SecurePNT EdgeGM 7000

with Multi-Orbit SecureTime altGNSS SM GEO/LEO Service

Users Guide

R000

SecurePNT EdgeGM 7000

Users Guide

22194201 R000

This page intentionally left blank.

This page intentionally left blank.

About this User Guide

This prefix explains how to use this User Guide.

Purpose and scope

This manual is intended to help you use the capabilities of the Secure PNT EdgeGM 7000.

This manual includes task-based instructions that describe how to configure, use, and troubleshoot the test capabilities available on your instrument assuming it is configured and optioned to support the capabilities.

Assumptions

This manual is intended for novice, intermediate, and experienced users who want to use their instrument effectively and efficiently. We are assuming that you have basic computer experience and are familiar with basic telecommunication concepts, terminology, and safety.

Related Information

This manual is application-oriented and contains information about using these instruments to test service carried on each of the listed networks. It includes an overview of testing features, instructions for using the instruments to generate and transmit traffic over a circuit, and detailed test result descriptions. This manual also provides contact information for VIAVI's Technical Assistance Center (TAC).

Safety and compliance information

The following sections describe the safety and compliance information for the Secure PNT EdgeGM 7000.

California Proposition 65

California Proposition 65, officially known as the Safe Drinking Water and Toxic Enforcement Act of 1986, was enacted in November 1986 with the aim of protecting individuals in the state of California and the state's drinking water and environment from excessive exposure to chemicals known to the state to cause cancer, birth defects or other reproductive harm.

For the VIAVI position statement on the use of Proposition 65 chemicals in VIAVI products, see the Hazardous Substance Control section of the VIAVI Policies & Standards web page.

Federal Communications Commission (FCC)

The equipment was 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 you will be required to correct the interference at your own expense.

The authority to operate this equipment is conditioned by the requirements that no modifications be made to the equipment unless the changes or modifications are expressly approved by VIAVI.

Product Environmental Compliance

VIAVI is committed to compliance with all applicable laws and regulations controlling the use of hazardous substances in its products, as well as the disposal of equipment (including batteries) and waste packaging. For details, see the VIAVI Policies & Standards web page or contact the VIAVI WEEE Program Management team at Global.WEEE@ViaviSolutions.com.

EU REACH

Article 33 of EU REACH regulation (EC) No 1907/2006 requires product suppliers to provide information when a substance included in the list of Substances of Very High Concern (SVHC) is present in an product above a certain threshold.

For information about the presence of REACH SVHC in VIAVI products, see the Hazardous Substance Control section of the VIAVI Policies & Standards web page.

Additional standards compliance

The equipment meets the following standards and requirements:

- Installation Category (Over Voltage Category) II under IEC 60664-1
- Pollution Degree 2 Category under IEC 62368-1 Safety Requirements for Electrical Equipment for Measurement, Control, and Laboratory Use

Technical assistance

If you require technical assistance, call 1-844-GO-VIAVI. For the latest TAC information, go to https://support.viavisolutions.com.

Table of Contents

This page intentionally left blank.

1 Introduction

The following topics are discussed in this chapter:

- SecurePNT EdgeGM 7000 Overview
- Physical Description
- Typical Applications

This page intentionally left blank.

1.1 SecurePNT EdgeGM 7000 Overview

The VIAVI **EdgeGM 7000** is a resilient 1/10/25G PTP Edge Grandmaster clock that integrates advanced resiliency from multi-orbit space and terrestrial sources and high-speed Grandmaster clock capabilities.

The EdgeGM 7000 solution is powered by innovative TrustedPNT™ technology, which authenticates, verifies, and qualifies multiple orbital and terrestrial timing sources, for smooth, seamless switching for a trusted timing reference.

1.1.1 Variants

The following table describes the **EdgeGM 7000** variants.

Part Number	Variant	Description
22187697	EGM-7000	EdgeGM Multi-Band Receiver with 8hr holdover
22187356	EGM-7000S	EGM 7000S Multi-band GNSS/STL Receiver • STL variant • Holdover capability of 8 hours to maintain 1.5µs accuracy
22187366	EGM-7000L	EGM-7000L Multi-Band GNSS / GEOL Receiver • GEOL variant • Holdover capability of 8 hours to maintain 1.5 µs accuracy

1.2 Physical Description

The following figure shows the EdgeGM 7000 front panel.

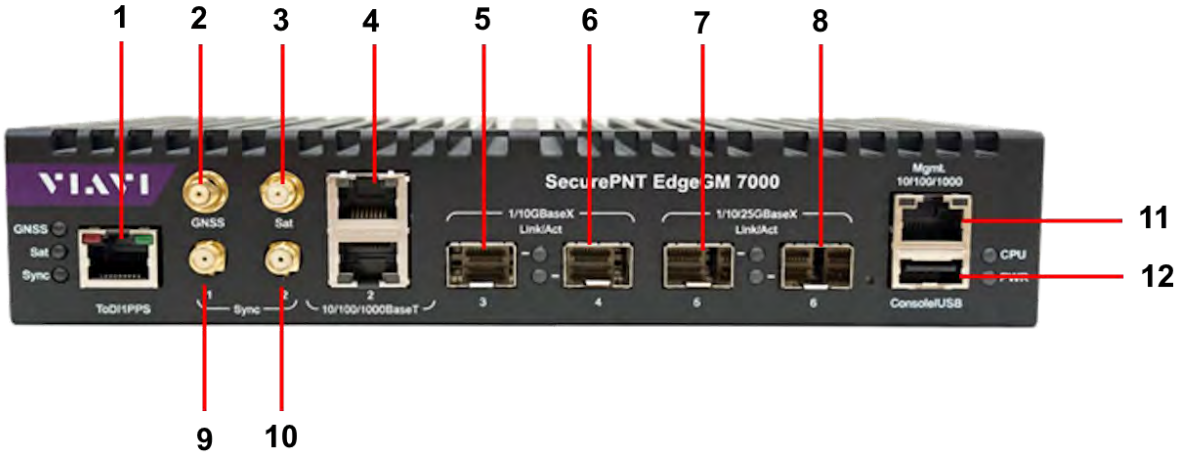


Figure 1-1: EdgeGM 7000 front panel

The following table describes the EdgeGM front panel.

Table 1-1: EdgeGM 7000 front and back panel description

#	Input	Description
1	ToD/1PPS	Time of Day (ToD) and 1 Pulse Per Second (1PPS) input.
2	GNSS	GNSS input L1/2/5 In (GPS/Galileo/Beidu/QZSS/NavIC)
3	altGNSS Sat In	LEO STL or GEO-L
4	Ethernet/PTP/SyncE/NTP	PTP, SyncE, or NTP In/Out (user settable) PTP unicast clients support: 256/1024 PTP profiles: Telecom (G.8275.1 L2 FOPS/G.8275.2 L3 unicast/POPS), Enterprise, Power, etc.
5	Ethernet/PTP/SyncE/NTP (1/10G)	
6	Ethernet/PTP/SyncE/NTP (1/10G)	
7	Ethernet/PTP/SyncE/NTP (10/25G)	
8	Ethernet/PTP/SyncE/NTP (10/25G)	
9	Sync1	1PPS or 10/1.544/2.028 MHz In/Out (user settable)
10	Sync2	
11	RJ45	10/100/1000 BaseT input for management
12	USB	Local console

1.3 Typical Applications

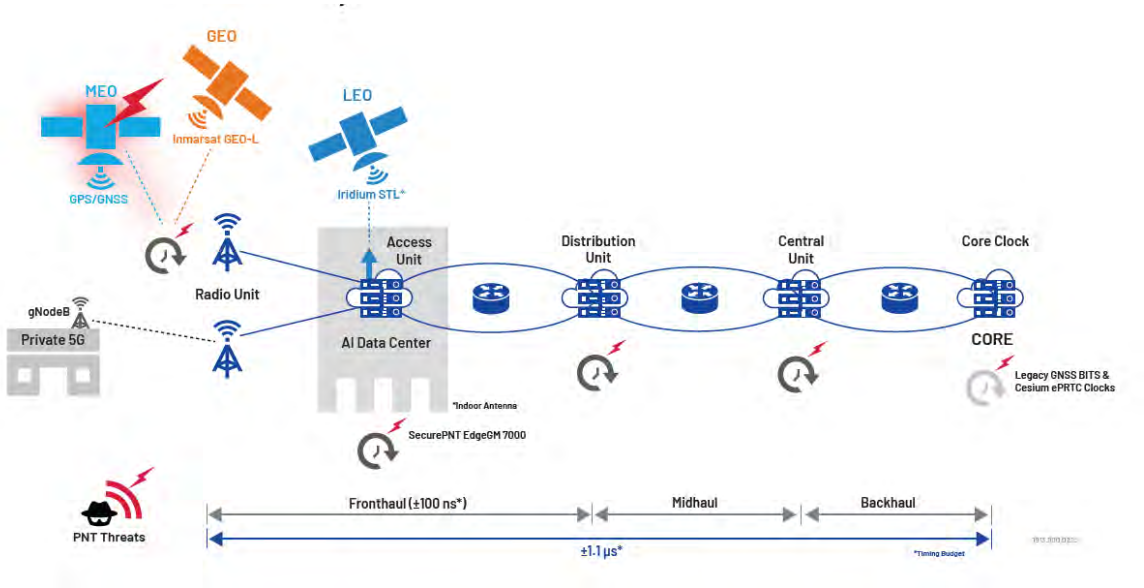
The following sections describe the typical applications of the EdgeGM 7000.

