auth.
<table>
<tr><th>Name</th><th>IEEE Name</th><th>Description</th></tr>
<tr><td>MAC Address</td><td>dot1xAuthLastEapolFrameSource</td><td>The MAC address of the last supplicant/client.</td></tr>
<tr><td>VLAN ID</td><td>-</td><td>The VLAN ID on which the last frame from the last supplicant/client was received.</td></tr>
<tr><td>Version</td><td>dot1xAuthLastEapolFrameVersion</td><td>802.1X-based:
The protocol version number carried in the most recently received EAPOL frame.
MAC-based:
Not applicable.</td></tr>
<tr><td>Identity</td><td>-</td><td>802.1X-based:
The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame.
MAC-based:
Not applicable.</td></tr>
</table></td></tr>
</table>

4.5.4 Port Security

4.5.4.1 Port Limit Control

This page allows you to configure the Port Security global and per-port settings.

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.. The Port Limit Control Configuration screen in Figure 4-5-15 appears.

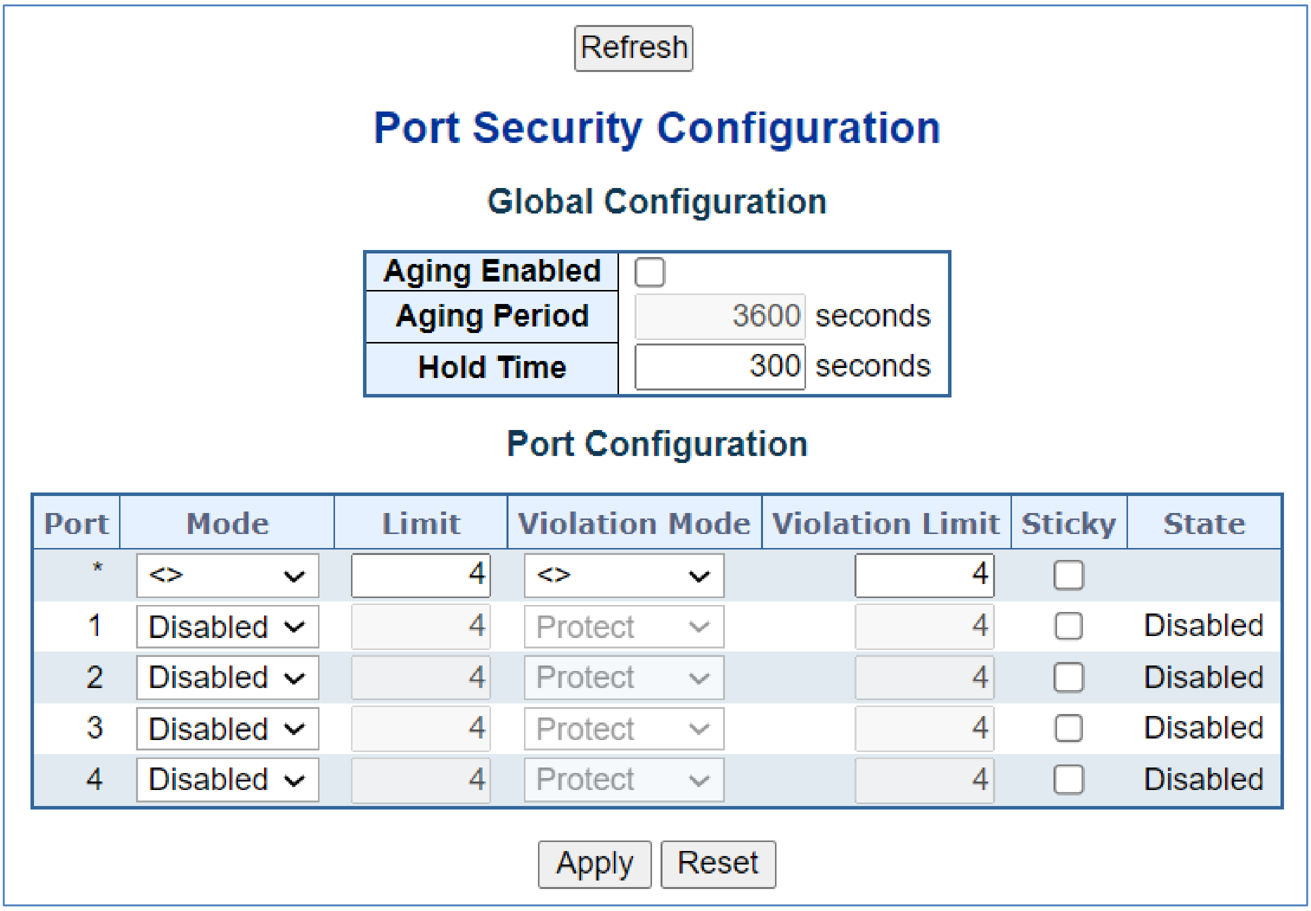


Figure 4-5-15: Port Limit Control Configuration Overview Page Screenshot

The page includes the following fields:

System Configuration

Object	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 port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality. The Aging Period can be set to a number between 10 and 10,000,000 seconds. To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.
• **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

The table has one row for each port and a number of columns, which are:

Object	Description
• **Port**	The port number for which the configuration below applies.
• **Mode**	Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.

• **Limit**	The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken. The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.
• **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. There are three ways to re-open the port: 1) In the "Configuration→Ports" page's "Configured" column, first disable the port, then restore the original mode. 2) Make a Port Security configuration change on the port. 3) Boot the switch.
• **Violation Limit**	■ The maximum number of MAC addresses that can be marked as violating on this port. This number cannot exceed 1024. 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. A port can be Sticky-enabled whether or not Port Security is enabled on that interface. In that way, it is possible to add sticky MAC addresses managementwise before enabling Port Security. To do that, use the "Configuration→Security→Port Security→MAC Addresses" page.
• **State**	This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values: ■ **Disabled**: Limit Control is either globally disabled or disabled on the port. ■ **Ready**: The limit is not yet reached. This can be shown for all actions. ■ **Limit Reached**: Indicates that the limit is reached on this port. This state can only be shown if Action is set to **None** or **Trap**. **Shutdown**: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to **Shutdown** or **Trap & Shutdown**.

Buttons

: Click to apply changes

: Click to undo any changes made locally and revert to previously saved values.

: Click to refresh the page. Note that non-committed changes will be lost.

4.5.4.2 Port Security Status

This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

The status page is divided into two sections - one with a legend of user modules and one with the actual port status. The Port Security Status screen in Figure 4-5-16 appears.

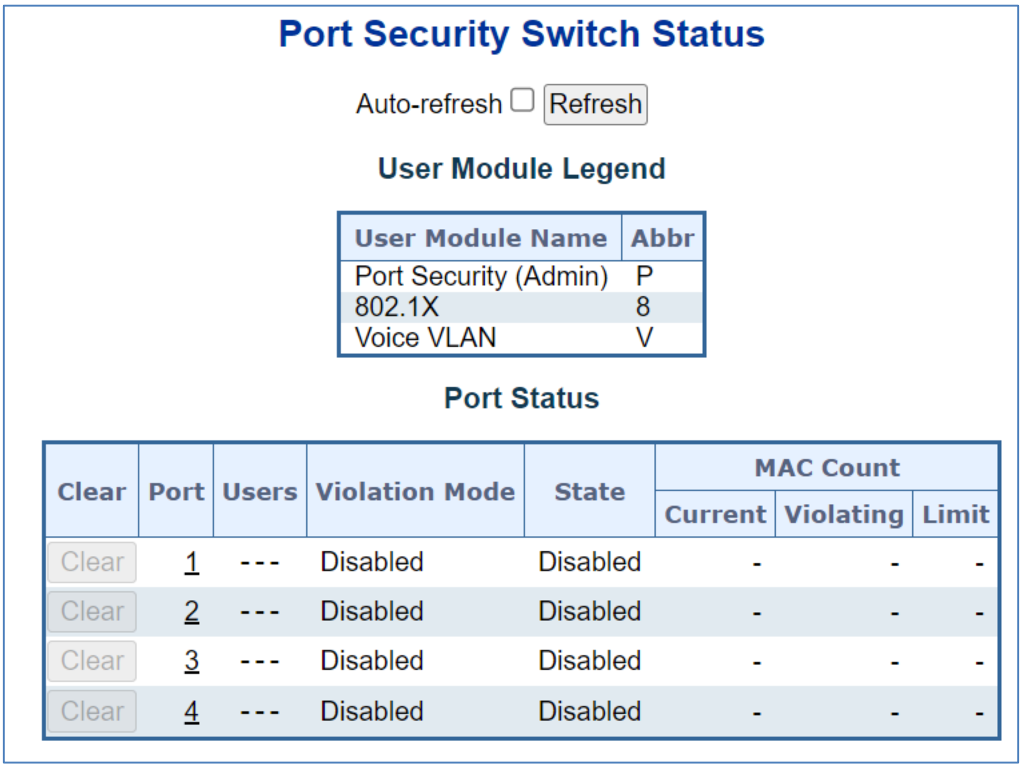


Figure 4-5-16: Port Security Status Screen Page Screenshot

The page includes the following fields:

User Module Legend

The legend shows all user modules that may request Port Security services.

Object	Description
• **User Module Name**	The full name of a module that may request Port Security services.
• **Abbr**	A one-letter abbreviation of the user module. This is used in the Users column in the port status table.

Port Status

The table has one row for each port on the selected switch in the switch and a number of columns, which are:

Object	Description
• **Clear**	Click to remove all MAC addresses on all VLANs on this port. The button is only clickable if number of secured MAC addresses is non-zero.
• **Port**	The port number for which the status applies. Click the port number to see the status for this particular port.
• **Users**	Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter has enabled port security.
• **Violation Mode**	Shows the configured Violation Mode of the port. It can take one of four values: **Disabled**: Port Security is not administratively enabled on this port. **Protect**: Port Security is administratively enabled in Protect mode. **Restrict**: Port Security is administratively enabled in Restrict mode. **Shutdown**: Port Security is administratively enabled in Shutdown mode.
• **State**	Shows the current state of the port. It can take one of four values: ■ **Disabled**: No user modules are currently using the Port Security service. ■ **Ready**: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive. ■ **Limit Reached**: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in. ■ **Shutdown**: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration web page.
• **MAC Count (Current, Limit)**	The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively. If no user modules are enabled on the port, the Current column will show a dash (-). If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4.5.4.3 Port Security Detail

This page shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise. The Port Security Detail screen in Figure 4-5-17 appears.

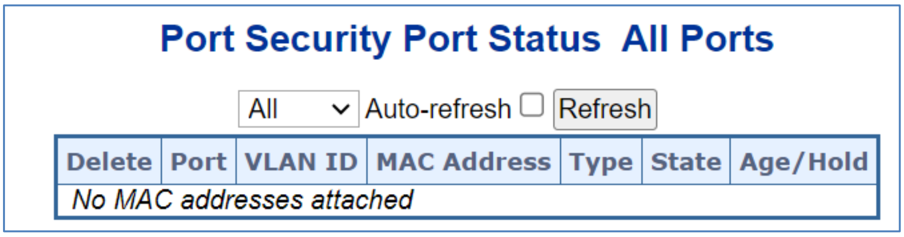


Figure 4-5-17: Port Security Detail Screen Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Click to remove this particular MAC addresses from MAC address table. The button is only clickable if the entry type is Dynamic. Use the "Configuration→Security→Port Security→MAC Addresses" page to remove Static and Sticky entries.
• **Port**	If all ports are shown (can be selected through the drop-down box on the top right), this one shows the port to which the MAC address is bound.
• **MAC Address & VLAN ID**	The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.
• **Type**	Indicates the type of entry. Takes one of three values: • **Dynamic**: The entry is learned through learn frames coming to the Port Security module while the port in question is not in sticky mode. • **Static**: The entry is entered by the end-user through management. Entry is not subject to aging. • **Sticky**: When the port is in sticky mode, all entries that would otherwise have been learned as dynamic are learned as sticky. Sticky entries are part of the running-config and can therefore be saved to startup-config. An important aspect of sticky MAC addresses is that they 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**	Indicates whether the corresponding MAC address is violating (administrative user has configured the interface in "Restrict" mode and the MAC address is blocked), blocked, or forwarding.
• **Age/Hold**	● If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. ● If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. ● If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin. ● If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4.5.4.4 MAC Address

On this page, you may add and delete static and sticky MAC addresses managed by Port Security.

Port security defines three types of MAC addresses, of which static and sticky can be added and removed on this page:

- **Dynamic**: A MAC address learned through learn frames coming to the Port Security module while the interface in qeustion is not in sticky mode. Dynamic entries disappear if it ages out or if the interface link goes down.
- **Static**: A MAC address added by end-user through management. Static MAC addresses are not subject to aging and will be added to the MAC address table once Port Security gets enabled on the interface.
  Static entries are part of the running-config and will survive interface link state changes and reboots if saved to startup-config. Static entries can be added to the running-config at any time whether or not Port Security is enabled.
- **Sticky**: When the interface is in sticky mode, all entries that would otherwise have been learned as dynamic are learned as sticky.
  Like static entries, sticky entries are part of the running-config and will survive interface link state changes and reboots if saved to the startup-config.
  Though not the intention with Sticky entries, they can be added by management to the running-config at any time whether or not Port Security is enabled on the interface, as long as the interface is in Sticky mode. Sticky entries will disappear if the interface is taken out of Sticky mode.

The MAC Address screen in Figure 4-5-18 appears.

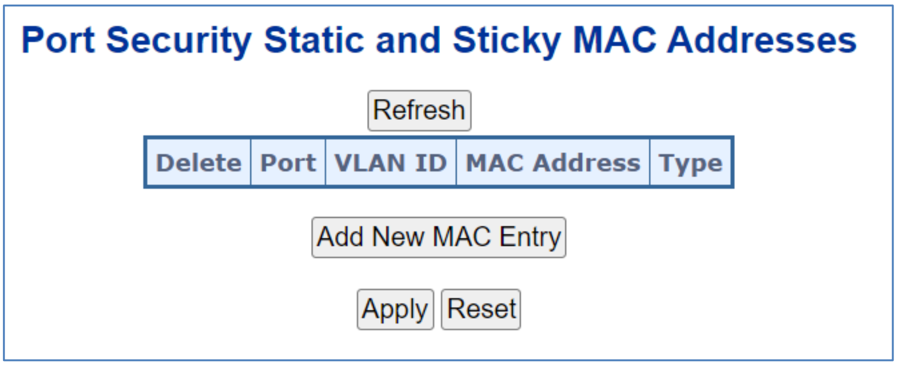


Figure 4-5-18: MAC Address Screen Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Press this button to remove the entry from the MAC address table (if present) and the running-config. Notice that dynamic entries may be removed all-together on an interface through "Monitor→Security→Port Security→Switch" and one-by-one through "Monitor→Security→Port Security→Port"
• **Port**	The port number to which this MAC address is bound.
• **VLAN ID & MAC Address**	The VLAN ID and MAC address in question.

• **Type**	Indicates the type of entry and may be either Static or Sticky (see description above).

Buttons

Add New MAC Entry: Clicking this button will add a new row to the table. This new row allows for adding a static or sticky MAC address to a particular interface. Once satisfied, click the Save-button to save the changes to running-config. Notice that sticky entries are normally added automatically through learning on the interface.

Refresh: Click to refresh the page. Note that non-committed changes will be lost.

Apply: Click to apply changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.5.5 Access Control Lists

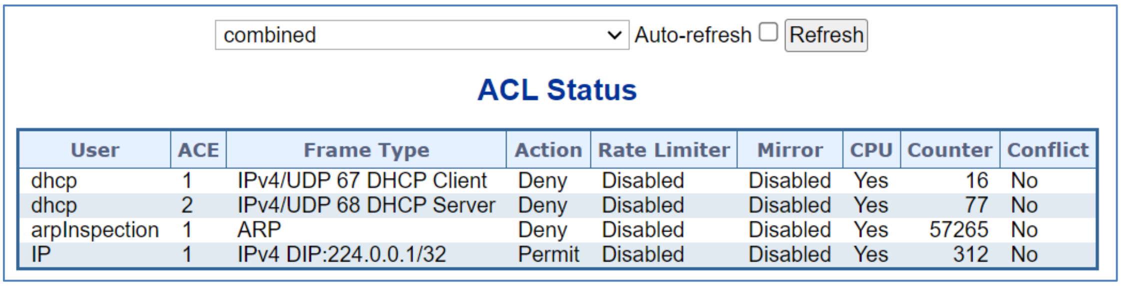
ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.
Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

ACE is an acronym for **Access Control Entry**. It describes access permission associated with a particular ACE ID.
There are three ACE frame types (**Ethernet Type**, **ARP**, and **IPv4**) and two ACE actions (**permit** and **deny**). The ACE also contains many detailed, different parameter options that are available for individual application.