1.3.1 Synchronizing Critical 5G AI-RAN, AI Data Center and Private 5G Networks

Synchronizing critical 5G AI-RAN, AI data center, and private 5G networks presents significant challenges due to increasingly stringent timing accuracy requirements, vulnerability of GNSS signals, and the need to distribute precise time across disaggregated, high-speed network architectures. Fronthaul, midhaul, and backhaul segments must meet tight timing budgets to support advanced radio functions, AI-driven workloads, and emerging use cases, while traditional GNSS-dependent clocks are exposed to jamming, spoofing, and other PNT threats. The EdgeGM 7000 addresses these issues by providing a resilient, edge-based timing solution that combines high-accuracy PTP distribution with GNSS-independent backup from alternative LEO and GEO satellite sources. Deployed at key network points such as radio units, access units, and data centers, the EdgeGM 7000 maintains precise and continuous synchronization during GNSS disruptions, ensuring deterministic timing performance and reliable operation across the entire 5G and AI-enabled network infrastructure.

1.3.2 Secure Multi-Orbit Network Timing

Modern 5G/6G, private 5G, and AI data center networks depend on extremely accurate and resilient timing to support fronthaul, midhaul, and backhaul synchronization. In this architecture, the EdgeGM 7000 serves as the edge Grandmaster clock, ingesting time from multiple independent sources—including traditional multi-band GNSS and secure alternative GNSS services delivered via GEO and LEO satellites. By continuously authenticating and validating these sources, the EdgeGM 7000 ensures trusted timing even during GNSS jamming or spoofing events. The verified time reference is then distributed over high-speed Ethernet using PTP, SyncE, or NTP to central units, distributed units, radio units (gNodeBs), and AI data center infrastructure, meeting tight fronthaul (±100 ns) and backhaul timing budgets without reliance on a single vulnerable timing source.



1.3.3 5G Fronthaul & Backhaul Convergence

Evolved mobile networks require high levels of synchronization to operate. The required accuracy level increases as the networks further evolve, reaching the point the expected time error of nanoseconds is needed in the 5G Fronthaul. The EdgeGM 7000 ability to provide this level of synchronization, on top of its line rate Ethernet forwarding, makes it the ideal Fronthaul switch. Additionally, the EdgeGM 7000 can also provide backhaul connection to complete gNodeB units towards the 5G Core.

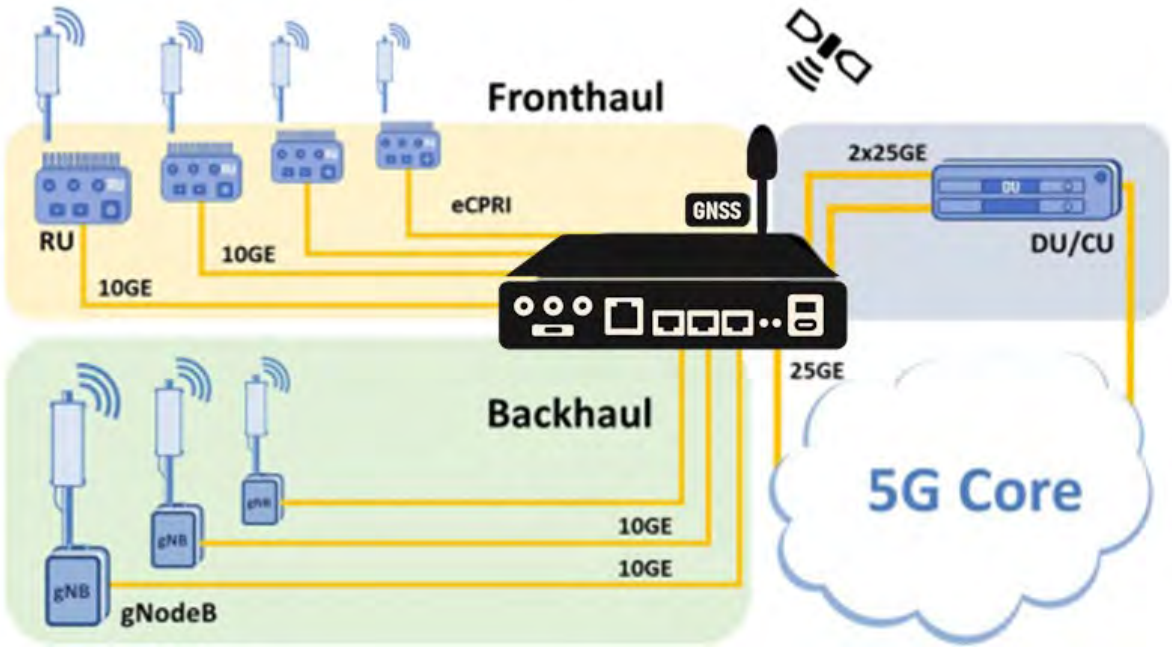
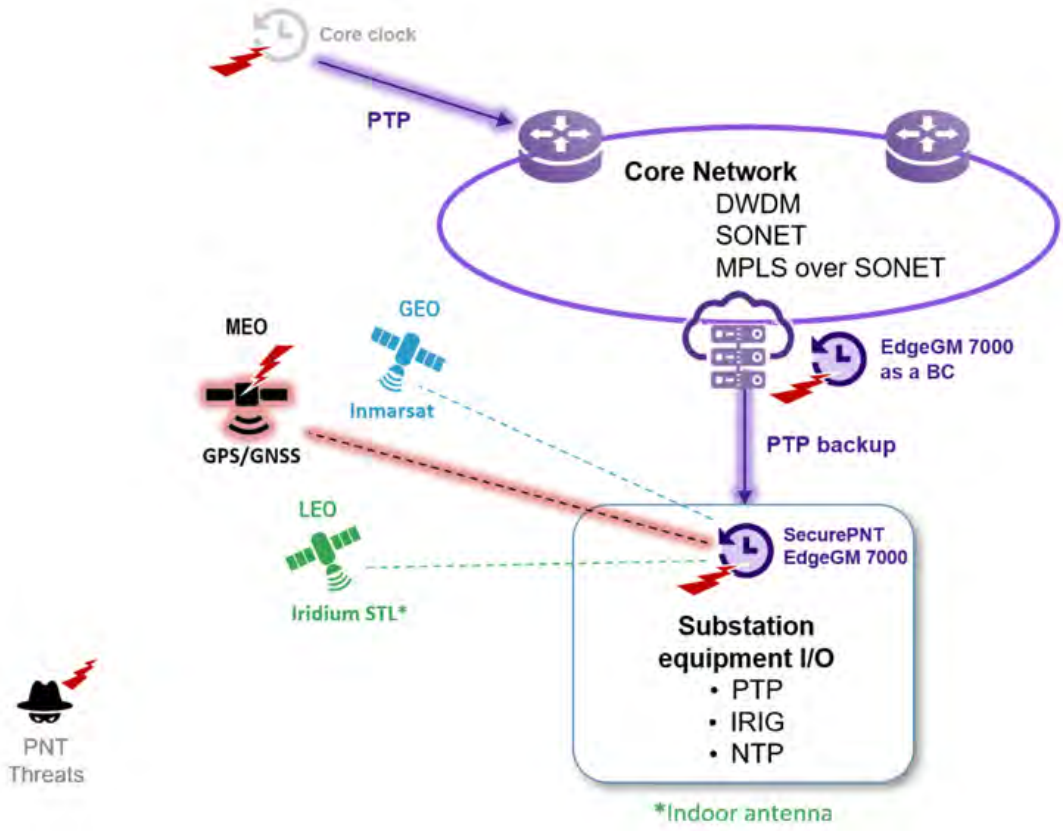


Figure 1-2: EdgeGM 7000 typical xHaul application

1.3.4 Synchronizing Critical Smart Grid Networks

Critical smart grid networks face two fundamental synchronization challenges that must be addressed to ensure reliable and secure operation. First, accurate timing can no longer rely solely on GPS/GNSS, as these signals are increasingly susceptible to jamming, spoofing, and meaconing; resilient operation therefore requires a defense-in-depth approach that incorporates GNSS-independent sources of opportunity, including GEO and LEO satellite signals, to maintain timing continuity during disruptions. Second, network architectures are evolving toward much higher data rates, driving the need to distribute Precision Time Protocol (PTP) over 25G and up to 100G interfaces, since legacy 1G and 10G PTP ports are becoming scarce in modern data centers and network offices. The EdgeGM 7000 addresses these problems by combining diverse timing sources with high-speed PTP distribution to maintain robust synchronization from the core network to substation equipment.



1.3.1 IIoT Campus deployment

Modern industrial campuses and factories are being designed to accommodate high level of automation and mobility in production, which dictates specific requirement for synchronization. In such environment where, man and machine coexist and work together side by side all actions must be coordinated and mutually aware. Synchronized packet networks and time sensitive networking (TSN) are key elements in building these enrolments.