4.5.5.1 Access Control List Status

This page shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is **512** on each switch. The Voice VLAN OUI Table screen in Figure 4-5-19 appears.



User	ACE	Frame Type	Action	Rate Limiter	Mirror	CPU	Counter	Conflict
dhcp	1	IPv4/UDP 67 DHCP Client	Deny	Disabled	Disabled	Yes	16	No
dhcp	2	IPv4/UDP 68 DHCP Server	Deny	Disabled	Disabled	Yes	77	No
arpInspection	1	ARP	Deny	Disabled	Disabled	Yes	57265	No
IP	1	IPv4 DIP:224.0.0.1/32	Permit	Disabled	Disabled	Yes	312	No

Figure 4-5-19: ACL Status Page Screenshot

The page includes the following fields:

Object	Description
• **User**	Indicates the ACL user.
• **ACE**	Indicates the ACE ID on local switch.
• **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.
• **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.
• **CPU**	Forward packet that matched the specific ACE to CPU
• **Counter**	The counter indicates the number of times the ACE was hit by a frame.
• **Conflict**	Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

4.5.5.2 Access Control List Configuration

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. The Access Control List Configuration screen in Figure 4-5-20 appears.

Figure 4-5-20: Access Control List Configuration Page Screenshot

The page includes the following fields:

Object	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.
• **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**	pecify 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.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh : Click to refresh the page; any changes made locally will be undone.

Clear : Click to clear the counters.

Remove All : Click to remove all ACEs.

4.5.5.3 ACL Ports Configuration

Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE. The ACL Ports Configuration screen in Figure 4-5-21 appears.

ACL Ports Configuration

Refresh Clear

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	<>	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	8732
4	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	863063

Apply Reset

Figure 4-5-21: ACL Ports Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The logical port for the settings contained in the same row.
• **Policy ID**	Select the policy to apply to this port. The allowed values are **0** through **255**. The default value is 0.
• **Action**	Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".
• **Rate Limiter ID**	Select which rate limiter to apply on this port. The allowed values are **Disabled** or the values **1** through **16**. The default value is "Disabled".
• **Port Redirect**	Select which port frames are redirected on. The allowed values are Disabled or a specific port number and it can't be set when action is permitted. The default value is "Disabled".
• **Mirror**	Specify the mirror operation of this 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".
• **Logging**	Specify the logging operation of this port. The allowed values are: ■ **Enabled**: Frames received on the port are stored in the System Log. ■ **Disabled**: Frames received on the port are not logged. The default value is "Disabled". Please note that the System Log memory size and logging rate are limited.
• **Shutdown**	Specify the port shut down operation of this port. The allowed values are: ■ **Enabled**: If a frame is received on the port, the port will be disabled. ■ **Disabled**: Port shut down is disabled.

	The default value is "Disabled".
• **State**	Specify the port state of this port. The allowed values are: ■ **Enabled**: To reopen ports by changing the volatile port configuration of the ACL user module. ■ **Disabled**: To close ports by changing the volatile port configuration of the ACL user module. The default value is "Enabled".
• **Counter**	Counts the number of frames that match this ACE.

Buttons

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

Refresh: Click to refresh the page; any changes made locally will be undone.

Clear: Click to clear the counters.

4.5.5.4 ACL Rate Limiters

Configure the rate limiter for the ACL of the switch.

The ACL Rate Limiter Configuration screen in Figure 4-5-22 appears.

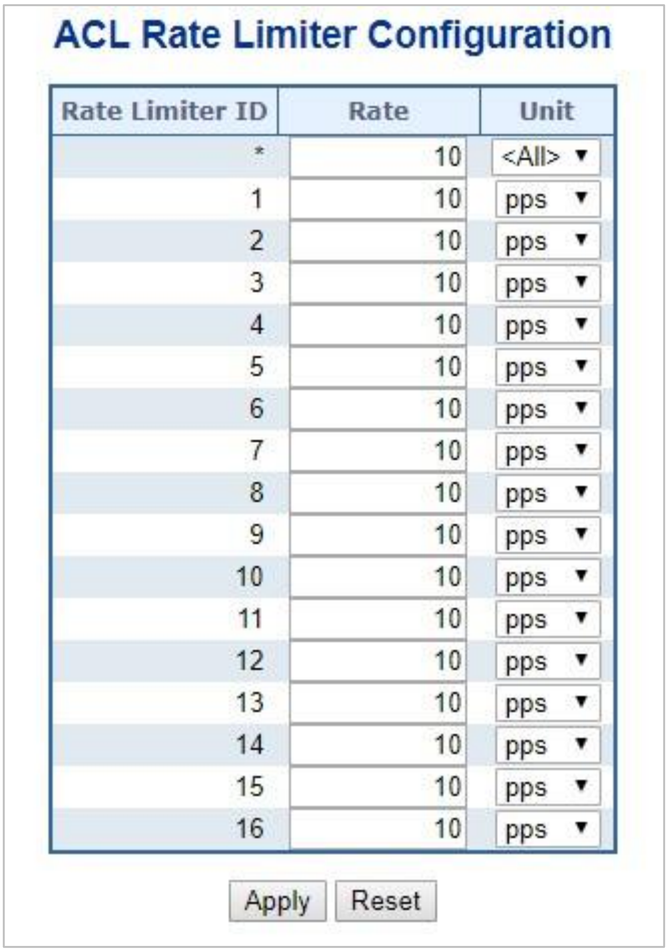


Figure 4-5-22: ACL Rate Limiter Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Rate Limiter ID**	The rate limiter ID for the settings contained in the same row.
• **Rate (pps)**	The allowed values are: **0-3276700** in pps or **0, 100, 200, 300, ..., 1000000** in kbps.
• **Unit**	Specify the rate unit. The allowed values are: **pps**: packets per second. **kbps**: Kbits per second.

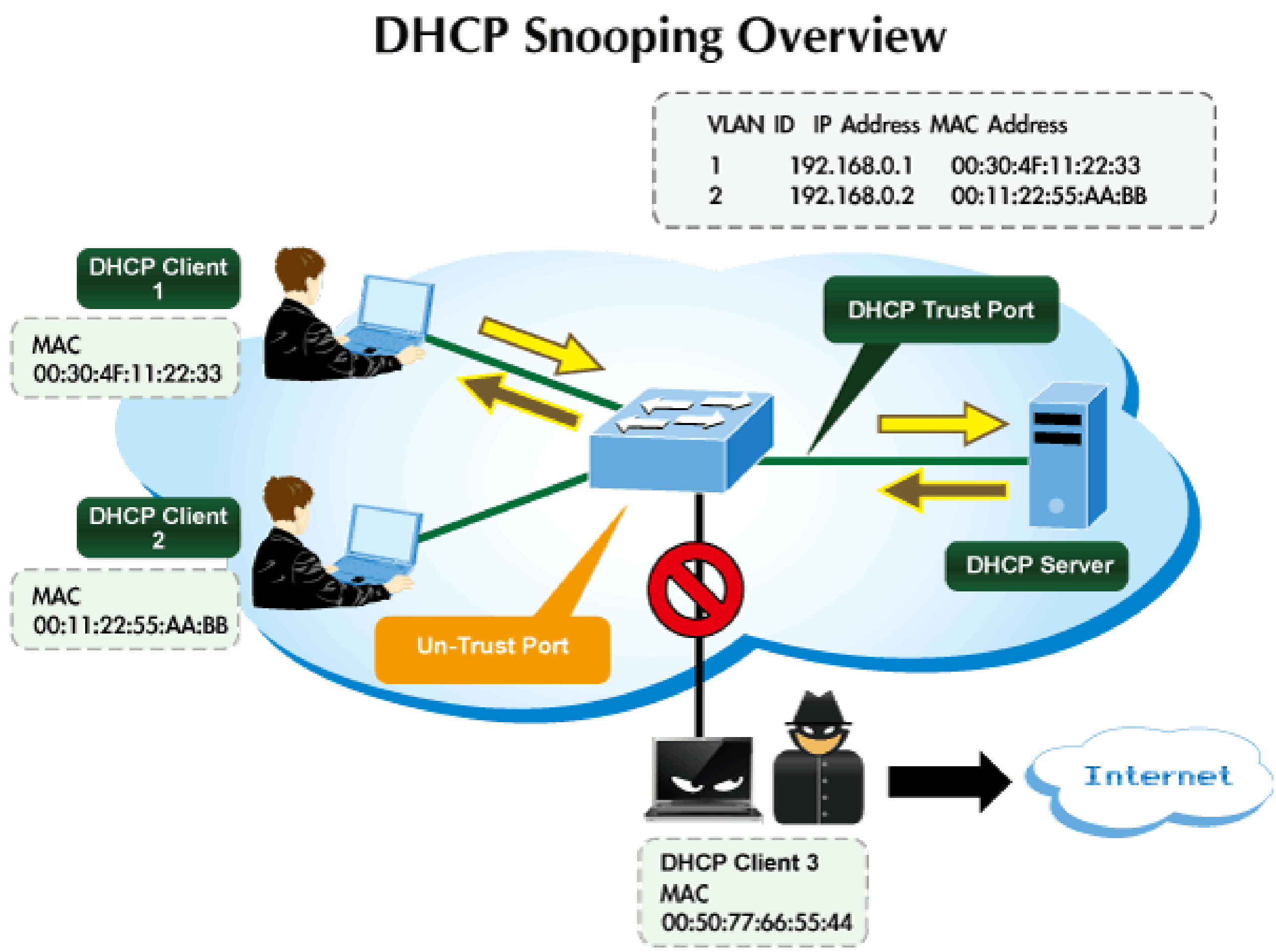
Buttons

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.5.6 DHCP Snooping

DHCP Snooping is used to block intruder on the untrusted ports of DUT when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.



4.5.6.1 DHCP Snooping Configuration

Configure DHCP Snooping on this page. The DHCP Snooping Configuration screen in Figure 4-5-23 appears.

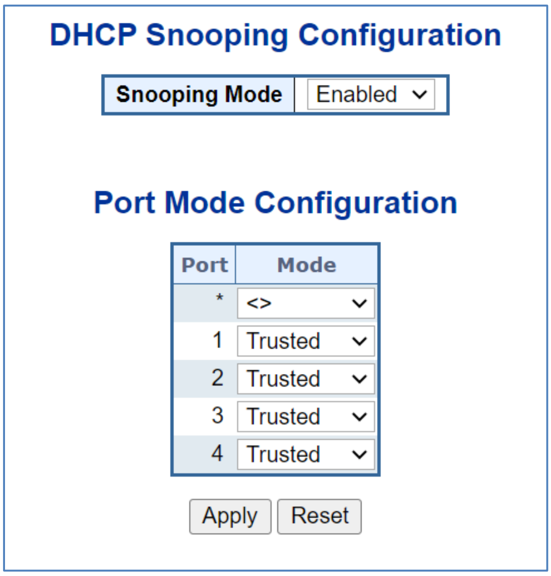


Figure 4-5-23: DHCP Snooping Configuration Screen Page Screenshot

The page includes the following fields:

Object	Description
• **Snooping Mode**	Indicates the DHCP snooping mode operation. Possible modes are: ■ **Enabled**: Enable DHCP snooping mode operation. When enable DHCP snooping mode operation, the request DHCP messages will be forwarded to trusted ports and only allowed reply packets from trusted ports. ■ **Disabled**: Disable DHCP snooping mode operation.
• **Port Mode Configuration**	Indicates the DHCP snooping port mode. Possible port modes are: ■ **Trusted**: Configures the port as trusted sources of the DHCP message. ■ **Untrusted**: Configures the port as untrusted sources of the DHCP message.

Buttons

: Click to apply changes

: Click to undo any changes made locally and revert to previously saved values.

4.5.6.2 Snooping Table

This page display the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCP clients obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP snooping Table are shown on this page. The Dynamic DHCP Snooping Table screen in Figure 4-5-24 appears.

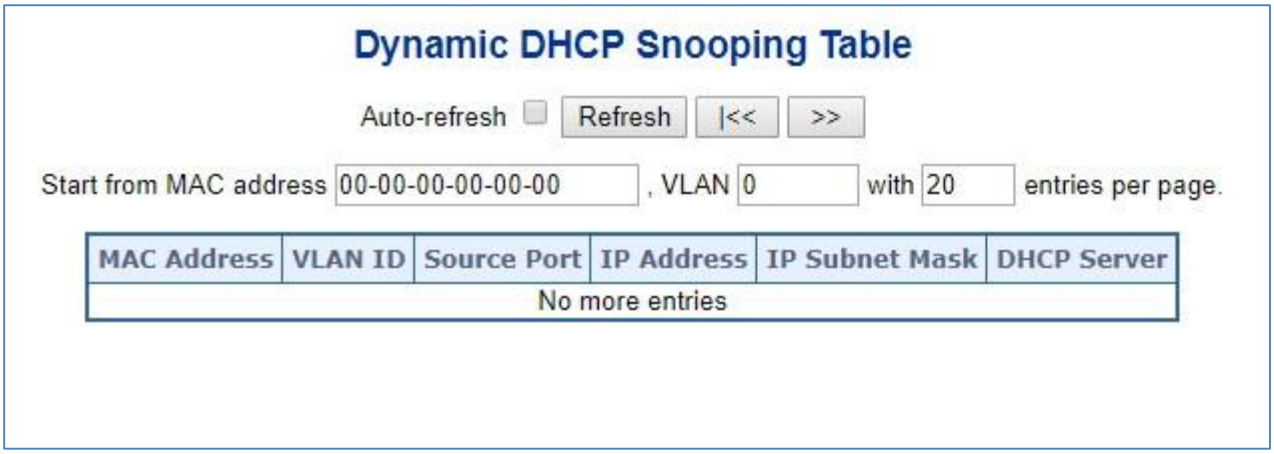


Figure 4-5-24: Dynamic DHCP Snooping Table Screen Page Screenshot

Object	Description
• **MAC Address**	User MAC address of the entry.
• **VLAN ID**	VLAN-ID in which the DHCP traffic is permitted.
• **Source Port**	Switch Port Number for which the entries are displayed.
• **IP Address**	User IP address of the entry.
• **IP Subnet Mask**	User IP subnet mask of the entry.
• **DHCP Server Address**	DHCP Server address of the entry.

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Refreshes the displayed table starting from the input fields

Clear: Flushes all dynamic entries.

>>: It will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table

|<<: To start over

4.5.7 DHCPv6 Snooping

4.5.7.1 DHCPv6 Snooping Configuration

Configure DHCPv6 (aka. DHCP over IPv6) Snooping on Figure 4-5-25 page.

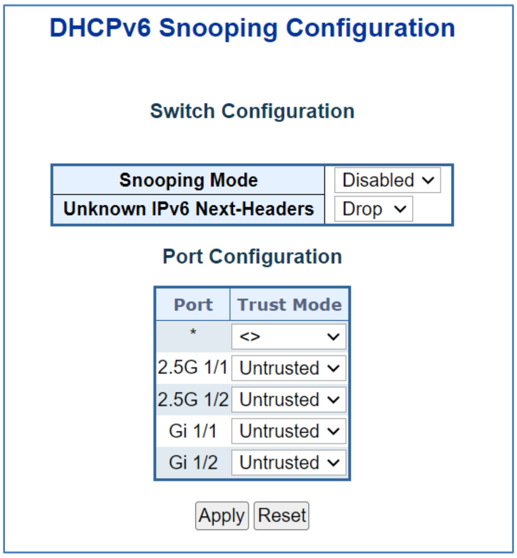


Figure 4-5-25: DHCPv6 Snooping Table Configuration Screen Page Screenshot

The displayed settings are:

Object	Description
• **Snooping Mode**	Indicates the DHCPv6 snooping mode operation. Possible modes are: Enabled: Enable DHCPv6 snooping mode operation. When DHCPv6 snooping mode operation is enabled, the DHCPv6 client request messages will be forwarded to trusted ports and only allow reply packets from trusted ports. Disabled: Disable DHCP snooping mode operation.
• **Unknown IPv6 Next-Headers**	Indicates how Unknown IPv6 Next-Header values should be treated. The switch needs to parse all IPv6 packets to a DHCPv6 client to determine if it is in fact a DHCPv6 message. If an unknown IPv6 extension header is encountered the parsing cannot continue. See RFC 7610, section 5, item 3 for details. Possible options are: Drop: Drop packets with unknown IPv6 extension headers. This is the most secure option but may result in traffic disruptions. Allow: Allow packets with unknown IPv6 extension headers. This is a less secure option but prevents traffic disruptions.
• **Port Mode Configuration**	Indicates the DHCPv6 snooping port mode. Possible port modes are: Trusted: Configures the port as trusted source of the DHCPv6 messages. Untrusted: Configures the port as untrusted source of the DHCPv6 messages.

4.5.8 IP Source Guard

4.5.8.1 IP Source Guard Configuration

IP Source Guard is a secure feature used to restrict IP traffic on **DHCP snooping untrusted ports** by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host. This page provides IP Source Guard related configuration. The IP Source Guard Configuration screen in Figure 4-5-26 appears.

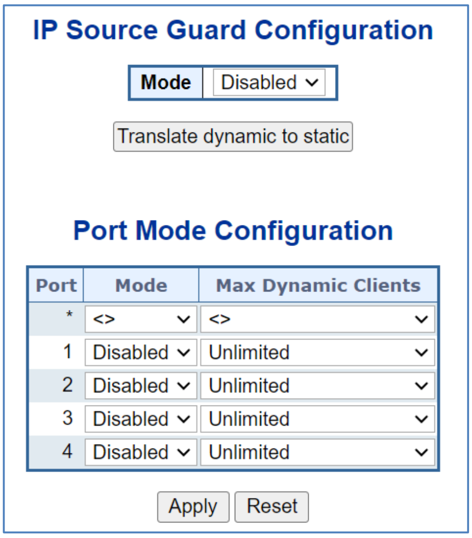


Figure 4-5-26: IP Source Guard Configuration Screen Page Screenshot

The page includes the following fields:

Object	Description
• **Mode of IP Source Guard Configuration**	Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.
• **Port Mode Configuration**	Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.
• **Max Dynamic Clients**	Specify the maximum number of dynamic clients can be learned on given ports. This value can be 0, 1, 2 and unlimited. If the port mode is enabled and the value of max dynamic client is equal 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port.

Buttons

Translate Dynamic to Static: Click to translate all dynamic entries to static entries.

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.5.8.2 Static IP Source Guard Table

This page provides Static IP Source Guard Table. The Static IP Source Guard Table screen in Figure 4-5-27 appears.

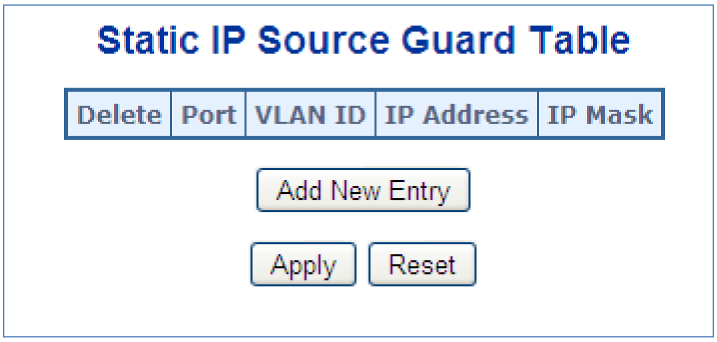


Figure 4-5-27: Static IP Source Guard Table Screen Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Port**	The logical port for the settings.
• **VLAN ID**	The VLAN ID for the settings.
• **IP Address**	Allowed Source IP address.
• **MAC Address**	Allowed Source MAC address.

Buttons

: Click to add a new entry to the Static IP Source Guard table.

: Click to apply changes

: Click to undo any changes made locally and revert to previously saved values.

4.5.8.3 Dynamic IP Source Guard Table

This page provides Static IP Source Guard Table. The Static IP Source Guard Table screen in Figure 4-5-28 appears.

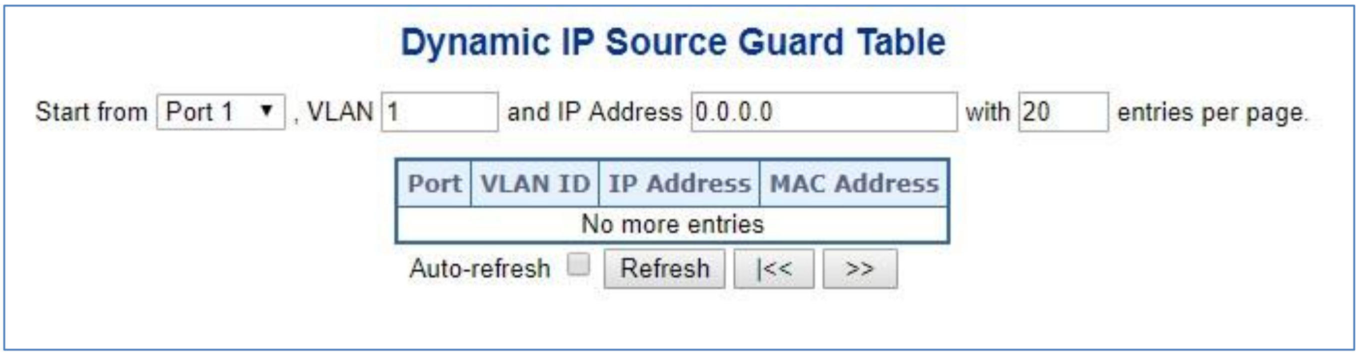


Figure 4-5-28: Static IP Source Guard Table Screen Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	Switch Port Number for which the entries are displayed.
• **VLAN ID**	VLAN-ID in which the IP traffic is permitted.
• **IP Address**	User IP address of the entry.
• **MAC Address**	Source MAC address.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds

Refresh: Refreshes the displayed table starting from the input fields..

Clear: Flushes all dynamic entries.

>>: Updates the table starting from the first entry in the Dynamic IP Source Guard Table.

|<<: Updates the table, starting with the entry after the last entry currently displayed.

4.5.9 IPv6 Source Guard

4.5.9.1 IPv6 Source Guard Configuration

This page provides IPv6 Source Guard related configuration. The IPv6 Source Guard Configuration screen in Figure 4-5-29 appears.

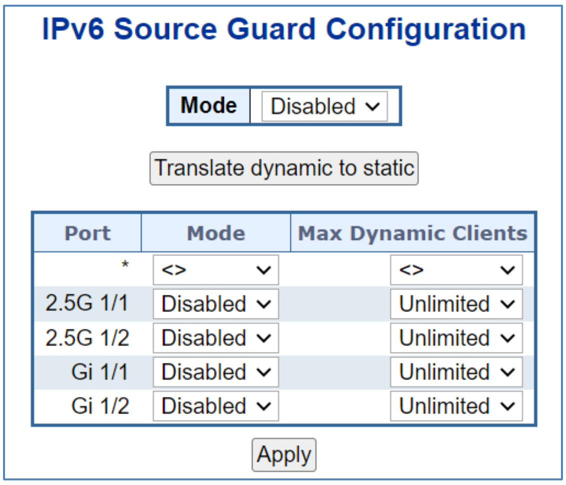
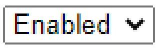


Figure 4-5-29: IPv6 Source Guard Configuration Screen Page Screenshot

The displayed settings are:

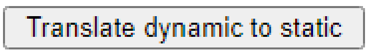
Object	Description
• **IPv6 Source Guard Mode Configuration**	Enable or disable the IPv6 Source Guard globally.
• **Port Mode Configuration**	The table shows all ports on the device. There IPv6 Source Guard can be enabled/disabled on individual ports. Only when both Global Mode and Port Mode on a given port are enabled, IPv6 Source Guard is enabled on this given port.
• **Max Dynamic Clients**	Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, only IPv6 packets that are matched in static entries on the specific port are forwarded.

Buttons



: Toggle to change global mode.

: Click to apply changes



: Click to translate all dynamic entries to static entries.

4.5.9.2 IPv6 Source Guard Static Table

This page shows the static IPv6 Source Guard entries. The maximum number of entries is 112 on the switch. The IPv6 Source Guard Static Table screen in Figure 4-5-30 appears.

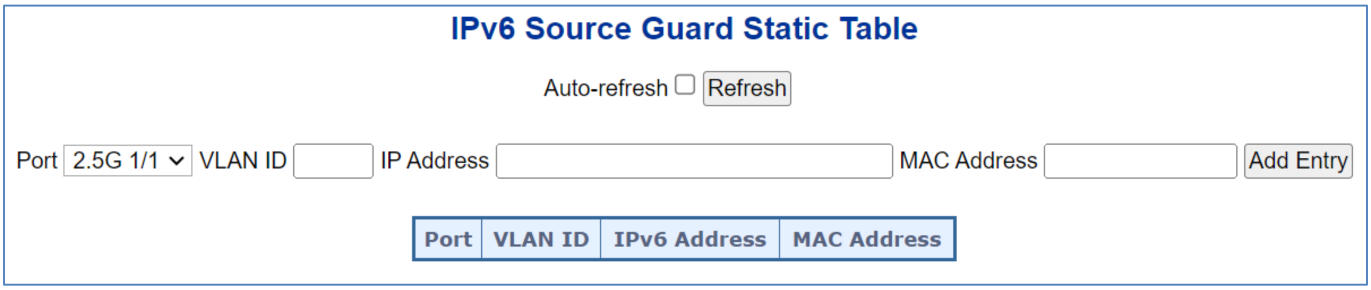


Figure 4-5-30: IPv6 Source Guard Static Table Screen Page Screenshot

The displayed settings are:

Object	Description
• **Delete**	Click entry Delete button to delete the entry.
• **Port**	The logical port the entry is bound to.
• **VLAN ID**	The VLAN Id for the entry. If no VLAN Id is associated with the entry, this field shows 0.
• **IPv6 Address**	Allowed Source IPv6 address.
• **Prefix Size**	Prefix size of the IPv6 address.
• **MAC Address**	Allowed Source MAC address.

Buttons

Gi 1/1 : Toggle to select entry port.

Add Entry : Click to add a new entry to the Static IPv6 Source Guard table.

Auto-refresh : Check this box to refresh the page automatically.

Refresh : Refreshes the display table.

4.5.9.3 IP Source Guard Table

Entries in the Dynamic IPv6 Source Guard Table are shown on this page. All dynamic entries are shown in the table which can be scrolled up and down when the number of entries exeeds the space allotted for the table.

The IPv6 Source Guard Dynamic Table screen in Figure 4-5-31 appears.

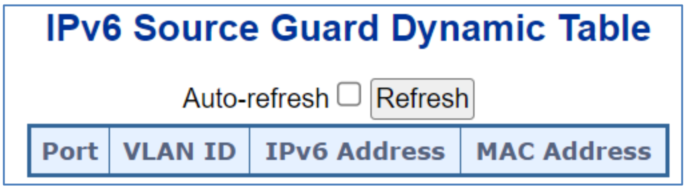


Figure 4-5-31: IPv6 Source Guard Dynamic Table Screen Page Screenshot

The displayed settings are:

Object	Description
• **Port**	Switch Port Number to which the entries are bound.
• **VLAN ID**	VLAN-ID in which the IP traffic is permitted. If no VLAN-ID is associated with the entry, this field shows 0.
• **IPv6 Address**	Source IPv6 address of the entry.
• **MAC Address**	Source MAC address.

Buttons

Auto-refresh : Check this box to refresh the page automatically.

Refresh : Refreshes the display table.

4.5.10 ARP Inspection

4.5.10.1 ARP Inspection

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through DUT. This page provides ARP Inspection related configuration. The ARP Inspection Configuration screen in Figure 4-5-32 appears.

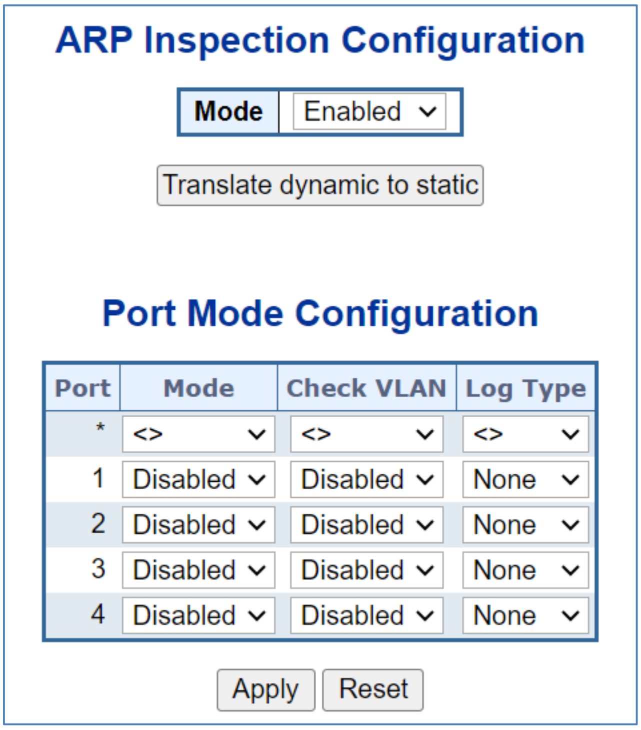


Figure 4-5-32: ARP Inspection Configuration Screen Page Screenshot

The page includes the following fields:

Object	Description
• **Mode of ARP Inspection Configuration**	Enable the Global ARP Inspection or disable the Global ARP Inspection.
• **Port Mode Configuration**	Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Possible **modes** are: ■ **Enabled**: Enable ARP Inspection operation. ■ **Disabled**: Disable ARP Inspection operation. If you want to inspect the VLAN configuration, you have to enable the setting of "**Check VLAN**". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of

	ARP Inspection will refer to the VLAN setting. Possible setting of "**Check VLAN**" are: ■ **Enabled**: Enable check VLAN operation. ■ **Disabled**: Disable check VLAN operation. Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. There are four **log types** and possible types are: ■ **None**: Log nothing. ■ **Deny**: Log denied entries. ■ **Permit**: Log permitted entries. ■ **ALL**: Log all entries.

Buttons

[Translate Dynamic to Static]: Click to translate all dynamic entries to static entries.

[Apply]: Click to apply changes

[Reset]: Click to undo any changes made locally and revert to previously saved values.

4.5.10.2 VLAN Configuration

This page provides ARP Inspection related configuration. Each page shows up to 9999 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the Refresh button will update the displayed table starting from that or the closest next VLAN Table match. The >> will use the next entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the warning message is shown in the displayed table. Use the |<< button to start over.The VLAN Mode Configuration screen in Figure 4-5-33 appears.

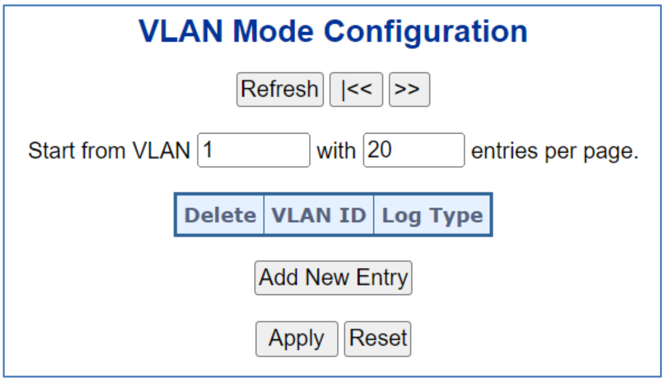


Figure 4-5-33: Static ARP Inspection Table Screen Page Screenshot

Specify ARP Inspection is enabled on which VLANs. First, you have to enable the port setting on Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN will be inspected on VLAN mode configuration web page. The log type also can be configured on per VLAN setting.

Possible types are:

None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

ALL: Log all entries.

Buttons

Add New Entry: Click to add a new VLAN to the ARP Inspection VLAN table.

Apply: Click to apply changes

Reset: Click to undo any changes made locally and revert to previously saved values.

4.5.10.3 ARP Inspection Static Table

This page provides Static ARP Inspection Table. The Static ARP Inspection Table screen in Figure 4-5-34 appears.