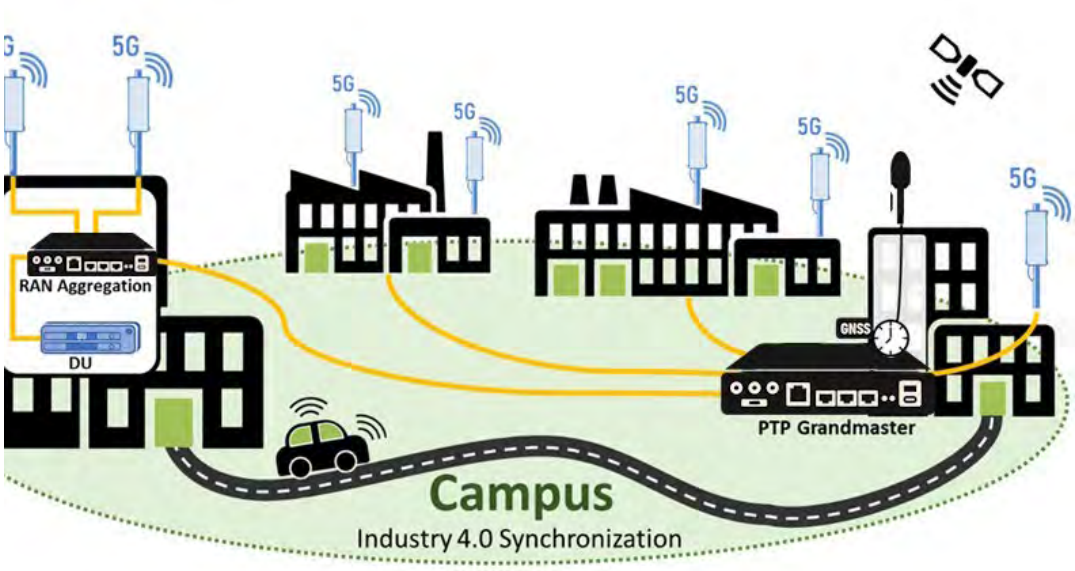


Figure 1-3: EdgeGM 7000 in IIoT campus deployment.

2 System Description

The following topics are discussed in this chapter:

- EdgeGM 7000 key features
- Block Diagram
- Management
- EdgeGM 7000 port features

This page intentionally left blank.

2.1 EdgeGM 7000 key features

- LTE/5G xHaul Transport and Timing RAN switch
- Integrated PTP Grandmaster
- Compatible with O-RAN architectures
- High capacity, low latency
- Extensive Sync and Timing with SyncE and PTP (PRTC/GM, BC, TC)
- Sub nanosecond timestamping, Class C/D performance
- Time Sensitive Networking support
- Based on 4th generation EdgeGM 7000 architecture
- Advanced QoS and service level traffic management
- Advanced OAM and management capabilities
- Multiple protection mechanisms for link, path, and ring service resilience
- Multisource receivers for GNSS backup: Multiband GNSS or LEO STL or GEO-L
- High-speed ≤25G PTP Grandmaster and NTP Time Server
- Flexible timing platform: SyncE, NTP, PTP (PRTC-A/B), GM, APTS, BC – Class C/D, Client Clock, TC, 1 PPS, ToD, 10 MHz, Gateway Clock
- High-performance sub-ns timestamping

2.2 Block Diagram

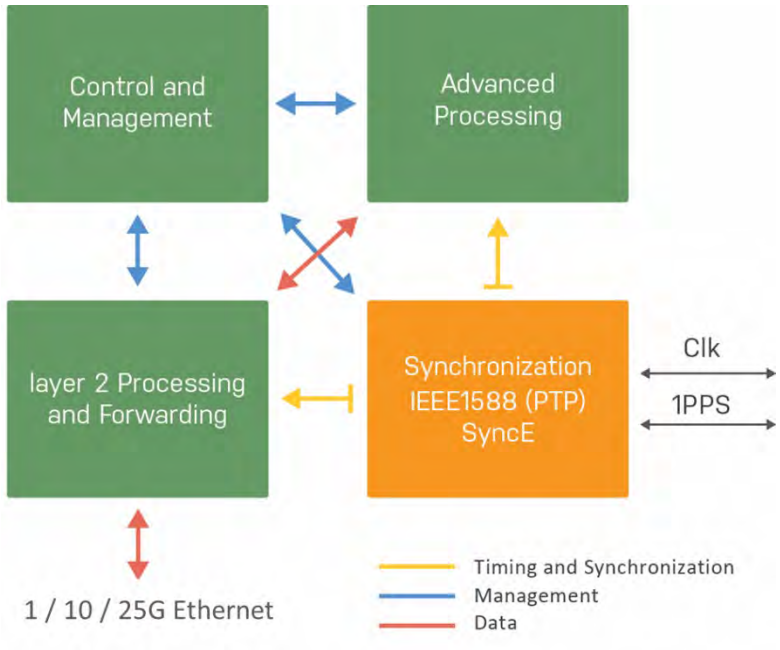


Figure 2-1: Functional block diagram

2.3 Management

The EdgeGM 7000 can be remotely managed via a variety of mechanisms and platforms:

- IP Based (in-band): SNMP (v1/v2/v3), Telnet, SSH, Web (HTTP, HTTPS).
- Console (RJ-45): RS-232 (115,200Bd), CLI (Cisco like).
- OAM/IEEE802.3ah: when connected to third party edge switch that supports the standard.

2.3.1 Management integration

Integration with 3rd party network management systems can be achieved via SNMP protocol, in addition to the following standards: NTPV4, SYSLOG, RADIUS, TACACS, DHCP, LACP, LLDP.

2.3.2 OAM & Diagnostics:

- IEEE802.3ah link OAM
- IEEE802.1ag CFM
- ITU-T Y.1731 PM (HW based measurements)
- Copper TDR
- SFP diagnostics (SFF-8472)
- Traffic mirroring

2.4 EdgeGM 7000 port features

EdgeGM ports can be configured to support special data-plain functions, extended traffic handling capabilities, more functionality, and processing power. These capabilities are Software and Firmware based and therefore field upgradeable and configurable.

The following special features are supported by the EdgeGM 7000 ports:

- Synchronous Ethernet
- IEEE1588-2008 - PTP
- Per port / queue policing
- Per port / queue shaping
- Per Port Counters: Support for frame and byte counters per port.
- Link OAM (IEEE802.3ah) and Service OAM (based on IEEE 802.1ag)
- Linear Ethernet Protection Switching (G.8031)
- Ethernet Ring Protection Switching (G.8032v2)
- TDR supports measuring of lines distance and calculates delays

3 Getting Started

The following topics are discussed in this chapter:

- Quick Setup Outline
- Console Connection and Configuration
- Web GUI

This page intentionally left blank.

3.1 Quick Setup Outline

To set up the EdgeGM 7000, carry out the following steps:

1. Mount the device at its location (rack or desktop).
2. Install the SFP transceivers.
3. Connect the unit to a console and a power source.
4. Verify that the Power (PS1, PS2 or both) LEDs are green lit.
5. Connect required cables to ports: twisted pair (RJ45 Ethernet) and fiber (Ethernet SFPs).
6. Verify that the ports Link and Speed LEDs are lit per connected interfaces.
7. Configure the selected device via the console to assign management IP address or use default IP address (192.168.1.90)
8. Establish management access via SSH, Telnet or Web GUI.

3.2 Console Connection and Configuration

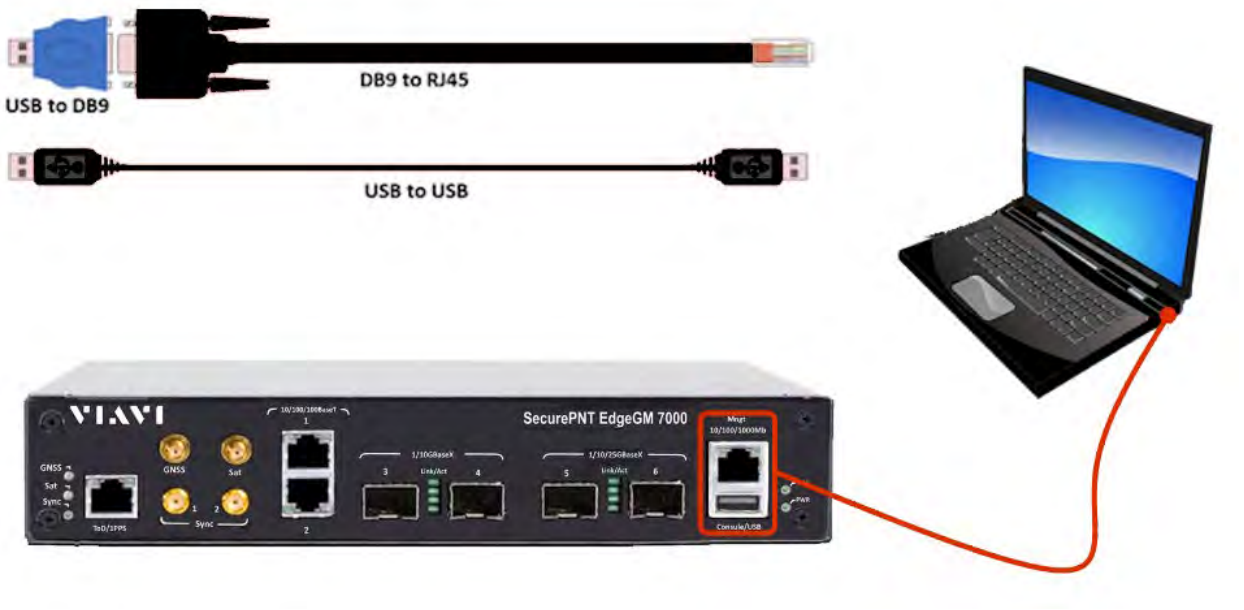


Figure 3-1: EdgeGM 7000 console connection

To enable basic console connection for initial setup, carry out the following steps:

1. Either:
    a. Connect a USB-to-USB cable from a PC directly to the USB port on EdgeGM 7000 front panel.
    b. Use an RJ-45-to-DB-9 console cable and insert the RJ-45 connector into the console port on the front panel.
2. Configure the baud rate and character format of the PC or terminal to match these console port default characteristics:
    - 115200 baud
    - 8 data bits
    - 1 stop bit

- No parity
- None (flow control)

3. Connect the device to a power source and wait until it boots up.
4. The system prompts you to log in.
   - Default username: **viavi02**
   - Default password: 25g#EGM7@@@

3.2.1 Initial IP address settings

This first configuration is done via the console; it enables the switch to connect to the IP network. Once the unit IP address is set via console, the system can be accessed through Web, Telnet, SSH or any other management options.