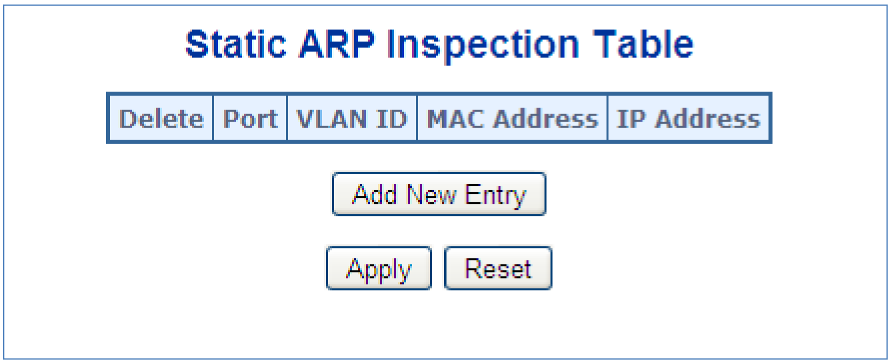


Figure 4-5-34: Static ARP Inspection Table Screen Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Port**	The logical port for the settings.
• **VLAN ID**	The VLAN ID for the settings.
• **MAC Address**	Allowed Source MAC address in ARP request packets.
• **IP Address**	Allowed Source IP address in ARP request packets.

Buttons

: Click to add a new entry to the Static ARP Inspection table.

: Click to apply changes

: Click to undo any changes made locally and revert to previously saved values.

4.5.10.4 Dynamic ARP Inspection Table

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address. The Dynamic ARP Inspection Table screen in Figure 4-5-35 appears.

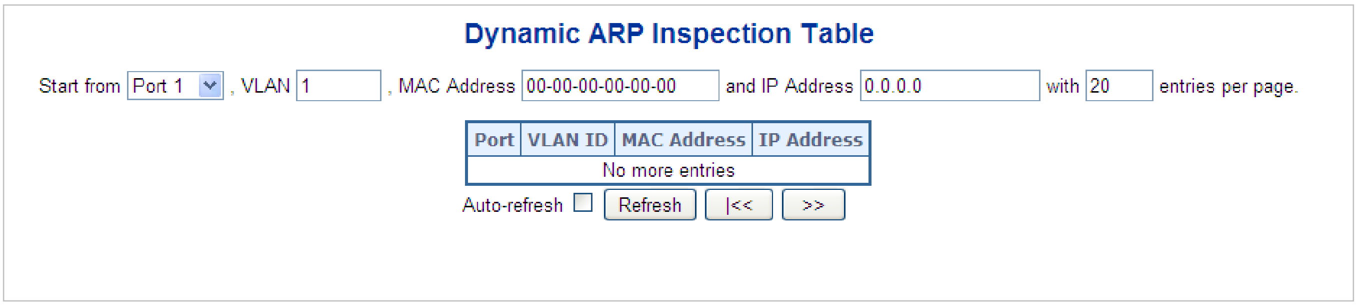


Figure 4-5-35: Dynamic ARP Inspection Table Screenshot

Navigating the ARP Inspection Table

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "**entries per Page**" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

The "**Start from port address**", "**VLAN**", "**MAC address**" and "**IP address**" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the "**Refresh**" button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a "**Refresh**" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The "**>>**" will use the last entry of the currently displayed as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "**|<<**" button to start over. The page includes the following fields:

Object	Description
• **Port**	The port number for which the status applies. Click the port number to see the status for this particular port.
• **VLAN ID**	The VLAN ID of the entry.
• **MAC Address**	The MAC address of the entry.
• **IP Address**	The IP address of the entry.

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.

Clear: Flushes all dynamic entries.

|<<: Updates the table starting from the first entry in the MAC Table, i.e. the entry with the lowest VLAN ID and MAC address.

>>: Updates the table, starting with the entry after the last entry currently displayed.

4.6 Ring

4.6.1 Ring Wizard

This page is on ring wizard and it is an interface for user to configure ERPS ring feature.

This wizard uses the fixed ring topology to indicate the ring owner, so if user needs to indicate the other switch to the ring owner or modify the ring topology, please modify MEP and ERPS settings manually.

If user wants to enable the ERPS ring, please disable the DHCP client feature and indicate the ring port that cannot be the Spanning Tree port.

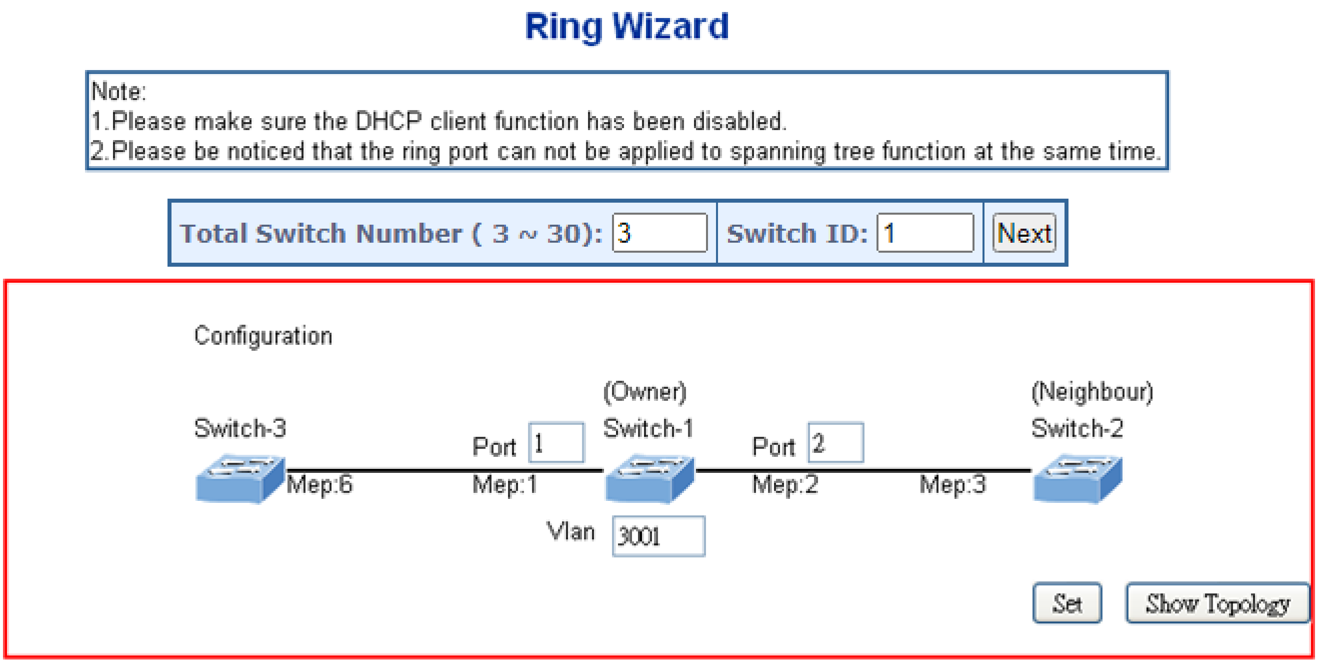
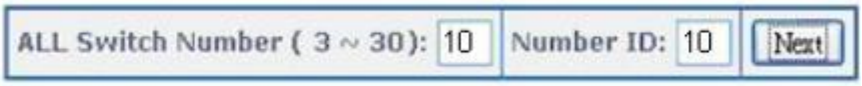


Figure 4-6-1: Ring Wizard page screenshot

The page includes the following fields:

Object	Description
• **All Switch Numbers (3 ~ 30)**	This option is for you to input a number to show how many switches will be used for the single ring. Ring wizard needs at least 3 switches for configuring and the maximum number is 30.
• **Number ID**	This option is for you to input a number that the ID of the switch you are setting for the single ring. For example, a single ring is grouped by 10 switches. If you want to set the ERPS ring wizard from the 2nd switch, you will have to input 2 for the Number ID option.
• **Next Button**	When you press the "Next" button, the system is going to generate the ERPS ring setting according to your setting.

• **Ring Wizard Setting Example**	[10 Switches For Single Ring] 1.We will create a ring by 10 switches and we are configuring the first switch, so the configuration should be as follows:  2.We are creating a ring that it is built by 10 switches and we are configuring the 2nd switch.  3.We are creating a ring that it is built by 10 switches and we are configuring the 10th switch. 

Ring Wizard Example:

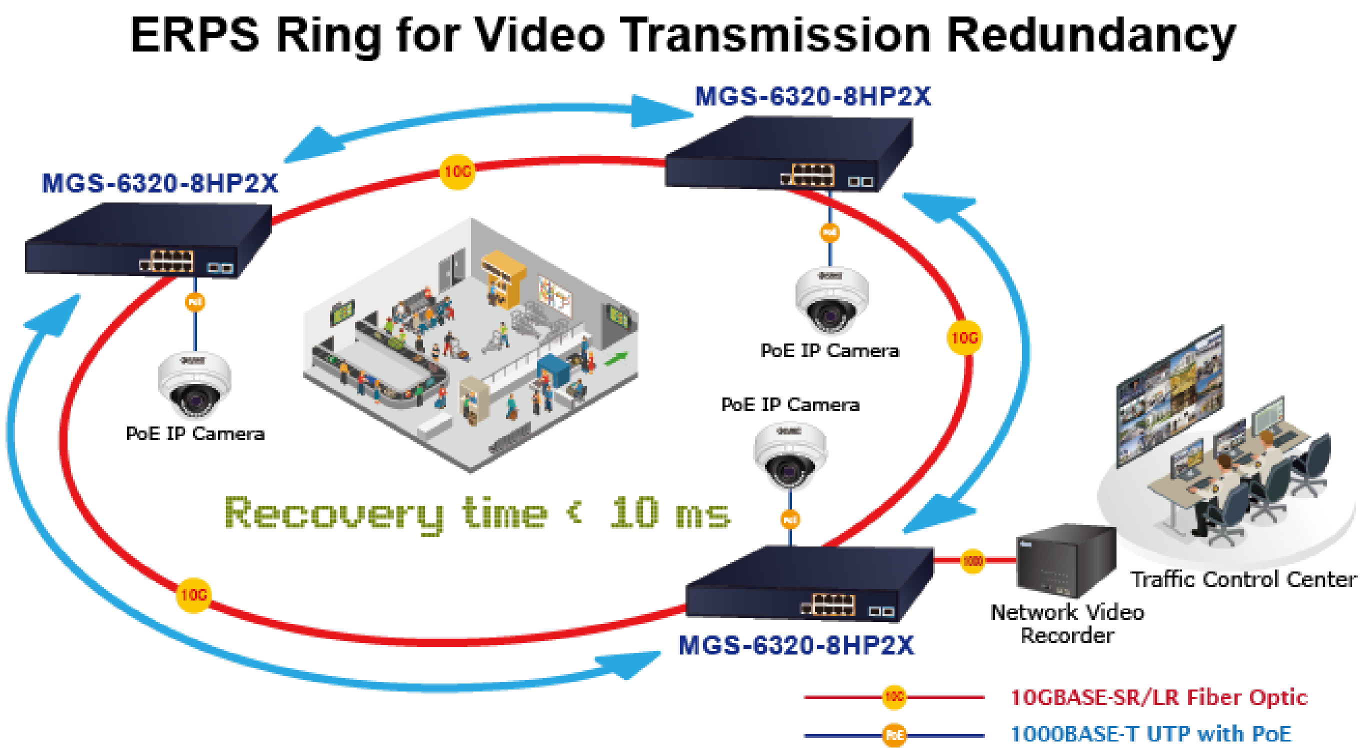


Figure 4-6-2: Ring Example Diagram

The above topology often occurs on using ERPS protocol. The multi switch constitutes a single ERPS ring; all of the switches only are configured as an ERPS in VLAN 3001, thereby constituting a single MRPP ring.

Switch ID	Port	MEP ID	RPL Type	VLAN Group
Switch 1	Port 1	1	None	3001
	Port 2	2	**Owner**	3001
Switch 2	Port 1	4	None	3001
	Port 2	3	**Neighbor**	3001
Switch 3	Port 1	6	None	3001
	Port 2	5	None	3001

Table 4-6-1: ERPS Configuration Table

The scenario described as follows:

1. Disable DHCP client and set proper static IP for Switch 1, 2 & 3. In this example, switch 1 is 192.168.0.101; switch 2 is 192.168.0.102 and switch 3 is 192.168.0.103.
2. On switch 1, 2 & 3, disable spanning tree protocol to avoid confliction with ERPS.

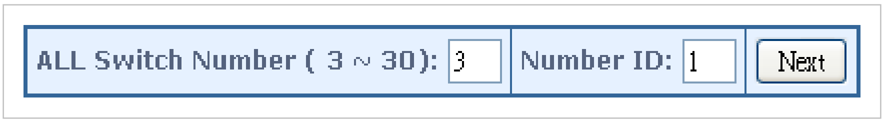
Setup steps

Set ERPS Configuration on Switch 1

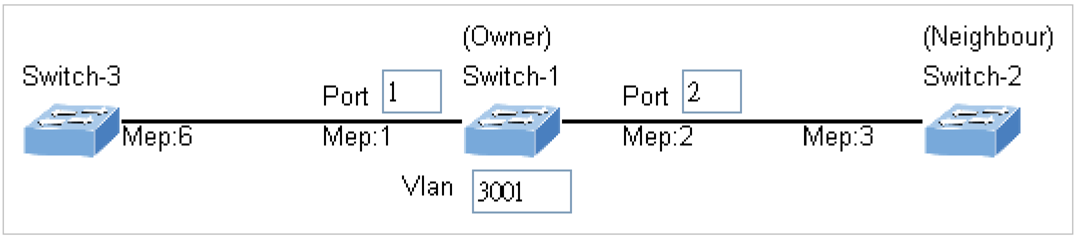
Connect PC to switch 1 directly; don't connect to port 1 & 2

Logging on the Switch 1 and click "Ring > Ring Wizard"

Set "All Switch Number" = 3 and "Number ID" = 1; click "Next" button to set the ERPS configuration for Switch 1.



Set "MEP1" = Port1, "MEP2" = Port2 and VLAN ID = 3001; click "Set" button to save the ERPS configuration for Switch 1.

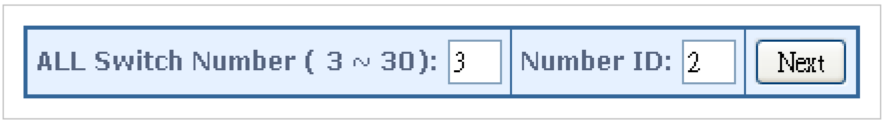


Set ERPS Configuration on Switch 2

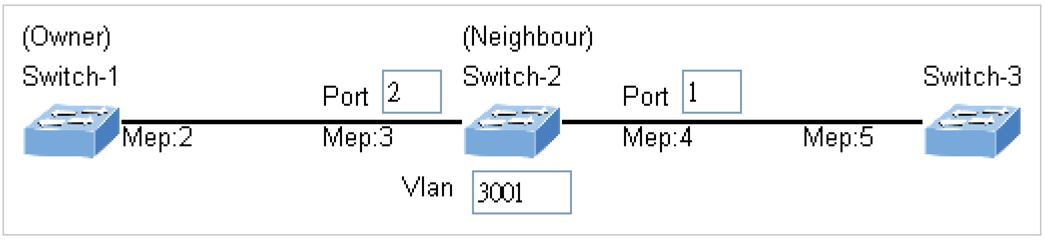
Connect PC to switch 2 directly; don't connect to port 1 & 2

Logging on the Switch 2 and click "Ring > Ring Wizard"

Set "All Switch Number" = 3 and "Number ID" = 2; click "Next" button to set the ERPS configuration for Switch 2.



Set "MEP3" = Port2, "MEP4" = Port1 and VLAN ID = 3001; click "Set" button to save the ERPS configuration for Switch 2.

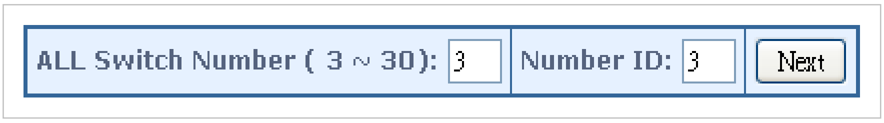


Set ERPS Configuration on Switch 3

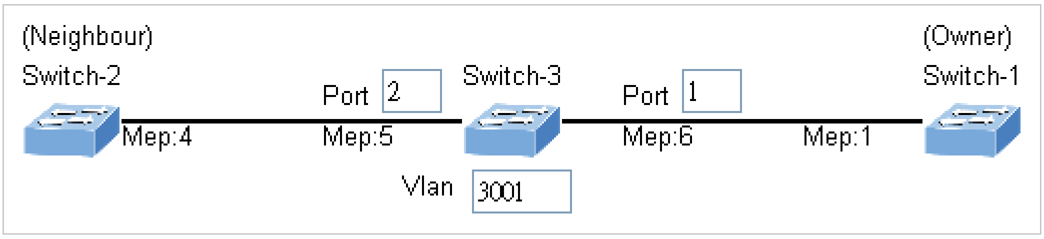
Connect PC to switch 3 directly; don't connect to port 1 & 2

Logging on the Switch 3 and click "Ring > Ring Wizard"

Set "All Switch Number" = 3 and "Number ID" = 3; click "Next" button to set the ERPS configuration for Switch 3.



Set "MEP5" = Port2, "MEP6" = Port1 and VLAN ID = 3001; click "Set" button to save the ERPS configuration for Switch 3.



Note

To avoid loop, please don't connect switch 1, 2 & 3 together in the ring topology before configuring the end of ERPS .

Follow the configuration or ERPS wizard to connect the Switch 1, 2 and 3 together to establish ERPS application:

MEP2 ⟷ MEP3 = Switch1 / Port2 ⟷ Switch2 / Port2

MEP4 ⟷ MEP5 = Switch2 / Port1 ⟷ Switch3 / Port2

MEP1 ⟷ MEP6 = Switch1 / Port1 ⟷ Switch3 / Port1

4.6.2 ERPS

The ERPS instances are configured here.

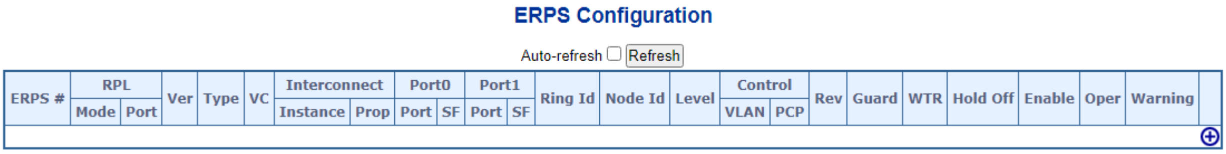


Figure 4-6-3: ERPS Configuration Screen Page Screenshot

The page includes the following fields:

Object	Description
• **ERPS #**	The ID of ERPS. Valid range 1 - 64
• **RPL Mode**	Ring Protection Link mode. Possible values: None: Owner: Neighbor:
• **RPL Port**	Indicates whether it is port0 or port1 that is the Ring Protection Link. Not used if RPL Mode is None.
• **Ver**	ERPS protocol version. v1 and v2 are supported
• **Type**	Type of ring. Possible values: Major: ERPS major ring (G.8001-2016, clause 3.2.39) Sub: ERPS sub-ring (G.8001-2016, clause 3.2.66) InterSub: ERPS sub-ring on an interconnection node (G.8001-2016, clause 3.2.66)
• **VC**	Controls whether to use a Virtual Channel with a sub-ring
• **Interconnect Instance**	For a sub-ring on an interconnection node, this must reference the instance ID of the ring to which this sub-ring is connected.
• **Interconnect Prop**	Controls whether the ring referenced by Interconnect Instance shall propagate R-APS flush PDUs whenever this sub-ring's topology changes.
• **Port0/Port1 Interface**	Interface index of ring protection Port0/Port1.
• **Port0/Port1 SF**	Selects whether Signal Fail (SF) comes from the link state of a given interface, or from a Down-MEP. Possible values: MEP: Down-MEP Link: Link
• **Ring Id**	The Ring ID is used - along with the control VLAN - to identify R-APS PDUs as belonging to a particular ring.
• **Node Id**	The Node ID is used inside the R-APS specific PDU to uniquely identify this node (switch) on the ring.

• **Level**	MD/MEG Level of R-APS PDUs we transmit.
• **Control VLAN**	The VLAN on which R-APS PDUs are transmitted and received on the ring ports.
• **Control PCP**	The PCP value used in the VLAN tag of the R-APS PDUs.
• **Rev**	Revertive (true) or Non-revertive (false) mode.
• **Guard**	Guard time in ms. Valid range is 10 - 2000 ms.
• **WTR**	"Wait-to-Restore time in seconds. Valid range 1 - 720 sec.
• **Hold Off**	Hold off time in ms. Value is rounded down to 100ms precision. Valid range is 0 - 10000 ms.
• **Enable**	The administrative state of this APS ERPS. Check to make it function normally and uncheck to make it cease functioning.
• **Oper**	The operational state of ERPS instance. : Active : Disabled or Internal error.
• **Warning**	Operational warnings of ERPS instance. : No warnings : There are warnings, use tooltip to see.
• **Configuration Buttons**	You can modify each ERPS in the table using the following buttons: : Edits the ERPS row. : Deletes the ERPS. : Adds new ERPS.

Buttons

Auto-refresh : Check this box to refresh the page automatically.

Refresh : Click to refresh the page immediately.

4.6.3 ERPS Status

This shows the current status of the ERPS instances screen in Figure 4-6-4 appears.

ERPS Status

Auto-refresh ☐ Refresh

ERPS #	Oper	Warning	State	TxRapsActive	cFOPTo	Tx Info							
						UpdateTimeSecs	Request	Version	Rb	Dnf	Bpr	Node Id	SMAC
No entry exists													

Figure 4-6-4: ERPS current status Screen Page Screenshot

The page includes the following fields:

Object	Description
• **ERPS #**	The ID of the ERPS. Click on link to get to ERPS detailed instance page, you can reset counters and issue commands.
• **Oper**	The operational state of ERPS instance. : Active : Disabled or Internal error.
• **Warning**	Operational warnings of ERPS instance. : No warnings : There are warnings, use tooltip to see.
• **State**	Specifies protection/node state of ERPS.
• **TxRapsActive**	Specifies whether we are currently supposed to be transmitting R-APS PDUs on our ring ports.
• **cFOPTo**	Failure of Protocol - R-APS Rx Time Out.
• **UpdateTimeSecs**	Time in seconds since boot that this structure was last updated.
• **Request**	Request/state according to G.8032, table 10-3.
• **Version**	Version of received/used R-APS Protocol. 0 means v1, 1 means v2, etc.
• **Rb**	RB (RPL blocked) bit of R-APS info. See Figure 10-3 of G.8032.
• **Dnf**	DNF (Do Not Flush) bit of R-APS info. See Figure 10-3 of G.8032."
• **Bpr**	BPR (Blocked Port Reference) of R-APS info. See Figure 10-3 of G.8032.
• **Node Id**	Node ID of this request.
• **SMAC**	The Source MAC address used in the request/state.

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically.

Refresh: Click to refresh the page immediately.

4.6.4 APS

4.6.4.1 APS Configuration

The APS module implements the protocol and linear protection switching mechanisms for point-to-point VLAN-based ETH SNC in Ethernet transport networks. Automatic Protection Switching is defined by the ITU G.8031 standard.

This page allows the user to create and configure an APS Instance.

APS Configuration

Refresh

APS #	Working			Protecting			Mode	Level	VLAN	PCP	SMAC	Rev	TxAps	WTR	HoldOff	Enable	Oper	Warning
	Port	SF Trigger	SF MEP	Port	SF Trigger	SF MEP												

Figure 4-6-5: APS Configuration Screen Page Screenshot

The displayed settings are:

APS Protocol:

Object	Description
• **APS #**	The ID of the APS. Maximum number of creatable APS instances is 10 . Click on link to get to APS instance page, you can reset counters and issue commands.
• **Port**	The Port this flow is attached to.
• **SF Trigger**	Selects whether Signal Fail (SF) comes from the link state of a given Port, or from a Down-MEP.
• **SF MEP**	The Domain::Service::MEPID refers to a MEP instance which shall represent the Working flow. Only used when SF Trigger is MEP. The selected MEP instance does not need to exist when this APS is configured.
• **Mode**	1:1 This will create a 1:1 APS. In the linear 1:1 protection switching architecture, the protection transport entity is dedicated to the working transport entity. However, the normal traffic is transported either on the working transport entity or on the protection transport entity using a selector bridge at the source of the protected domain. The selector at the sink of the protected domain selects the entity which carries the normal traffic. 1+1 Uni This will create a 1+1 Unidirectional APS. 1+1 Bi This will create a 1+1 Bidirectional APS. In the linear 1+1 protection switching architecture, a protection transport entity is dedicated to each working transport entity. The normal traffic is copied and fed to both working and protection transport entities with a permanent bridge at the source of the protected domain. The traffic on working and protection transport entities is transmitted simultaneously to the sink of the protected domain, where a selection between the working and protection transport entities is made based on some predetermined criteria, such as server defect indication.

• **Level**	MD/MEG Level (0-7).
• **VLAN**	The VLAN ID used in the L-APS PDUs. 0 means untagged.
• **PCP**	PCP (priority) (default 7). The PCP value used in the VLAN tag unless the L-APS PDU is untagged. Must be a value in range 0 - 7.
• **SMAC**	Source MAC address used in L-APS PDUs. Must be a unicast address. If all-zeros, the switch port's MAC address will be used.
• **Rev**	When checked, the port recovery mode is revertive, that is, traffic switches back to the working port after the condition(s) causing a switch has cleared. In the case of clearing a command (e.g. forced switch), this happens immediately. In the case of clearing of a defect, this generally happens after the expiry of the WTR (Wait-To-Restore) timer. When unchecked, the port recovery mode is non-revertive and traffic is allowed to remain on the protect port after a switch reason has cleared.
• **TxAps**	Choose whether this end transmits APS PDUs. Only used for 1+1, unidirectional.
• **WTR**	When Rev is checked, WTR (Wait-To-Restore) tells how many seconds to wait before restoring to the working port after a fault condition has cleared. Valid range 1 - 720
• **HoldOff**	When a new (or more severe) defect occurs, the hold-off timer will be started and the event will be reported after the timer expires. HoldOff time is measured in milliseconds, and valid values are in the range 0 - 10000. Default is 0, which means immediate reporting of the defect.
• **Enable**	The administrative state of this APS instance. Check to make it function normally and uncheck to make it cease functioning.
• **Oper**	This field can not be configured, but shows the operational state. You can click on the link in the APS # field to get more details on the status. APS instance is functional. APS instance is not functional.
• **Warning**	If the operational state is Active, the APS instance is indeed active, but it may be that it doesn't run as the administrator thinks, because of configuration errors, which are reflected in the warnings below. The Warning information is indicated by : no warning, : warning. Use the tooltip to get the detailed warning information.
• **Configuration Buttons**	You can modify each APS in the table using the following buttons: : Edits the APS row. : Deletes the APS. : Adds new APS.

Buttons

Refresh: Click to refresh the page immediately.

4.6.4.2 APS Status

This shows the current status of the APS instances.

APS Status

Auto-refresh ☐ Refresh

APS #	State			Defect state		TxAps			RxAps			Dfop				SMAC	TxCnt	RxCnt	
	Operational	Warning	Protection	Working	Protecting	Request	ReSignal	BrSignal	Request	ReSignal	BrSignal	CM	PM	NR	TO			Valid	Invalid
No entry exists																			

Figure 4-6-6: APS Status Screen Page Screenshot

The displayed settings are:

Object	Description
• **APS #**	The ID of the APS. Click on link to get to APS instance page, you can reset counters and issue commands.
• **State, Operational**	The operational state of the APS instance. There are many ways to not have the instance active. Each of them has its own value. Only when the state is Active, will the APS instance be active and up and running. If the Operational state is not "Active", the remaining fields are invalid. The possible values of this field are shown below: Administratively disabled: Instance is inactive, because it is administratively disabled. Active: The instance is active and up and running. Internal Error: Instance is inactive, because an internal error has occurred. Working MEP not Found:Instance is inactive, because the Working MEP is not found. Protecting MEP not Found: Instance is inactive, because the Protecting MEP is not found. Working MEP is not administrative active: Instance is inactive, because the Working MEP is not admin enabled. Protecting MEP is not administrative active: Instance is inactive, because the Protecting MEP is not admin enabled. Working MEP is not a Down MEP: Instance is inactive, because the Working MEP is not a Down-MEP. Protecting MEP is not a Down MEP: Instance is inactive, because the Protecting MEP is not a Down-MEP. Working and Protecting MEP use the same interface: Instance is inactive, because both Working and Protecting MEPs use the same I/F. Another instance use the same Working port: Instance is inactive, because another instance uses the same Working port.
• **State, Warning**	If the operational state is Active, the APS instance is indeed active, but it may be that it doesn't run as the administrator thinks, because of configuration errors,

	which are reflected in the warnings below. The Warning information is indicated by : no warning, : warning. Use the tooltip to get the detailed warning information.
• **State, Protection**	The possible protection group states. The letters refers to the state as described in G.8031 Annex No request Working: A. No request Protecting: B. Lockout: C. Forced Switch: D. Signal fail Working: E. Signal fail Protecting: F. Manual switch to Protecting: G. Manual switch to Working: H. Wait to restore: I. Do not revert: J. Exercise Working: K. Exercise Protecting: L. Reverse request Working: M. Reverse request Protecting: N. Signal degrade Working: P. Signal degrade Protecting: Q.
• **Defect state, Working, Protection**	The possible values of this field are shown below: ok: The port defect state is OK sd: The port defect state is Signal Degrade sf: The port defect state is Signal Fail
• **TxAps, RxAps - Request**	The possible transmitted or received APS request according to G.8031, Table 11-1. nr: No Request. dnr: Do Not Revert. rr: Reverse Request. exer: Exercise. wtr: Wait-To-Restore. ms: Manual Switch. sd: Signal Degrade. sfW: Signal Fail for Working. fs: Forced Switch. sfP: Signal Fail for Protect. lo: Lockout.
• **TxAps, ReSignal**	Transmitted requested signal according to G.8031 figure 11-2

• **TxAps, BrSignal**	Transmitted bridged signal according to G.8031 figure 11-2
• **RxAps, ReSignal**	Received requested signal according to G.8031 figure 11-2
• **RxAps, BrSignal**	Received bridged signal according to G.8031 figure 11-2
• **Dfop**	Dfop is "Failure of Protocol defect" and the presence of a defect is indicated by : no defect, : defect. CM: Configuration Mismatch (received APS PDU on working interface within last 17.5 seconds). PM: Provisioning Mismatch (far and near ends are not using the same mode; bidir only) NR: No Response (far end hasn't agreed on 'Requested Signal' within 50 ms; bidir only) TO: Time Out (near end hasn't received a valid APS PDU within last 17.5 seconds; bidir only)
• **SMAC**	Source MAC address of last received APS PDU or all-zeros if no PDU has been received.
• **TxCnt**	Number of APS PDU frames transmitted.
• **RxCnt, Valid**	Number of valid APS PDU frames received on the protect port.
• **RxCnt, Invalid**	Number of invalid APS PDU frames received on the protect port.

Buttons

Refresh: Click to refresh the page immediately.

4.7 Maintenance

4.7.1 Web Firmware Upgrade

This page facilitates an update of the firmware controlling the switch. The Web Firmware Upgrade screen in Figure 4-7-1 appears.

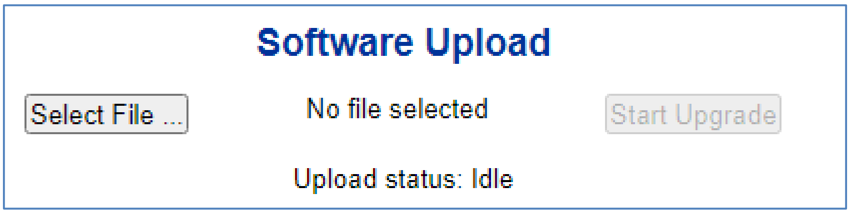


Figure 4-7-1: Web Firmware Upgrade Page Screenshot

To open **Firmware Upgrade** screen, perform the following:

1. Click **Maintenance** -> Web **Firmware Upgrade**.
2. The Firmware Upgrade screen is displayed as in Figure 4-7-2.
3. Click the "Choose File "button of the Main page; the system would pop up the file selection menu to choose firmware.
4. Select on the firmware and then click "Upload". The **Software Upload Progress** would show the file with upload status.
5. Once the software is loaded to the system successfully, the following screen appears. The system will load the new software after reboot.