Initial IP setup can be implemented by manually setting the IP address Parameters or by an automatic DHCP setup (if a DHCP server is present).

The EdgeGM 7000 will initially boot-up with this default IP address: `192.168.1.90/24`

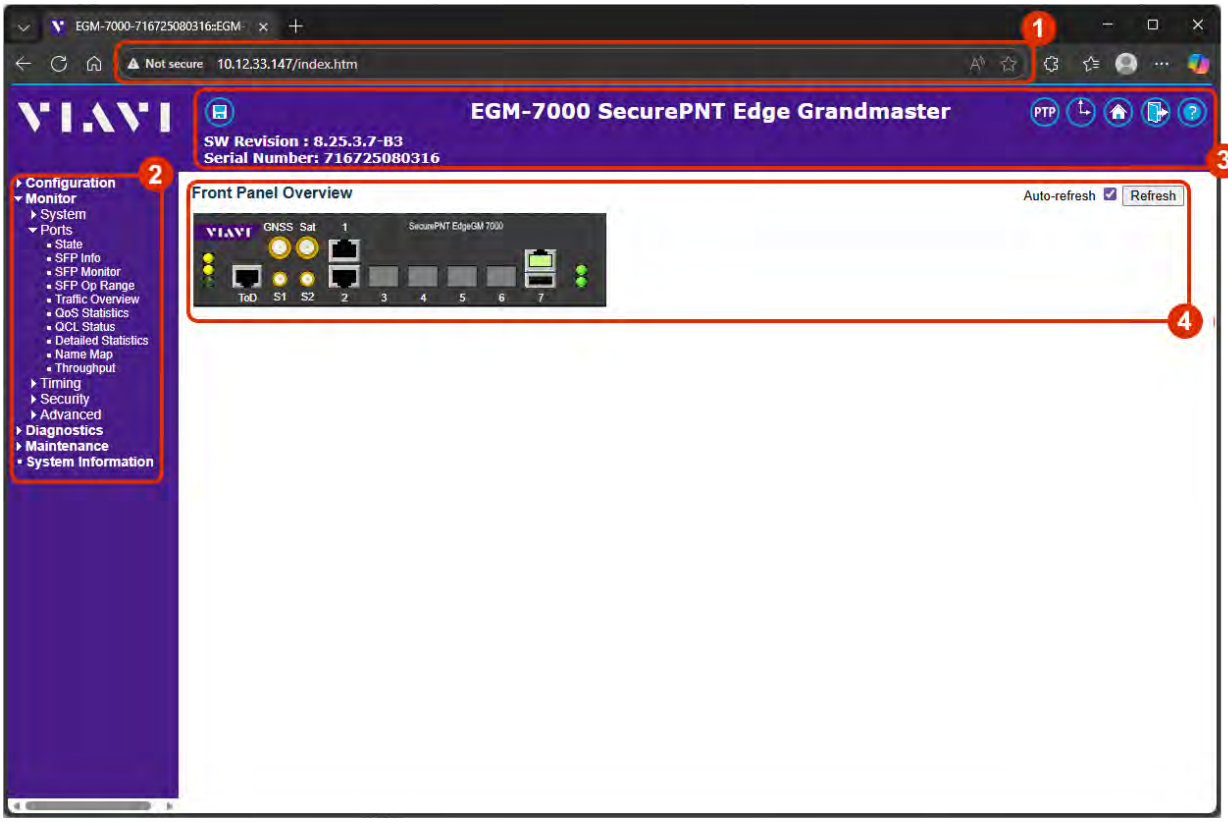
To assign a new IP address to the device enter the following CLI commands:

- `configure terminal`
- `interface vlan 1`
- `ip address 192.168.1.`*`XXX`*` 255.255.255.0`
  where *XXX* is any value between 0 and 255 except 90

3.3 Web GUI

The Web management is accessed by setting the required IP address in the URL Browser. When accessing the devices via the Web interface, its initial Port State Overview window is displayed.

Web GUI: Monitor > Ports > State



1	IP address of device in explorer URL line.
2	Five functionality management menus: Configuration, Monitor, Diagnostics, Maintenance, and System Information. **Configuration**: For setting all system parameters relevant to proper operation of the device. **Monitor**: Displays a variety of statuses from the device and other device info that enable system administrator to following up and check if the device is working properly. **Diagnostics**: Includes tools to diagnose and troubleshoot networking issues **Maintenance**: For restarting your device, returning to factory defaults and upgrading your device. **System Information:** Displays information about the device system, hardware, software, and firmware.

3	Main Bar: consists of the following buttons:  **Show help**: online help specific to the displayed dynamic configuration screen.  **Logout**: User can end access to device web site.  **Home**: Access to device front panel.  **Clock Central**: Control center of system synchronization interfaces and timing signal and their distribution.  **PTP:** Manage PTP clock instances
4	Dynamic configuration section: Displays detailed data for the selected from one of the functionality menus. • **Auto-refresh**: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds • **Refresh**: Click to refresh the page.

4 Functional Description

The following topics are discussed in this chapter:

- Overview
- Frame Processing Overview
- System Information
- Ports Configuration and Monitoring
- Security Features
- Clock Central Configuration
- Clock Central Monitoring
- GNSS Module
- IEEE1588 Precision Time Protocol
- Synchronous Ethernet (SyncE)
- Spanning Tree
- IP Multicast
- Link Aggregation
- LLDP-Link Discovery
- Link OAM
- RMON (Remote Network Monitoring)
- Loop Protection
- GVRP Configuration
- sFlow Consideration
- UDLD Configuration
- TSN

This page intentionally left blank.

4.1 Overview

This section provides introduction to the **EdgeGM 7000** functionality and instructions for configuration and monitoring.

The configuration and monitoring functionalities can be accessed via various management interfaces. This chapter demonstrates the configuration various functions and setting mainly using the Web interface. However, any configuration can be implemented using other management interfaces (CLI, Telnet, and SNMP).

4.2 Frame Processing Overview

This section provides a general description of the Frame Forwarding Process at the EdgeGM 7000 from the input port toward the output port, as illustrated below.

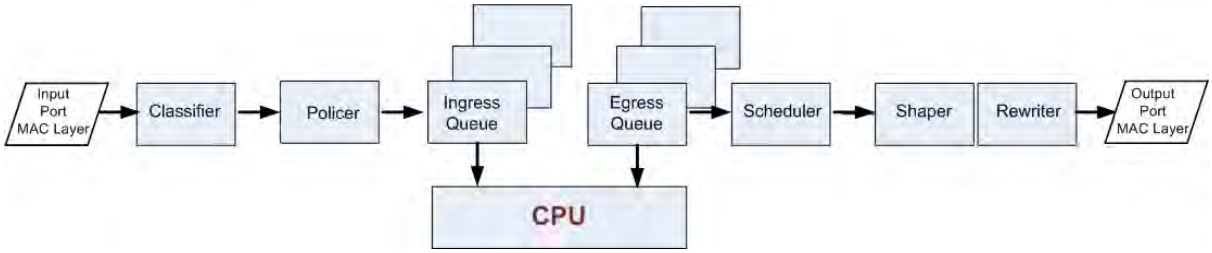


Figure 4-1: Frame Forwarding Diagram

Input frame flow

Frames received on the input port (MAC layer) are handed to the classifiers in order to classify frames into different flows (e.g., management frames, specific service/user frames, etc.). Following the classification, the frames are passed to the Policer. If the Policer is not selected the frames pass untouched. From the Policer the frames enter the Ingress Queue. Some prioritization algorithms are used to handle traffic and to avoid buffer overrun and Frame loss.

Output frame flow

The frames, which pass from the Ingress Queue, are transferred to the Egress Queue (8 parallel queues). The topmost queue handles management frames injected by the CPU, which have super priority over the other four queues. The remaining queues transfer data frames. At this stage, a scheduling process is taking place in order to decide which frame will be sent out of the port (out of the 8 candidate queues). For scheduling either a Strict-Priority or a Weighted Fair Queuing algorithm is being used. The output of the queue is passed to the Shaper. If the Shaper is not selected the frame passes untouched. The frames are then passed to the Rewriter. The Rewriter examines the frame header information and adjusts it if required. From there on the frame is sent to the output port (MAC layer).

Packet forwarding

Packet forwarding decisions are based on the following criteria:

- ACL:(Access Control List) The ACL can drop a frame or redirect it to a specific port
- MAC address and VLAN: The standard Ethernet switch forwarding – a frame is forwarded by searching the learn-table and sending it to the port where the MAC-address + VLAN was learnt. If the address is not found, or the frame is a broadcast frame it will be sent to all the other member ports of the VLAN.

4.3 System Information

The switch system information is provided here.

The display is similar in all EdgeGM 7000 series

4.3.1 System Information Configuration

Web GUI: Configuration > System > Information

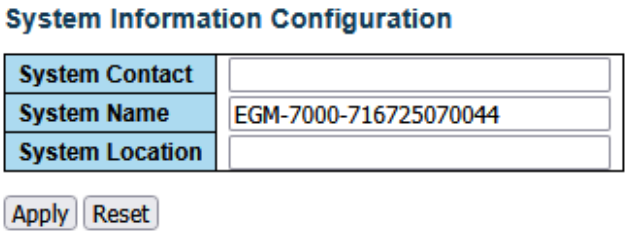


Figure 4-2: System Information Configuration

Table 4-1: System Information Configuration Parameters

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.

4.3.2

4.3.3 IP Configuration

Configure IP basic settings, control IP interfaces and IP routes. The maximum number of interfaces supported is 32 and the maximum number of routes is 32.

Web GUI: Configuration > System > IP

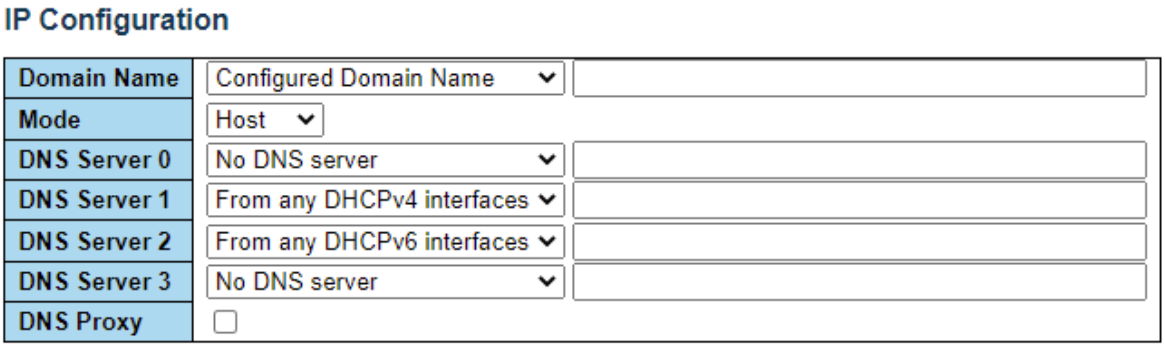


Figure 4-3: IP Configuration

Table 4-2: IP Configuration Parameters

IP Configuration- Basic Settings	
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	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. Only IPv4 DNS proxy is currently supported.

Web GUI: Configuration > System > IP

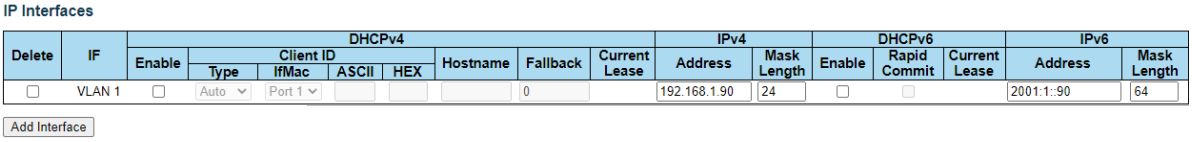


Figure 4-4: IPv4 / IPv6 Configuration

Table 4-3: IP Interfaces Parameters

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.
IPv4 DHCP 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
IPv4 DHCP Client Identifier Type	This specified which of the three types below, i.e., IfMac, ASCII or HEX, shall be used for the Client Identifier. See RFC-2132 section 9.14.
IPv4 DHCP Client Identifier IfMac	The interface name of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type is 'ifMac', the configured interface's hardware MAC address will be used in the DHCP option 61 field.
IPv4 DHCP Client Identifier ASCII	The ASCII string of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type is 'ascii', the ASCII string will be used in the DHCP option 61 field.
IPv4 DHCP Client Identifier HEX	The hexadecimal string of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type 'hex', the hexadecimal value will be used in the DHCP option 61 field.
IPv4 DHCP Hostname	The hostname of DHCP client. If DHCPv4 client is enabled, the configured hostname will be used in the DHCP option 12 field. When this value is empty string, the field use the configured system name plus the latest three bytes of system MAC addresses as the hostname.

IPv4 DHCP Fallback Timeout	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.
IPv4 DHCP 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.
IPv4 Mask	The IPv4 network mask, in number of bits (*prefix length*). Valid values are between 0 and 30 bits for a 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.
DHCPv6 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.
DHCPv6 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. A 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, 2001:1::90. 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.
IPv6 Mask	The IPv6 network mask, in number of bits (*prefix length*). Valid values are between 1 and 128 bits for a IPv6 address. The field may be left blank if IPv6 operation on the interface is not desired.
Resolving IPv6 DAD	The link-local address is formed from an interface identifier based on the hardware address which is supposed to be uniquely assigned. Once the DAD (Duplicate Address

	Detection) detects the address duplication, the operation on the interface SHOULD be disabled. At this moment, manual intervention is required to resolve the address duplication. For example, check whether the loop occurs in the VLAN or there is indeed other device occupying the same hardware address as the device in the VLAN. After making sure the specific link-local address is unique on the IPv6 link in use, delete and then add the specific IPv6 interface to restart the IPv6 operations on this interface.
Buttons	**Add Interface**: Click to add a new IP interface. A maximum of 8 interfaces is supported.

Web GUI: Configuration > System > IP

IP Routes

Delete	Network	Mask Length	Gateway	Distance(IPv4) / Next Hop VLAN(IPv6)
☐	0.0.0.0	0	192.168.5.1	1
☐	192.168.50.0	24	192.168.5.185	1

Figure 4-5: IP Routes

Table 4-4: IP Routes Parameters

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 0.0.0.0or 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 for a valid IPv6 notation. Gateway and Network must be of the same type.
Distance (Only for IPv4)	The distance value of route entry is used to provide the priority information of the routing protocols to routers. When there are two or more different routing protocols are involved and have the same destination, the distance value can be used to select the best path.
Next Hop VLAN (Only for IPv6)	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 VLAN for the gateway. If the IPv6 gateway address is not link-local, system ignores the next hop VLAN for the gateway.
Buttons	**Add Route** Click to add a new IP route. A maximum of 32 routes is supported.

4.3.4 Time

This section describes the Time Zone and Daylight Saving Time settings.

Web GUI: Configuration > System > Time

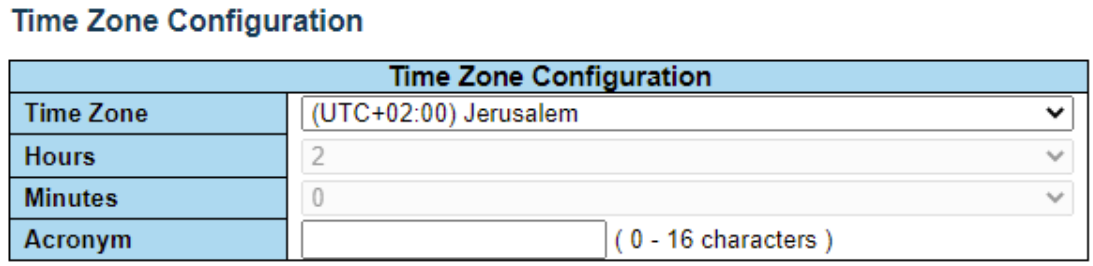


Figure 4-6: Time Zone Configuration

Table 4-5: Time Zone Configuration Parameters

Time Zone Configuration	
Time Zone	Lists various Time Zones worldwide. Select appropriate Time Zone from the drop down and click Save to set.
Hours / Minutes	Local time versus GMT (Greenwich Mean Time).
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)

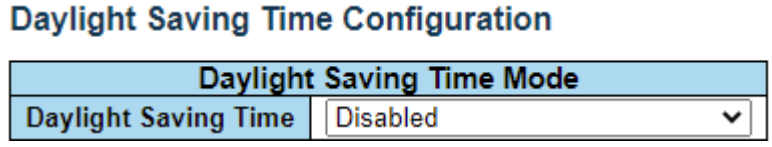


Figure 4-7: Daylight Saving Time Configuration

Table 4-6: Daylight Saving Time Configuration Parameters

Daylight Saving Time Mode	
This section is used to setup Daylight Saving Time Configuration	
Daylight Saving Time	Clear event occurred indication 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. (Default) 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.

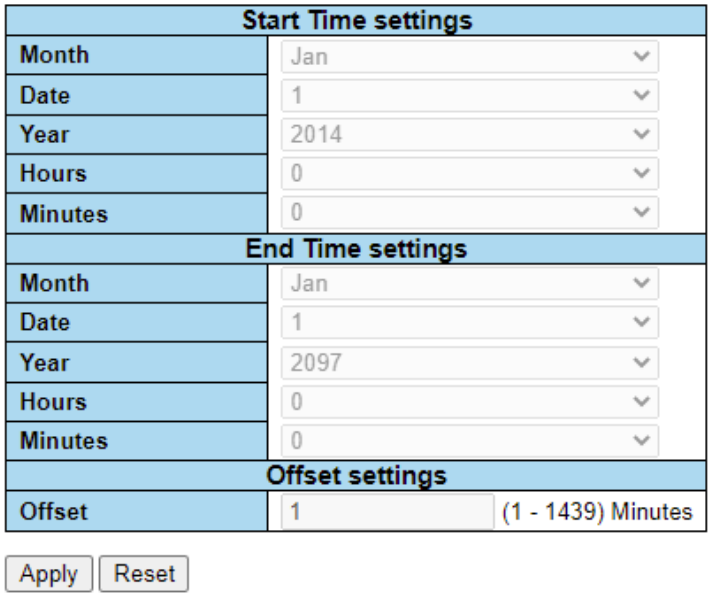


Figure 4-8: Time Settings displays

Table 4-7: Time Settings Parameters

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 1440)
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)

4.3.5 Log

Configure System Log on this section.