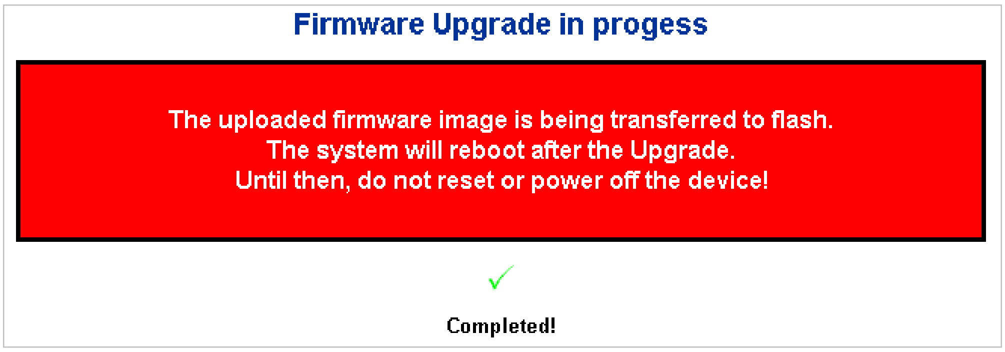


Figure 4-7-2: Software Successfully Loaded Notice Screen

Note

DO NOT Power OFF the Managed Switch until the update progress is complete.

Note

Do not quit the Firmware Upgrade page without pressing the "**OK**" button after the image is loaded. Or the system won't apply the new firmware. User has to repeat the firmware upgrade processes.

4.7.2 Save Startup Config

This function allows to save the current configuration, thereby ensuring that the current active configuration can be used at the next reboot as the screen in Figure 4-7-3 appears. After saving the configuration, the screen in Figure 4-7-4 will appear.

Figure 4-7-3: Configuration Save Page Screenshot

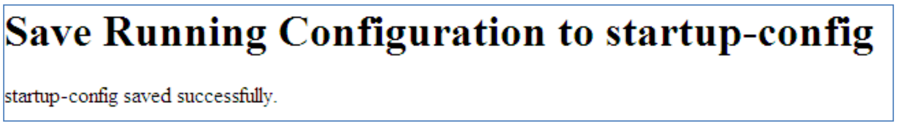


Figure 4-7-4: Finish Saving Page Screenshot

4.7.3 Configuration Download

The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch.

There are three system files:

- running-config: A virtual file that represents the currently active configuration on the switch. This file is volatile.
- startup-config: The startup configuration for the switch, read at boot time.
- default-config: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

It is also possible to store up to two other files and apply them to running-config, thereby switching configuration.

Configuration Download page allows the download the running-config, startup-config and default-config on the switch. Please refer to the Figure 4-7-5 shown below.

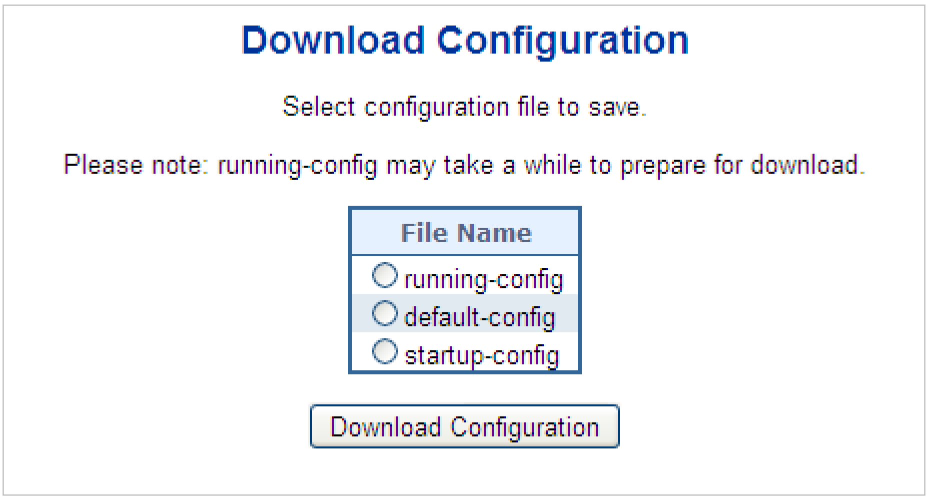


Figure 4-7-5: Configuration Download Page Screenshot

4.7.4 Configuration Upload

Configuration Upload page allows the upload the running-config and startup-config on the switch. Please refer to the Figure 4-7-6 shown below.

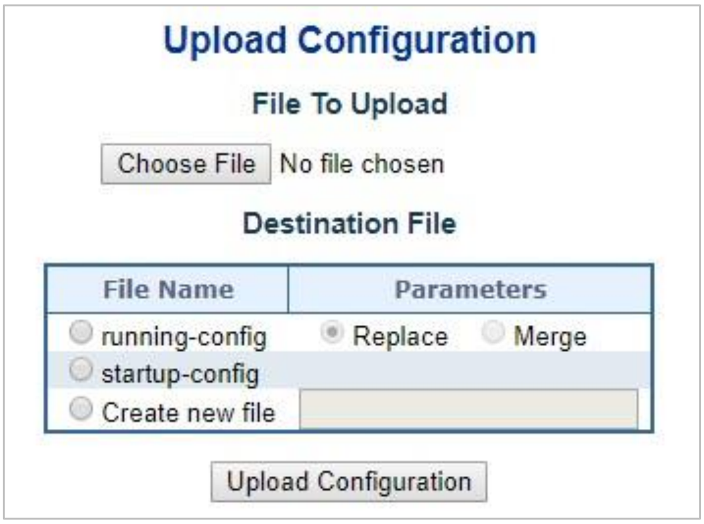


Figure 4-7-6: Configuration Upload Page Screenshot

If the destination is running-config, the file will be applied to the switch configuration. This can be done in two ways:

- 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*.

If the file system is full (i.e. contains the three system files mentioned above plus two other files), it is not possible to create new files, but an existing file must be overwritten or another deleted first.

4.7.5 Configure Activate

Thje Configure Activate page allows to activate the startup-config and default-config files present on the switch. Please refer to the Figure 4-7-7 shown below.

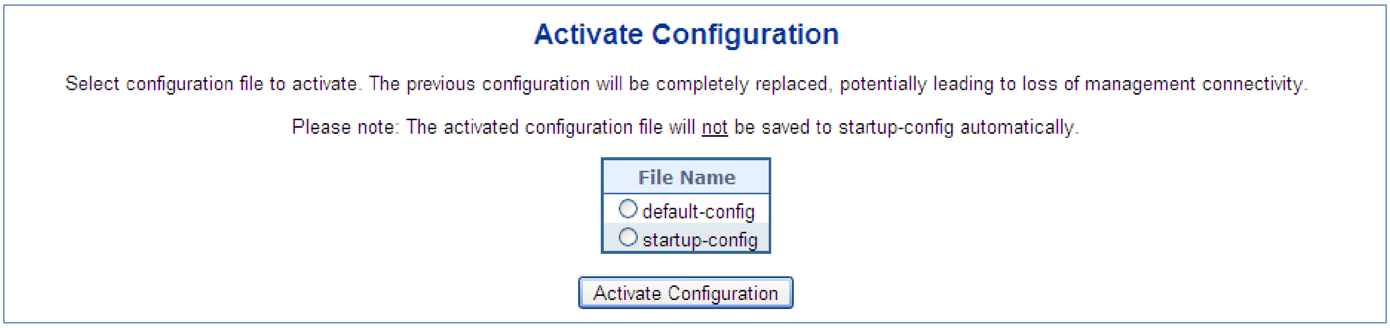


Figure 4-7-7: Configuration Activate Page Screenshot

It is possible to activate any of the configuration files present on the switch, except for *running-config* which represents the currently active configuration.

Select the file to activate and click 

. This will initiate the process of completely replacing the existing configuration with that of the selected file.

4.7.6 Configure Delete

The Configure Delete page allows to delete the startup-config and default-config files which are stored in FLASH. If this is done and the switch is rebooted without a prior Save operation, this effectively resets the switch to default configuration. Please refer to the Figure 4-7-8 shown below.

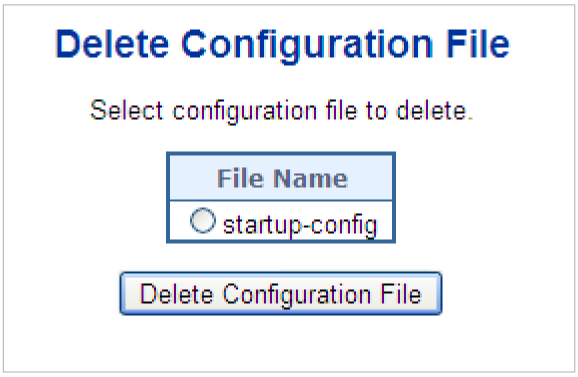


Figure 4-7-8: Configuration Delete Page Screenshot

4.7.7 Image Select

This page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image. The web page displays two tables with information about the active and alternate firmware images. The Image Select screen in Figure 4-7-9 appears.

> **Note:** In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the Activate Alternate Image button is also disabled.

> **Note:**
> 1. If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.
> 2. The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

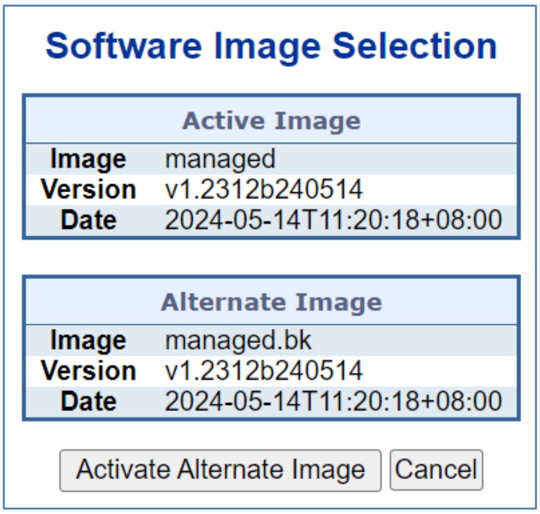


Figure 4-7-9: Software Image Selection Page Screenshot

The page includes the following fields:

Object	Description
• **Image**	The flash index name of the firmware image. The name of primary (preferred) image is image, the alternate image is named image.bk.
• **Version**	The version of the firmware image.
• **Date**	The date when the firmware was produced.

Buttons

: Click to use the alternate image. This button may be disabled depending on system state.

4.7.8 Factory Default

You can reset the configuration of the Managed Switch on this page. Only the IP configuration is retained. The new configuration is available immediately, which means that no restart is necessary. The Factory Default screen in Figure 4-7-10 appears.

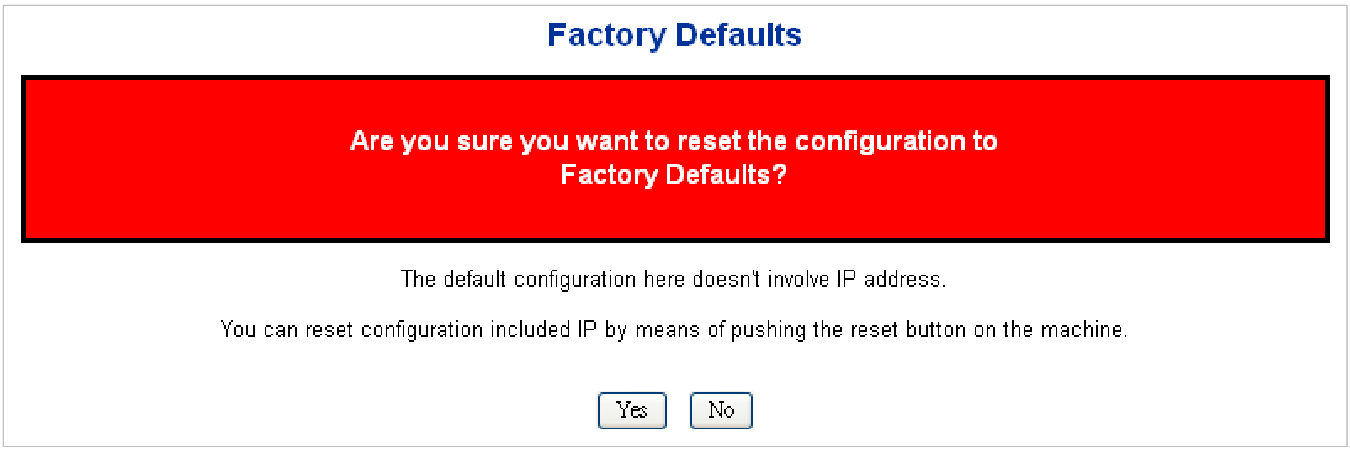


Figure 4-7-10: Factory Default Page Screenshot

Buttons

Yes: Click to reset the configuration to Factory Defaults.

No: Click to return to the Port State page without resetting the configuration.

Note: To reset the Managed Switch to the Factory default setting, you can also press the hardware reset button at the front panel about 10 seconds. After the device is rebooted, you can login the management Web interface within the same subnet of 192.168.0.xx.

4.7.9 System Reboot

The **Reboot** page enables the device to be rebooted from a remote location. Once the Reboot button is pressed, user has to re-login the Web interface about 60 seconds later; the System Reboot screen in Figure 4-7-11 appears.

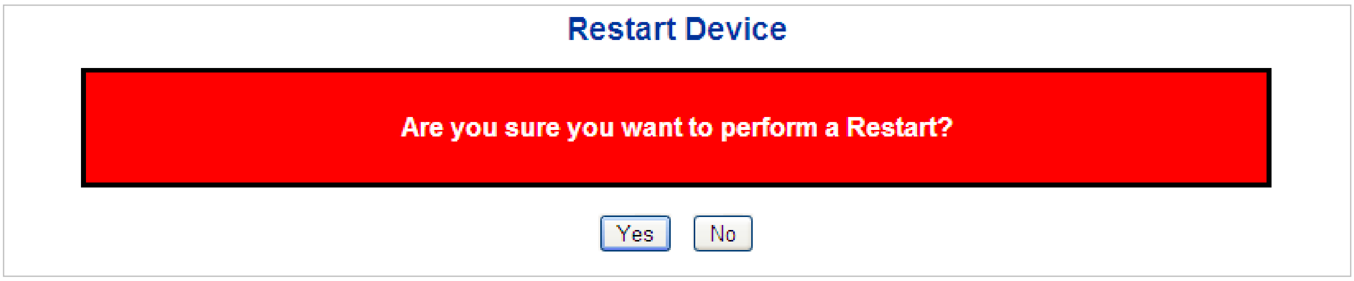
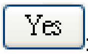
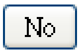


Figure 4-7-11: System Reboot Page Screenshot

Buttons



: Click to reboot the system.



: Click to return to the Port State page without rebooting the system.

You can also check the **SYS LED** on the front panel to identify whether the System is loaded completely or not. If the SYS LED is blinking, then it is in the firmware load stage; if the SYS LED light is on, you can use the Web browser to login the Managed Switch.

4.9.10 Ping

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.

After you press "**Start**", 5 ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs. The ICMP Ping screen in Figure 4-7-12 appears.

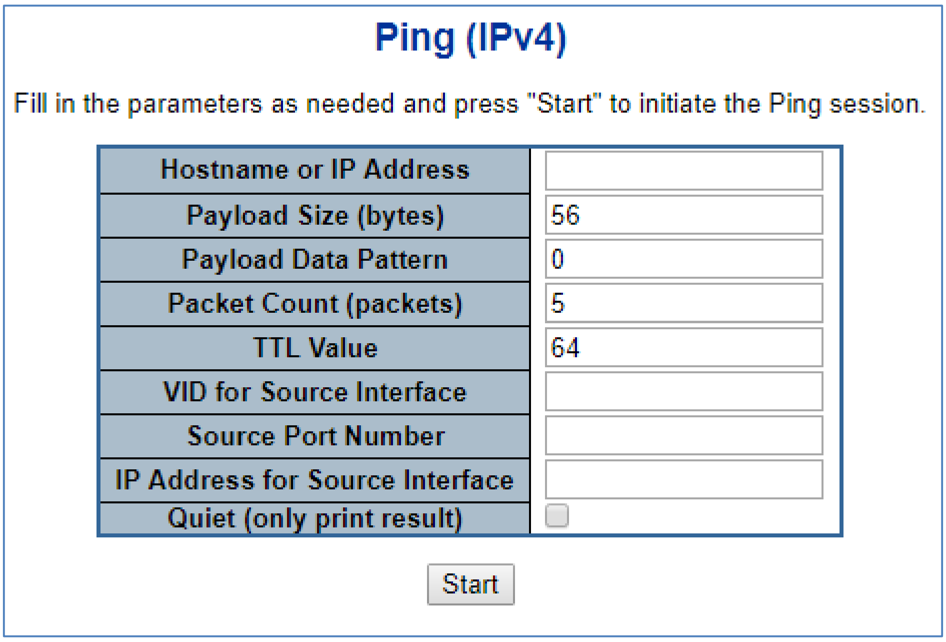


Figure 4-7-12: ICMP Ping Page Screenshot

The page includes the following fields:

Object	Description
• **IP Address**	The destination IP Address.
• **Ping Length**	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

Note

Be sure the target IP Address is within the same network subnet of the Managed Switch, or you had setup the correct gateway IP address.