Web GUI: Configuration > System > Log

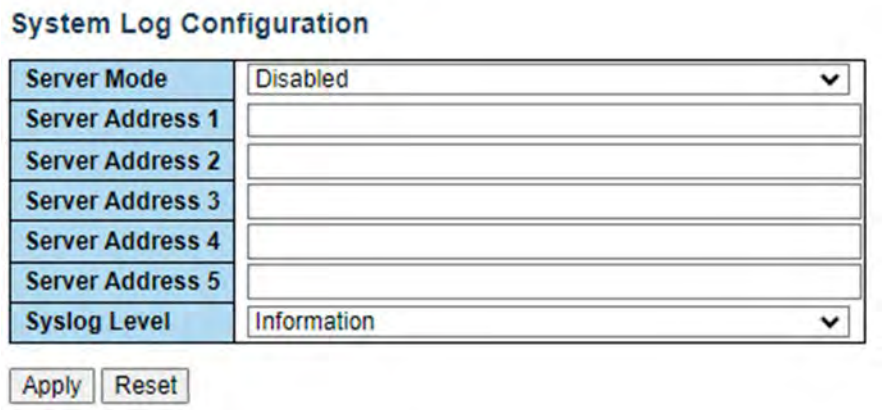


Figure 4-9: System Log Configuration displays

Table 4-8: System Log Configuration Parameters

System Log Configuration	
Server 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 server mode operation. **Disabled:** Disable server mode operation.
Server Address	Indicates the IPv4 host address of syslog server. If the switch provides DNS feature, it also can be a domain name.
Syslog Level	Indicates what kind of message will send to syslog server. Possible modes are: • **Error**: Send the specific messages which severity code is less or equal than Error (3). • **Warning**: Send the specific messages which severity code is less or equal than Warning (4). • **Notice**: Send the specific messages which severity code is less or equal than Notice (5). • **Informational**: Send the specific messages which severity code is less or equal than Informational (6).

4.3.1 Events

This page allows the user to change (enable/disable) and their corresponding interfaces to the current events configuration.

Web GUI: Configuration > System > Events

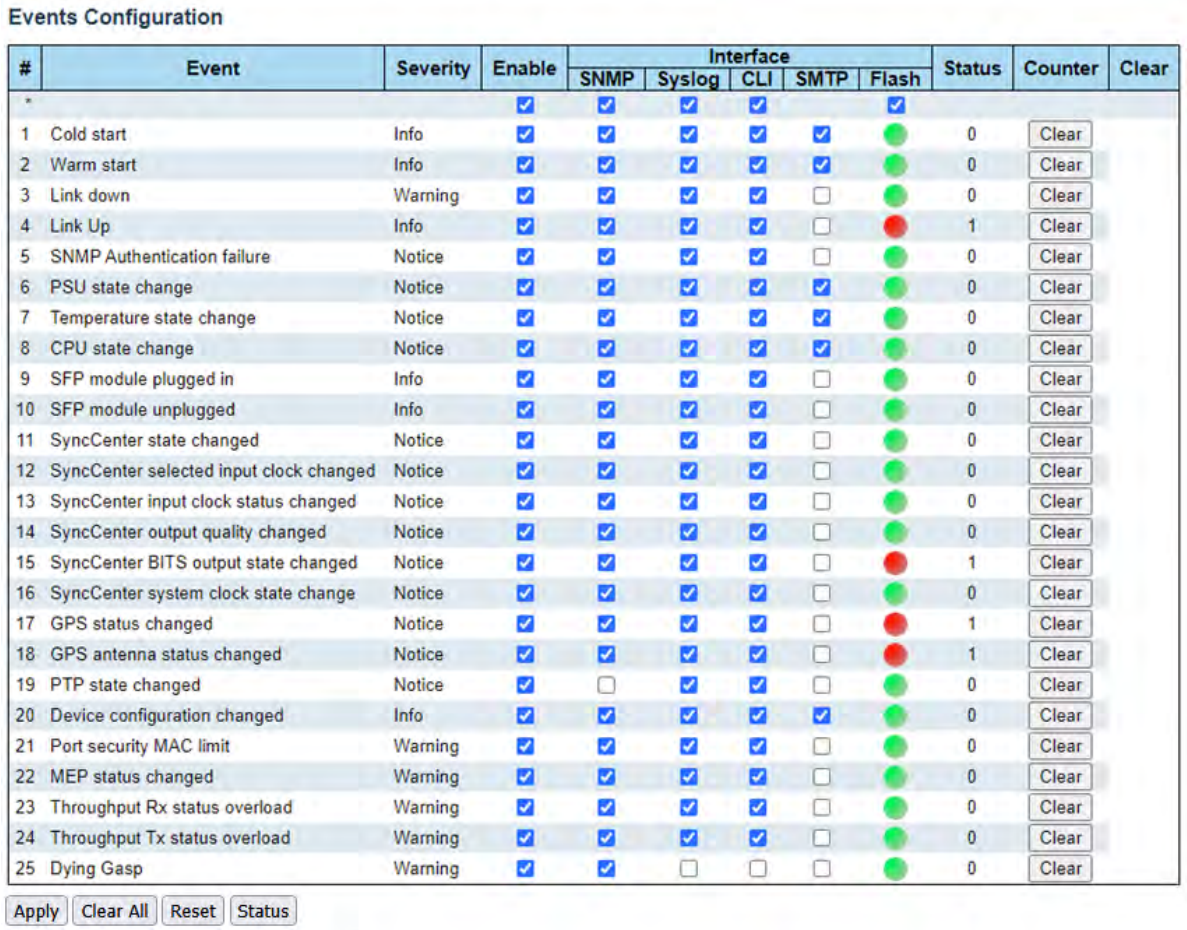


Figure 4-10: Events Configuration

Table 4-9: Events Configuration Parameters

#	Event Index
Event	Unique Name of the Event.
Severity	Indicates the severity of the event (Notice, Info, Warning).
Enable	Disable/Enable Event (Change will take effect on all checked interfaces: SNMP, syslog, cli).
Interface	Distribute event on a given interface: SNMP, Syslog, CLI, Flash.
Status	Indication whether an event occurred or not.
Counter	The number of occurrences of the event since last Clear operation.
Clear	Clear event occurred indication.

4.3.1 NTP Configuration

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. The EdgeGM 7000supports both client and server functions of the protocol.

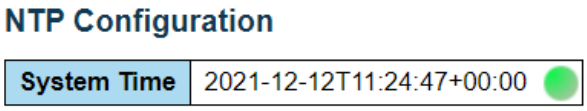


Figure 4-11: System Time Display

4.3.1.1 NTP Client Configuration

The NTP client configuration allows the switch to set the IP address of up to 5 different NTP servers as a time source. Additionally, server polling interval and encryption options can be configured. Maximum and minimum polling values in seconds are between 8-131072(approximately 36.4 hours).

Web GUI: Configuration > Timing > NTP

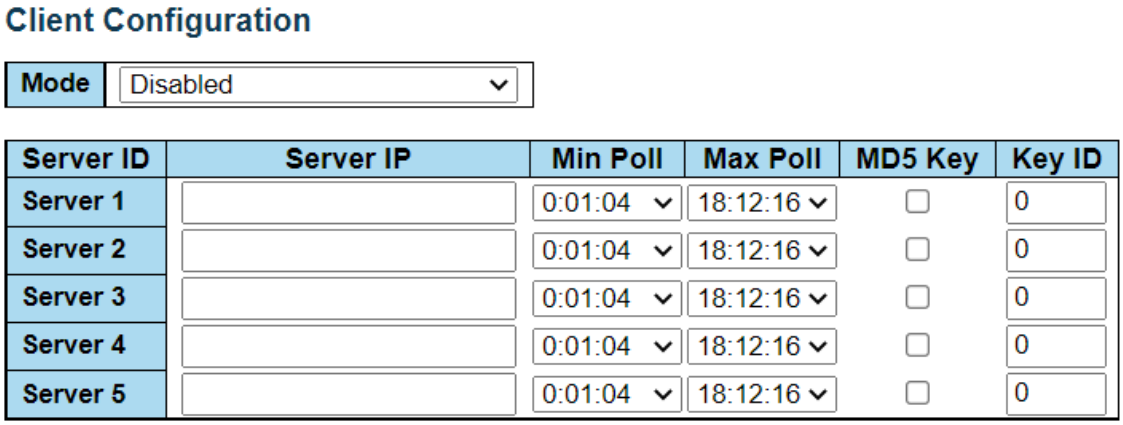


Figure 4-12: NTP Client Configuration

Table 4-10: NTP Client Configuration Parameters

Client Configuration	
Mode	Indicates the NTP Client operation mode. Possible modes are: **Enabled**: Enable NTP mode operation. **Disabled**: Disable NTP mode operation.
Server ID	Up to 5 different servers can be configured
Server IP	Provide the IPv4 or Ipv6 address of a NTP server..
Min Poll	Value in seconds. Available selected options are 2^3, 2^4, 2^5 … 2^{17}
Max Poll	Value in seconds. Available selected options are 2^3, 2^4, 2^5 … 2^{17}
MD5 Key	Enable per server MD5 encryption for NTP session authentication
Key ID	Set per server MD5 encryption key value for NTP session

4.3.1.2 NTP Server Configuration

EdgeGM 7000 NTP server function allows it to propagate the Clock Central time via NTP to other clients in the network. The server supports three operational modes: Unicast, Broadcast and Multicast. Allowed polling rate and encryption can be set for each mode separately.

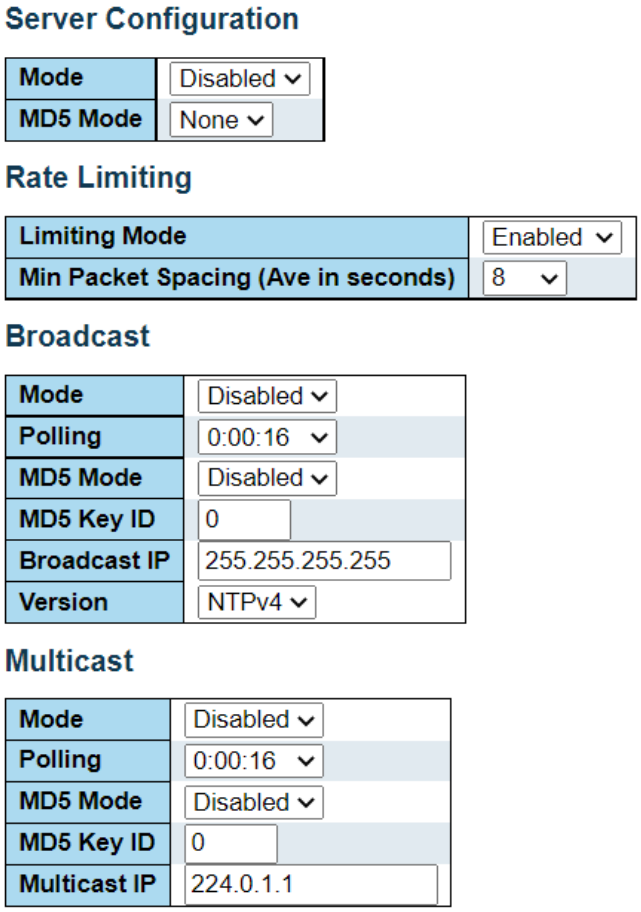


Figure 4-13: NTP Server Configuration

Table 4-11: NTP Server Configuration Parameters

Client Configuration	
Mode	Indicates the NTP Client operation mode. Possible modes are: **Enabled**: Enable NTP mode operation. **Disabled**: Disable NTP mode operation.
Server ID	Up to 5 different servers can be configured
Server IP	Provide the IPv4 or Ipv6 address of a NTP server..
Min Poll	Value in seconds. Available selected options are 2^3, 2^4, 2^5 … 2^{17}
Max Poll	Value in seconds. Available selected options are 2^3, 2^4, 2^5 … 2^{17}

MD5 Key	Enable per server MD5 encryption for NTP session authentication
Key ID	Set per server MD5 encryption key value for NTP session

4.4 Ports Configuration and Monitoring

This section shows current port configurations. Ports may be configured here.

Ports are also monitored here.

Web GUI: Configuration > System > Ports

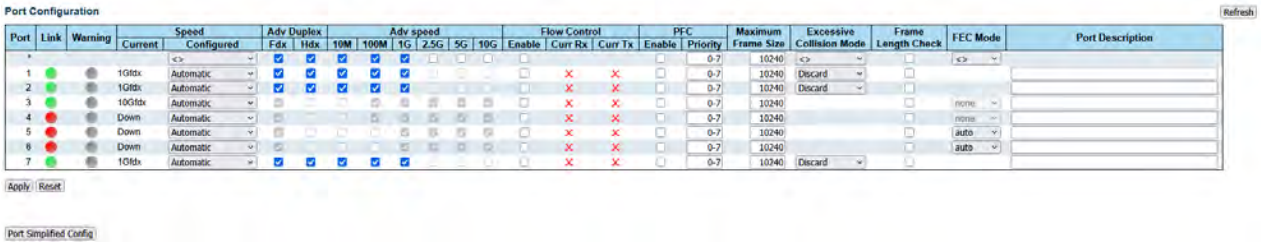


Figure 4-14: Port Configuration

Table 4-12: Port Configuration Parameters

Port	This is the logical port number for this row.
Link	The current link state is displayed graphically. • "**Green**" indicates that the link is up. • "**Red**" indicates that the link is down. • "**Grey**" Indicates that the port is inactive
Warning	Displays any warnings.
Current Speed	Provides the current link speed of the port.
Configured Speed	Selects available link speed for the given switch port. Only speeds supported by the specific port are shown. Possible speeds are: • **Disabled** - Disables the switch port operation. • **Auto** - Port auto negotiating speed and duplex with the link partner and selects the highest speed that is compatible with the link partner. • **10Mbps HDX** - Forces Cu port in 10Mbps half-duplex mode. • **10Mbps FDX** - Forces Cu port in 10Mbps full duplex mode. • **100Mbps HDX** - Forces Cu port in 100Mbps half-duplex mode. • **100Mbps FDX** - Forces Cu port in 100Mbps full duplex mode. • **1Gbps FDX** - Forces port in 1Gbps full duplex mode.

	• **2.5Gbps FDX** - Forces port in 2.5Gbps full duplex mode. • **10Gbps FDX** - Forces port in 10Gbps full duplex mode. • **25Gbps FDX** - Forces port in 25Gbps full duplex mode.
Advertise Duplex	When duplex is set as auto i.e., auto negotiation, the port will only advertise the specified duplex as either **FDX** or **HDX** to the link partner. By default, port will advertise all the supported duplexes if the Duplex is Auto.
Advertise Speed	When speed is set as auto, i.e., auto negotiation, the port will only advertise the specified speeds (10M, 100M, 1G, 2.5G, 10G, 25G) to the link partner. By default, port will advertise all the supported speeds if speed is set as Auto.
Flow Control	When "**Auto Speed"** is selected for a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed speed setting is selected, traffic that is what is selected. **Current Rx**: This column indicates whether pause frames on the port are obeyed. **Current Tx:** This 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. **Configured**: Check the configured column to use flow control; this setting is related to the setting for **Configured Link Speed.** NOTICE: The 100FX standard does not support Auto Negotiation, so when in 100FX mode the flow control capabilities will always be shown as "disabled".
PFC	When PFC (802.1Qbb Priority Flow Control) is enabled on a port then flow control on a priority level is enabled. Through the **Priority** field, range (one or more) of priorities can be configured, e.g., '0-3,7' which equals '0,1,2,3,7'. PFC is not supported through auto negotiation. PFC and Flow control cannot both be enabled on the same port.
Maximum Frame Size	Enter the maximum frame size allowed for the switch port, including FCS. The range is 1518-9600 bytes.
Excessive Collision Mode	Configure port transmit collision behavior: **Discard**: Discards frame after 16 collisions (default). **Restart**: Restarts backoff algorithm after 16 collisions.
Frame Length Check	Configures if frames with incorrect frame length in the EtherType/Length field shall be dropped. An Ethernet frame contains a field EtherType which can be used to indicate the frame payload size (in bytes) for values of 1535 and below. If the EtherType/Length field is above 1535, it indicates that the field is used as an EtherType (indicating which protocol is encapsulated in the payload of the frame). If "frame length check" is enabled, frames with payload size less than 1536

	bytes are dropped, if the EtherType/Length field doesn't match the actual payload length. If "frame length check" is disabled, frames are not dropped due to frame length mismatch. Note: No drop counters count frames dropped due to frame length mismatch
FEC Mode	Toggle Enable/Disable Reed-Solomon Forward Error Correction
Description	User defined free text (up to 63 characters)
Buttons	**Apply** - **Reset** - **Refresh** - **Port detailed** - **Port Simplified Config** -

4.4.1 Port State

This section provides an overview of the current switch port states (Each EdgeGM 7000 device has its own Port State display).

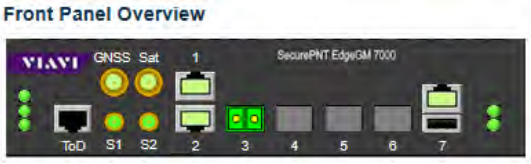


Figure 4-15: Port State

The port states are illustrated as follows:

RJ45 ports			
SFP ports			
GNSS/SAT ports			
State	Disabled	Down	Link

4.4.2 SFP Information

This section shows SFP Information.

Web GUI: Monitor > Ports > SFP Info

SFP Information

Port	Vendor	Part #	Type	Range	Wavelength (nm)		Serial #
					Transmit	Receive	
3							
4							
5							
6							

Figure 4-16: SFP information

Table 4-13: SFP Information Parameters

Vendor #	Indicates vendor's name.
Part #	Indicates part number.
Type	Indicates module Type.
Range	Indicates the SFP's nominal optical range.
Wavelength	Indicates the SFP wavelength (separately for transmit and receive).
Serial #	Indicates the SFP's serial number.

4.4.1 SFP Monitoring

This section shows SFP digital diagnostic information

Web GUI: Monitor > Ports > SFP Monitor

SFP Monitoring

Port	Status	Rx Power	Tx Power	Temperature	Bias current	Supply voltage
3				Unplugged		
4				Unplugged		
5				Unplugged		
6				Unplugged		

Figure 4-17: SFP Monitoring

Table 4-14: SFP Monitoring Parameters

RX Power	Modules receive optical power [dBm].
TX Power	Modules transmit optical power [dBm].
Temperature	Module's internal temperature.
Bias Current	Module's transmitter bias current [mA].
Supply voltage	Module's supply voltage [V].

Note: Green indicator implies that the parameters are within the allowed range

4.4.2 SFP Operational Range

This section shows SFP operational range.

Web GUI: Monitor > Ports > SFP Op Range

SFP Operational Range

Port	Status	Rx Power	Tx Power	Temperature	Bias current	Supply voltage
3				Unplugged		
4				Unplugged		
5				Unplugged		
6				Unplugged		

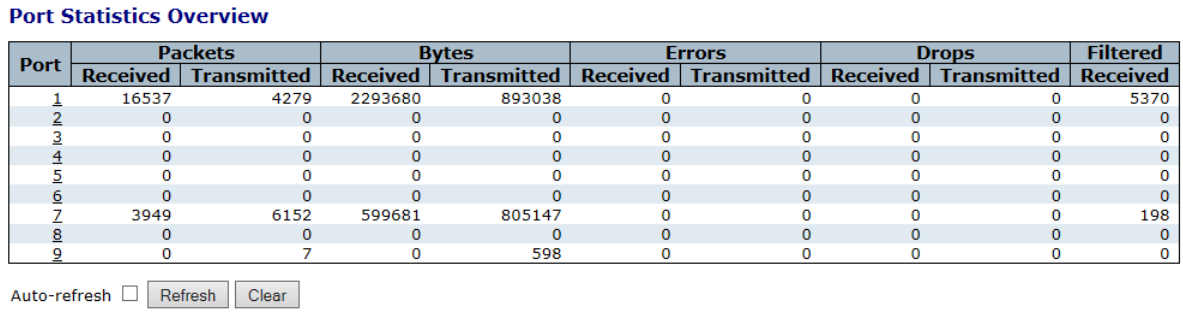
Figure 4-18: Operational Range

Table 4-15: SFP Operational Range Parameters

Port	The physical port in which the SFP is installed
Status	The status of the SFP port: • **Grey**=unplugged • **Red**=when SFP is plugged and operational • **Green** when the SFP is connected to another similar SFP (installed in another device)
RX Power	Module's allowed receive optical power range [dBm].
TX Power	Module's allowed transmit optical power range [dBm]
Temperature	Module's allowed internal temperature range.
Bias Current	Module's allowed transmitter bias current range [mA].
Supply voltage	Module's allowed supply voltage range [V].