Buttons

Start: Click to transmit ICMP packets.

New Ping: Click to re-start diagnostics with PING.

4.7.11 IPv6 Ping

This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

After you press "**Start**", 5 ICMPv6 packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs. The ICMPv6 Ping screen in Figure 4-7-13 appears.

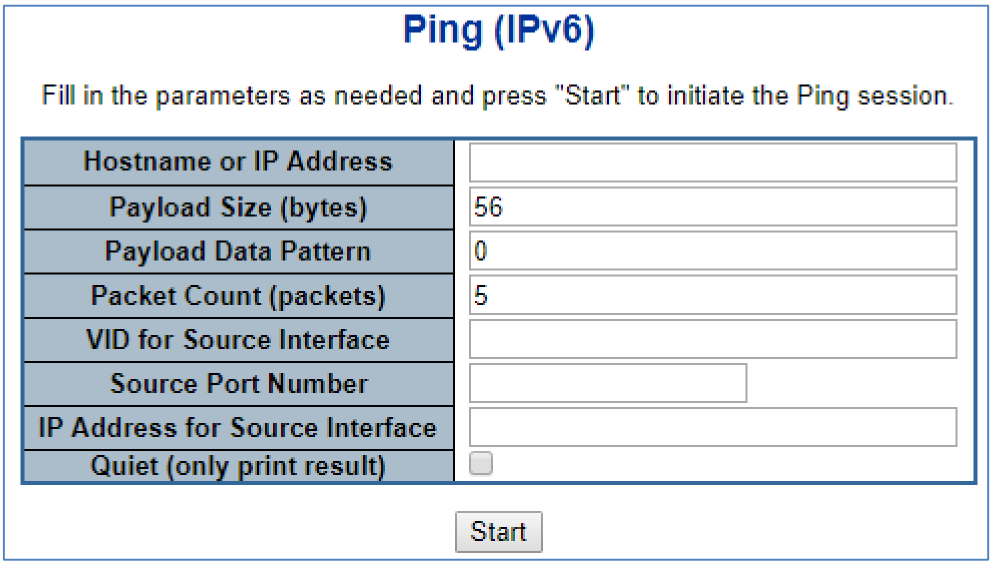


Figure 4-7-13: ICMPv6 Ping Page Screenshot

The page includes the following fields:

Object	Description
• **IP Address**	The destination IP Address.
• **Ping Length**	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

Buttons

: Click to transmit ICMP packets.

: Click to re-start diagnostics with PING.

4.7.12 Remote IP Ping

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues on special port.

After you press “**Test**”, 5 ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs. The ICMP Ping screen in Figure 4-7-14 appears.

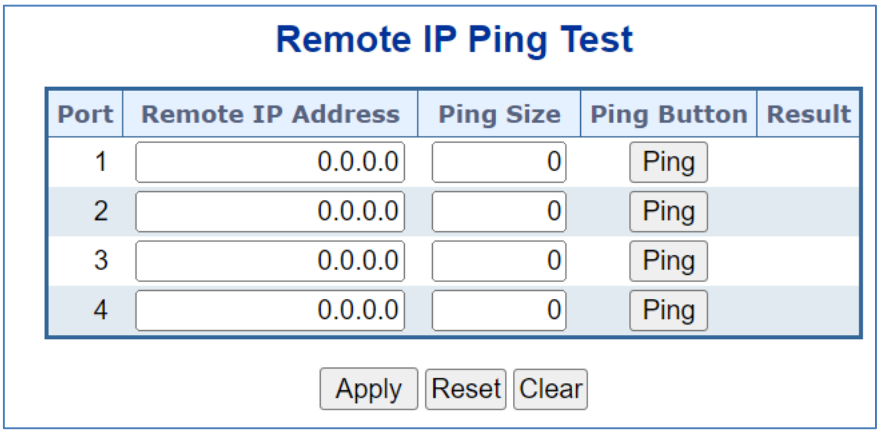


Figure 4-7-14: Remote IP Ping Test Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The logical port for the settings.
• **Remote IP Address**	The destination IP Address.
• **Ping Size**	The payload size of the ICMP packet. Values range from 8 bytes to 1400 bytes.
• **Result**	Display the ping result.

Buttons

: Click to apply changes

: Click to undo any changes made locally and revert to previously saved values.

: Clears the IP Address and the result of ping value.

4.7.13 Traceroute (IPv4)

This page allows you to perform a **traceroute** test over IPv4 towards a remote host. **Traceroute** is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv4 network. The Traceroute(IPv4) screen in Figure 4-7-15 appears.

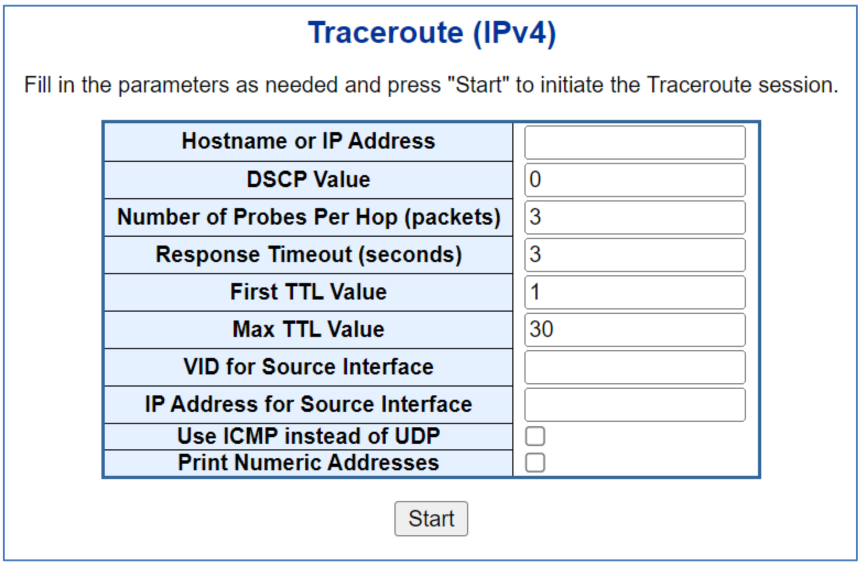


Figure 4-7-15: Remote IP Ping Test Page Screenshot

The page includes the following fields:

Object	Description
• **Hostname or IP Address**	The destination IP Address.
• **DSCP Value**	This value is used for the DSCP value in the IPv4 header. The default value is 0. The valid range is 0-63.
• **Number of Probes Per Hop**	Determines the number of probes (packets) sent for each hop. The default value is 3. The valid range is 1-60.
• **Response Timeout**	Determines the number of seconds to wait for a reply to a sent request. The default number is 3. The valid range is 1-86400.
• **First TTL Value**	Determines the value of the Time-To-Live (TTL) field in the IPv4 header in the first packet sent. The default number is 1. The valid range is 1-30.
• **Max TTL Value**	Determines the maximum value of the Time-To-Live (TTL) field in the IPv4 header. If this value is reached before the specified remote host is reached the test stops. The default number is 30. The valid range is 1-255.
• **VID for Source Interface**	This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.

• **Address for Source Interface**	This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.
• **Use ICMP instead of UDP**	By default the **traceroute** command will use UDP datagrams. Selecting this option forces it to use ICMP ECHO packets instead.
• **Print Numeric Addresses**	By default the **traceroute** command will print out hop information using a reverse DNS lookup for the acquired host ip addresses. This may slow down the display if the DNS information is not available. Selecting this option will prevent the reverse DNS lookup and force the **traceroute** command to print numeric IP addresses instead.

Buttons

Start : Click "Start" to initiate the Traceroute session.

4.7.14 Traceroute (IPv6)

This page allows you to perform a **traceroute** test over IPv6 towards a remote host. **Traceroute** is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv6 network. The Traceroute(IPv6) screen in Figure 4-7-16 appears.

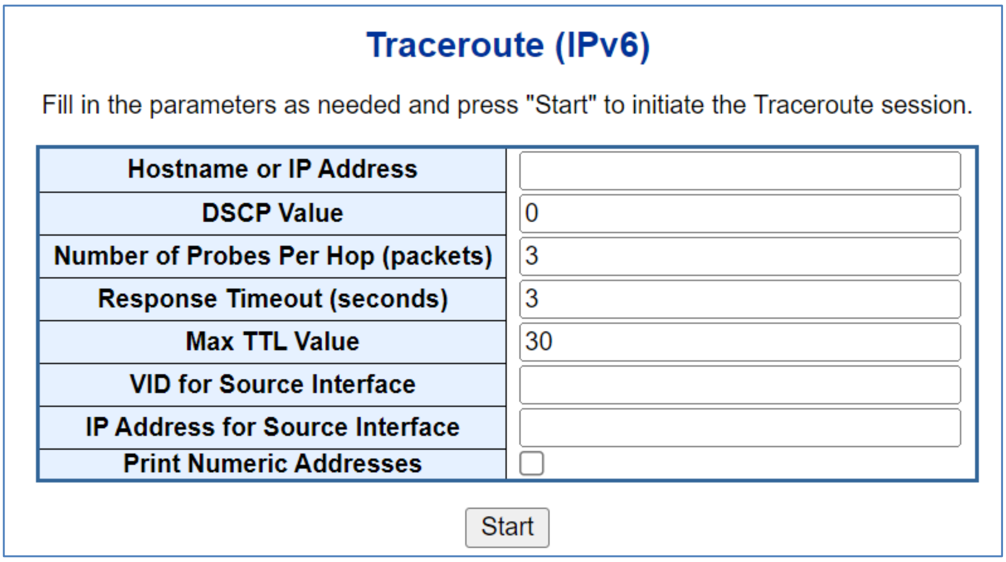


Figure 4-7-16: Remote IP Ping Test Page Screenshot

The page includes the following fields:

Object	Description
• **Hostname or IP Address**	The destination IP Address.
• **DSCP Value**	This value is used for the DSCP value in the IPv6 header. The default value is 0. The valid range is 0-63.
• **Number of Probes Per Hop**	Determines the number of probes (packets) sent for each hop. The default value is 3. The valid range is 1-60.
• **Response Timeout**	Determines the number of seconds to wait for a reply to a sent request. The default number is 3. The valid range is 1-86400.
• **Max TTL Value**	Determines the maximum value of the Time-To-Live (TTL) field in the IPv4 header. If this value is reached before the specified remote host is reached the test stops. The default number is 30. The valid range is 1-255.
• **VID for Source Interface**	This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.

• **Address for Source Interface**	This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.
• **Print Numeric Addresses**	By default the **traceroute** command will print out hop information using a reverse DNS lookup for the acquired host ip addresses. This may slow down the display if the DNS information is not available. Selecting this option will prevent the reverse DNS lookup and force the **traceroute** command to print numeric IP addresses instead.

Buttons

Start: Click "Start" to initiate the Traceroute session.

5. SWITCH OPERATION

5.1 Address Table

The **Industrial Managed TSN Device** is implemented with an address table. This address table is composed of many entries. Each entry is used to store the address information of some nodes in the network, including MAC address, port no, etc. This information comes from the learning process of **Industrial Managed TSN Device**.

5.2 Learning

When one packet comes in from any port, the **Industrial Managed TSN Device** will record the source address, port no., and the other related information in address table. This information will be used to decide either forwarding or filtering for future packets.

5.3 Forwarding & Filtering

When one packet comes from some port of the **Industrial Managed TSN Device**, it will also check the destination address besides the source address learning. The **Industrial Managed TSN Device** will look up the address-table for the destination address. If not found, this packet will be forwarded to all the other ports except the port, which this packet comes in. And these ports will transmit this packet to the network it connected. If found, and the destination address is located at a different port from this packet comes in, the **Industrial Managed TSN Device** will forward this packet to the port where this destination address is located according to the information from address table. But, if the destination address is located at the same port with this packet comes in, then this packet will be filtered, thereby increasing the network throughput and availability.

5.4 Store-and-Forward

Store-and-Forward is one type of packet-forwarding techniques. A Store-and-Forward **Industrial Managed TSN Device** stores the incoming frame in an internal buffer and do the complete error checking before transmission. Therefore, no error packets occur; it is the best choice when a network needs efficiency and stability.

The **Industrial Managed TSN Device** scans the destination address from the packet-header, searches the routing table provided for the incoming port and forwards the packet, only if required. The fast forwarding makes the switch attractive for connecting servers directly to the network, thereby increasing throughput and availability. However, the switch is most commonly used to segment existence hubs, which nearly always improves the overall performance. An Ethernet switching can be easily configured in any Ethernet network environment to significantly boost bandwidth using the conventional cabling and adapters.

Due to the learning function of the **Industrial Managed TSN Device**, the source address and corresponding port number of each incoming and outgoing packet are stored in a routing table. This information is subsequently used to filter packets whose destination address is in the same segment as the source address. This confines network traffic to its respective domain and reduce the overall load on the network.

The **Industrial Managed TSN Device** performs **"Store and Fforward"**; therefore, no error packets occur. More reliably, it reduces the re-transmission rate. No packet loss will occur.

5.5 Auto-Negotiation

The STP ports on the Switch have built-in **"Auto-negotiation"**. This technology automatically sets the best possible bandwidth when a connection is established with another network device (usually at Power On or Reset). This is done by detecting the modes and speeds both connected devices are capable of. Both 10BASE-T and 100BASE-TX devices can connect with the port in either half- or full-duplex mode. 1000BASE-T can be only connected in full-duplex mode.

6. TROUBLESHOOTING

This chapter contains information to help you solve issues. If the **Industrial Managed TSN Device** is not functioning properly, make sure the **Industrial Managed TSN Device** was set up according to instructions in this manual.

■ **The Link LED is not lit.**

Solution: Check the cable connection and remove duplex mode of the **Industrial Managed TSN Device**.

■ **Some stations cannot talk to other stations located on the other port.**

Solution: Please check the VLAN settings, trunk settings, or port enabled/disabled status.

■ **Performance is bad.**

Solution: Check the full duplex status of the **Industrial Managed TSN Device**. If the **Industrial Managed TSN Device** is set to full duplex and the partner is set to half duplex, then the performance will be poor. Please also check the in/out rate of the port.

■ **Why the Switch doesn't connect to the network.**

Solution:

1. Check the LNK/ACT LED on the switch.
2. Try another port on the Switch.
3. Make sure the cable is installed properly.
4. Make sure the cable is the right type.
5. Turn off the power. After a while, turn on power again.

■ **1000BASE-T port link LED is lit, but the traffic is irregular.**

Solution: Check that the attached device is not set to dedicate full duplex. Some devices use a physical or software switch to change duplex modes. Auto-negotiation may not recognize this type of full-duplex setting.

■ **Switch does not power up.**

Solution:

1. DC wire or AC power cord is not inserted or faulty.
2. Check that the DC wire/AC power cord is inserted correctly.
3. Replace the DC wire/AC power cord if the cord is inserted correctly; check that the DC/AC power source is working by connecting a different device in place of the switch.
4. If that device works, refer to the next step.
5. If that device does not work, check the DC/AC power.

APPENDIX A: Networking Connection

A.1 Switch's Data RJ45 Pin Assignments - 1000Mbps, 1000BASE-T

PIN NO	MDI	MDI-X
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

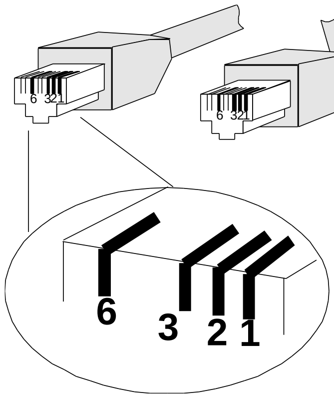
Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

A.2 10/100Mbps, 10/100BASE-TX

When connecting your Switch to another Fast Ethernet switch, a bridge or a hub, a straight or crossover cable is necessary. Each port of the Switch supports auto-MDI/MDI-X detection. That means you can directly connect the Switch to any Ethernet devices without making a crossover cable. The following table and diagram show the standard RJ45 receptacle/ connector and their pin assignments:

RJ45 Connector pin assignment		
PIN NO	MDI Media Dependent Interface	MDI-X Media Dependent Interface-Cross
1	Tx + (transmit)	Rx + (receive)
2	Tx - (transmit)	Rx - (receive)
3	Rx + (receive)	Tx + (transmit)
4, 5	Not used	
6	Rx - (receive)	Tx - (transmit)
7, 8	Not used	

The standard cable, RJ45 pin assignment



The standard RJ45 receptacle/connector

There are 8 wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and color of straight-through cable and crossover cable connection:

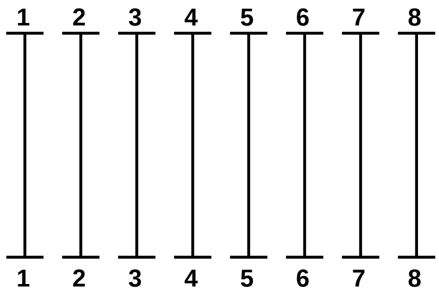
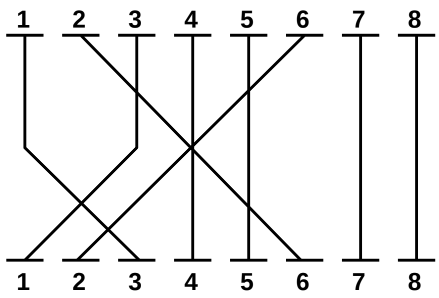
Straight Cable		**SIDE 1**	**SIDE 2**
	**SIDE 1** **SIDE 2**	**1 = White / Orange** **2 = Orange** **3 = White / Green** **4 = Blue** **5 = White / Blue** **6 = Green** **7 = White / Brown** **8 = Brown**	**1 = White / Orange** **2 = Orange** **3 = White / Green** **4 = Blue** **5 = White / Blue** **6 = Green** **7 = White / Brown** **8 = Brown**
Crossover Cable		**SIDE 1**	**SIDE 2**
	**SIDE 1** **SIDE 2**	**1 = White / Orange** **2 = Orange** **3 = White / Green** **4 = Blue** **5 = White / Blue** **6 = Green** **7 = White / Brown** **8 = Brown**	**1 = White / Green** **2 = Green** **3 = White / Orange** **4 = Blue** **5 = White / Blue** **6 = Orange** **7 = White / Brown** **8 = Brown**

Figure A-1: Straight-through and Crossover Cable

Please make sure your connected cables are with the same pin assignment and color as the above picture before deploying the cables into your network.

APPENDIX B : GLOSSARY

A

ACE

ACE is an acronym for **A**ccess **C**ontrol **E**ntry. It describes access permission associated with a particular ACE ID.

There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

ACL

ACL is an acronym for **A**ccess **C**ontrol **L**ist. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

There are 3 web pages associated with the manual ACL configuration:

ACL|Access Control List: The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that policy can be associated with a group of ports under the "Ports" web page. There are number of parameters that can be configured with an ACE. Read the web page help text to get further information for each of them. The maximum number of ACEs is 64.

ACL|Ports: The ACL Port configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List". You can you also set up specific traffic properties (Action / Rate Limiter / Port copy, etc) for each ingress port. They will though only apply if the frame gets past the ACE matching without getting matched. In that case a counter associated with that port is incremented. See the web page help text for each specific port property.

ACL|Rate Limiters: On this page, you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1 to 1024K packets per second. Under "Ports" and "Access Control List", you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

AES

AES is an acronym for **A**dvanced **E**ncryption **S**tandard. The encryption key protocol is applied in 802.1x standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

AMS

AMS is an acronym for **A**uto **M**edia **S**elect. AMS is used for dual media ports (ports supporting both copper (cu) and fiber (SFP) cables. AMS automatically determines if an SFP or a CU cable is inserted and switches to the corresponding media. If both SFP and cu cables are inserted, the port will select the prefered media.

APS

APS is an acronym for **A**utomatic **P**rotection **S**witching. This protocol is used to secure switching that is done bidirectional in both ends of a protection group, as defined in G.8031.

Aggregation

Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.

(Also *Port Aggregation, Link Aggregation*).

ARP

ARP is an acronym for **A**ddress **R**esolution **P**rotocol. It is a protocol that used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP Inspection

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

Auto-Negotiation

Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

C

CC

CC is an acronym for **C**ontinuity **C**heck. It is a MEP functionality that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.

CCM

CCM is an acronym for **C**ontinuity **C**heck **M**essage. It is a OAM frame transmitted from a MEP to its peer MEP and used to implement CC functionality.

CDP

CDP is an acronym for **C**isco **D**iscovery **P**rotocol.

D

DEI

DEI is an acronym for **D**rop **E**ligible **I**ndicator. It is a 1-bit field in the VLAN tag.

DES

DES is an acronym for **D**ata **E**ncryption **S**tandard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.

DHCP

DHCP is an acronym for **D**ynamic **H**ost **C**onfiguration **P**rotocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID. The parameter of "port_no" is the fourth byte and it means the port number.
The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.

DHCP Snooping

DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DNS

DNS is an acronym for **D**omain **N**ame **S**ystem. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

DoS

DoS is an acronym for **D**enial of **S**ervice. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at network sites or network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.

Dotted Decimal Notation

Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets.
An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.

DSCP

DSCP is an acronym for **D**ifferentiated **S**ervices **C**ode **P**oint. It is a field in the header of IP packets for packet classification purposes.

E

EEE

EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

EPS

EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.

Ethernet Type

Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.

F

FTP

FTP is an acronym for **F**ile **T**ransfer **P**rotocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.

Fast Leave

IGMP snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously.

H

HTTP

HTTP is an acronym for **H**ypertext **T**ransfer **P**rotocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW).

HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested web page. The other main standard that controls how the World Wide Web works is HTML, which covers how web pages are formatted and displayed.

Any Web server machine contains, in addition to the web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS

HTTPS is an acronym for **H**ypertext **T**ransfer **P**rotocol over **S**ecure Socket Layer. It is used to indicate a secure HTTP connection.

HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.

HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I

ICMP

ICMP is an acronym for **I**nternet **C**ontrol **M**essage **P**rotocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP

IGMP is an acronym for **I**nternet **G**roup **M**anagement **P**rotocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier

A router sends IGMP Query messages onto a particular link. This router is called the Querier.

IMAP

IMAP is an acronym for **I**nternet **M**essage **A**ccess **P**rotocol. It is a protocol for email clients to retrieve email messages from a mail server.

IMAP is the protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server.

The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves your email messages on the server rather than downloading them to your computer. If you wish to remove your messages from the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.

IP

IP is an acronym for **I**nternet **P**rotocol. It is a protocol used for communicating data across a internet network.

IP is a "best effort" system, which means that no packet of information sent over it is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPMC

IPMC is an acronym for **IP** **M**ulti**C**ast.

IP Source Guard

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

L

LACP

LACP is an IEEE 802.3ad standard protocol. The **L**ink **A**ggregation **C**ontrol **P**rotocol allows bundling several physical ports together to form a single logical port.

LLDP

LLDP is an IEEE 802.1ab standard protocol.

The **L**ink **L**ayer **D**iscovery **P**rotocol(LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP-MED

LLDP-MED is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).

LOC

LOC is an acronym for **L**oss **O**f **C**onnectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as a switch criteria by EPS

M

MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

MEP

MEP is an acronym for **M**aintenance **E**ntity **E**ndpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).

MD5

MD5 is an acronym for **M**essage-**D**igest algorithm **5**. MD5 is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.

Mirroring

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MLD

MLD is an acronym for **M**ulticast **L**istener **D**iscovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

MVR

Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs. The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them (Wikipedia).

N

NAS

NAS is an acronym for Network Access Server. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

NetBIOS

NetBIOS is an acronym for **Net**work **B**asic **I**nput/**O**utput **S**ystem. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN).

The NetBIOS giving each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, provides the session and transport services described in the Open Systems Interconnection (OSI) model.

NFS

NFS is an acronym for **N**etwork **F**ile **S**ystem. It allows hosts to mount partitions on a remote system and use them as though they are local file systems.

NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NTP

NTP is an acronym for **N**etwork **T**ime **P**rotocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.

O

OAM

OAM is an acronym for **O**peration **A**dministration and **M**aintenance. It is a protocol described in ITU-T Y.1731 used to implement carrier Ethernet functionality. MEP functionality like CC and RDI is based on this.

Optional TLVs.

An LLDP frame contains multiple TLVs. For some TLVs it is configurable if the switch includes the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLV is disabled the corresponding information is not included in the LLDP frame.

OUI

OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of an MAC address.

P

PCP

PCP is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.

PD

PD is an acronym for **P**owered **D**evice. In a PoE> system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

PHY

PHY is an abbreviation for Physical Interface Transceiver and is the device that implement the Ethernet physical layer (IEEE-802.3).

PING

Ping is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.

Ping uses Internet Control Message Protocol (ICMP) packets. The Ping Request is the packet from the origin computer, and the Ping Reply is the packet response from the target.

Policer

A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

POP3

POP3 is an acronym for **P**ost **O**ffice **P**rotocol version 3. It is a protocol for email clients to retrieve email messages from a mail server.

POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a "store-and-forward" service.

An alternative protocol is Internet Message Access Protocol (IMAP). IMAP provides the user with more capabilities for retaining e-mail on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server.

POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP). You send e-mail with SMTP, and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP. IMAP4 and POP3 are the two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both.

PPPoE

PPPoE is an acronym for Point-to-Point Protocol over Ethernet. It is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks (Wikipedia).

Private VLAN

In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.

PTP

PTP is an acronym for Precision Time Protocol, a network protocol for synchronizing the clocks of computer systems.

Q

QCE

QCE is an acronym for **Q**oS **C**ontrol **E**ntry. It describes QoS class associated with a particular QCE ID.

There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.

QCL

QCL is an acronym for **Q**oS **C**ontrol **L**ist. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects.

Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QL

QL In SyncE this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.

QoS

QoS is an acronym for **Q**uality **o**f **S**ervice. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

QoS class

Every incoming frame is classified to a QoS class, which is used throughout the device for providing queuing, scheduling and congestion control guarantees to the frame according to what was configured for that specific QoS class. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.

R

RARP

RARP is an acronym for **R**everse **A**ddress **R**esolution **P**rotocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

RADIUS

RADIUS is an acronym for **Re**mote **A**uthentication **D**ial In **U**ser **S**ervice. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

RDI

RDI is an acronym for **R**emote **D**efect **I**ndication. It is an OAM functionality that is used by a MEP to indicate defect detected to the remote peer MEP

Router Port

A router port is a port on the Ethernet switch that leads switch towards the Layer 3 multicast device.

RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of STP: the **R**apid **S**panning **T**ree **P**rotocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

S

SAMBA

Samba is a program running under UNIX-like operating systems that provides seamless integration between UNIX and Microsoft Windows machines. Samba acts as file and print servers for Microsoft Windows, IBM OS/2, and other SMB client machines. Samba uses the Server Message Block (SMB) protocol and Common Internet File System (CIFS), which is the underlying protocol used in Microsoft Windows networking.

Samba can be installed on a variety of operating system platforms, including Linux, most common Unix platforms, OpenVMS, and IBM OS/2.

Samba can also register itself with the master browser on the network so that it would appear in the listing of hosts in Microsoft Windows "Neighborhood Network".

SHA

SHA is an acronym for **S**ecure **H**ash **A**lgorithm. It designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

Shaper

A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

SMTP

SMTP is an acronym for **S**imple **M**ail **T**ransfer **P**rotocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

SNAP

The SubNetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier.

SNMP

SNMP is an acronym for **S**imple **N**etwork **M**anagement **P**rotocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP

SNTP is an acronym for **S**imple **N**etwork **T**ime **P**rotocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

SPROUT

Stack **P**rotocol using **ROU**ting **T**echnology. An advanced protocol for almost instantaneous discovery of topology changes within a stack as well as election of a master switch. SPROUT also calculates parameters for setting up each switch to perform shortest path forwarding within the stack.

SSID

Service **S**et **Id**entifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one (wikipedia).

SSH

SSH is an acronym for **S**ecure **SH**ell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality (Wikipedia).

SSM

SSM In SyncE this is an abbreviation for Synchronization Status Message and is containing a QL indication.

STP

Spanning **T**ree **P**rotocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

SyncE

SyncE Is an abbreviation for Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. Not to be confused with real time clock synchronized (IEEE 1588).

T

TACACS+

TACACS+ is an acronym for **T**erminal **A**ccess **C**ontroller **A**ccess **C**ontrol **S**ystem **P**lus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Tag Priority

Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.

TCP

TCP is an acronym for **T**ransmission **C**ontrol **P**rotocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

TELNET

TELNET is an acronym for **Tel**etype **Net**work. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.

TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.

TFTP

TFTP is an acronym for **T**rivial **F**ile **T**ransfer **P**rotocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provides directory service and security features.

Toss

Toss is an acronym for **T**ype **o**f **S**ervice. It is implemented as the IPv4 Toss priority control. It is fully decoded to determine the priority from the 6-bit Toss field in the IP header. The most significant 6 bits of the Toss field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0~63).

TLV

TLV is an acronym for **T**ype **L**ength **V**alue. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV.

TKIP

TKIP is an acronym for **T**emporal **K**ey **I**ntegrity **P**rotocol. It used in WPA to replace WEP with a new encryption algorithm. TKIP comprises the same encryption engine and RC4 algorithm defined for WEP. The key used for encryption in TKIP is 128 bits and changes the key used for each packet.

U

UDP

UDP is an acronym for **U**ser **D**atagram **P**rotocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

UPnP

UPnP is an acronym for **U**niversal **P**lug and **P**lay. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components

User Priority

User Priority is a 3-bit field storing the priority level for the 802.1Q frame.

V

VLAN

A method to restrict communication between switch ports. VLANs can be used for the following applications:

VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.

VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.

Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

VLAN ID

VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

W

WEP

WEP is an acronym for **W**ired **E**quivalent **P**rivacy. WEP is a deprecated algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages using radio, so are more susceptible to eavesdropping than wired networks. When introduced in 1999, WEP was intended to provide confidentiality comparable to that of a traditional wired network (Wikipedia).

Wi-Fi

Wi-Fi is an acronym for **Wi**reless **Fi**delity. It is meant to be used generically when referring of any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term is promulgated by the Wi-Fi Alliance.

WPA

WPA is an acronym for **W**i-Fi **P**rotected **A**ccess. It was created in response to several serious weaknesses researchers had found in the previous system , Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is specifically designed to also work with pre-WPA wireless network interface cards (through firmware upgrades), but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards (Wikipedia).

WPA-PSK

WPA-PSK is an acronym for **W**i-Fi **P**rotected **A**ccess - **P**re **S**hared **K**ey. WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)

WPA-Radius

WPA-Radius is an acronym for **W**i-Fi **P**rotected **A**ccess - Radius (802.1X authentication server). WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)

WPS

WPS is an acronym for **W**i-Fi **P**rotected **S**etup. It is a standard for easy and secure establishment of a wireless home network. The goal of the WPS protocol is to simplify the process of connecting any home device to the wireless network (Wikipedia).

WRED

WRED is an acronym for **W**eighted **R**andom **E**arly **D**etection. It is an active queue management mechanism that provides preferential treatment of higher priority frames when traffic builds up within a queue. A frame's DP level is used as input to WRED. A higher DP level assigned to a frame results in a higher probability that the frame is dropped during times of congestion.

WTR

WTR is an acronym for **W**ait **T**o **R**estore. This is the time a fail on a resource has to be 'not active' before restoration back to this (previously failing) resource is done.