4.4.3 Traffic Overview

Web GUI: Monitor > Ports > Traffic Overview



Port Statistics Overview

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	16537	4279	2293680	893038	0	0	0	0	5370
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	3949	6152	599681	805147	0	0	0	0	198
8	0	0	0	0	0	0	0	0	0
9	0	7	0	598	0	0	0	0	0

Auto-refresh ☐ Refresh Clear

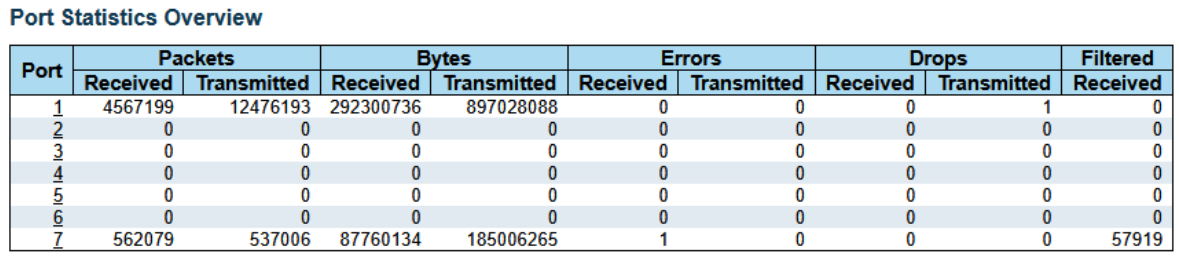
Figure 4-19: Port Statistics

Table 4-16: Port Statistics Overview Parameters

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 frames discarded due to ingress or egress congestion

4.4.4 QoS Statistics

Web GUI: Monitor > Ports > Traffic Overview



Port Statistics Overview

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	4567199	12476193	292300736	897028088	0	0	0	1	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	562079	537006	87760134	185006265	1	0	0	0	57919

Figure 4-20: Queuing Counters Display

Table 4-17: Queuing Counters Parameters

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.

4.4.5 QoS Control List Status

This section 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.

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.

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.

Web GUI: Monitor > Ports > QCL Status

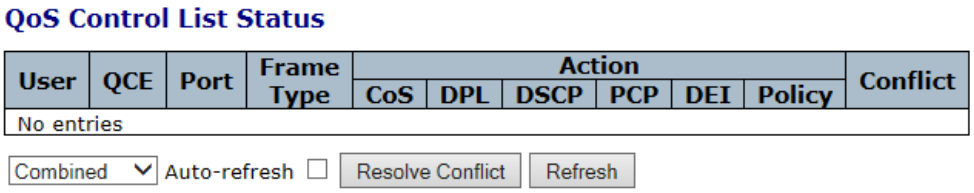


Figure 4-21: QoS Control List Status

Table 4-18: QoS Control List Status Parameters

User	Indicates the QCL user.
QCE	Indicates the index of QCE.
Frame type	Indicates the type of frame to look for incoming frames. Possible frame types are: • **Any**: Match any frame type. • **Ethernet**: Match Ether type frames. • **LLC:** Match (LLC) frames • **SNAP**: Match (SNAP) frames • **IPv4**: Match IPV4 frames. • **IPv6:** Match IPV6 frames.
Port	Indicates the list of ports configured with the QCE.
Action	Indicates the classification action taken on ingress frame if Parameters configured are matched with the frame's content. • There are three action fields: Class, DPL and DSCP. • CoS: Classify Class of Service • DPL: Classify Drop Precedence Level • DSCP: Classify DSCP value • PCP: Classify PCP value • DEI: Classify DEI value. • Policy: Classify ACL Policy number. • Ingress Map: Classify Ingress Map ID.

Conflict	Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that the 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 **Resolve Conflict:** Click to release the resources required to add QCL entry in case the conflict status for any QCL entry is 'yes'.

4.4.6 Detailed Port Statistics

This section provides detailed traffic statistics for a specific switch port. Use the port select box to select what 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.

Web GUI: Monitor > Ports > QCL Status

Detailed Port Statistics Port 1

Receive Total		Transmit Total	
Rx Packets	5819	Tx Packets	1106
Rx Octets	479205	Tx Octets	203183
Rx Unicast	304	Tx Unicast	296
Rx Multicast	372	Tx Multicast	807
Rx Broadcast	5143	Tx Broadcast	3
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	4747	Tx 64 Bytes	37
Rx 65-127 Bytes	678	Tx 65-127 Bytes	930
Rx 128-255 Bytes	233	Tx 128-255 Bytes	52
Rx 256-511 Bytes	153	Tx 256-511 Bytes	33
Rx 512-1023 Bytes	8	Tx 512-1023 Bytes	11
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	43
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	5819	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	1106
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	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	376		

Figure 4-22: Detailed Port Statistics

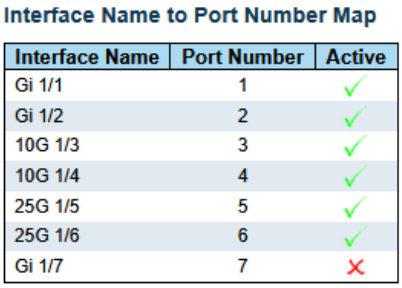
Table 4-19: Detailed Port Statistics Parameters

Receive Total and Transmit Total	
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. Includes FCS but excludes 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 have 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 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	
Rx Drops	The number of frames dropped due to lack of receives buffers or egress congestion.
Rx CRC/Alignment	The number of frames received with CRC or alignment errors.
Rx Undersize	The number of short [1] frame received with valid CRC. [1] Short frames are frames that are smaller than 64 bytes**.**
Rx Oversize	The number of long [2] frames received with valid CRC. [2] Long frames are frames that are longer than the configured maximum frame length for this port**.**
Rx Fragments	The number of short [1] frame received with invalid CRC.
Rx Jabber	The number of long [2] frames received with invalid CRC.
Rx Filtered	The number of received frames filtered by the forwarding process.
[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	
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.

4.4.7 Interface Name to Port Number Map

This page provides a mapping of Interface Names to their corresponding port numbers, and whether the interface is active or not.



Interface Name to Port Number Map

Interface Name	Port Number	Active
Gi 1/1	1	✓
Gi 1/2	2	✓
10G 1/3	3	✓
10G 1/4	4	✓
25G 1/5	5	✓
25G 1/6	6	✓
Gi 1/7	7	✗

Figure 4-23: Interface Name to Port Number Map

4.5 Security Features

EdgeGM 7000 enables a set of security features. Security is realized by several different mechanisms included in the Switch and Network section.

4.5.1 Switch

The Switch section contains the following sub-sections:

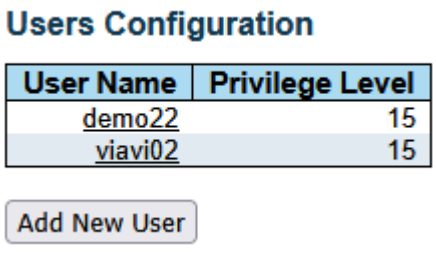
- User Configuration
- Privilege Level Configuration
- Authentication Method Configuration
- SSH Configuration
- HTTPS Configurations
- Access Management Configuration
- Access Management Statistics

4.5.1.1 User Configuration

This subsection 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.

Web GUI: Configuration > Security > Switch > Users



Users Configuration

User Name	Privilege Level
demo22	15
viavi02	15

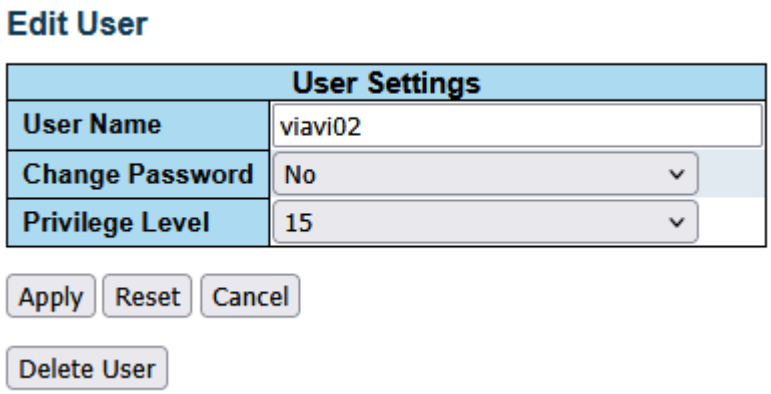
Add New User

Figure 4-24: User Configuration

Table 4-20: User Configuration Parameters

Username	The name identifying the 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 fully control of the device. Other values 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, group privilege level 5 has the read-only access and privilege level 10 has the read-write access. System maintenance (software upload, factory defaults 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	**Add New User:** Click to add a new user. The maximum numbers of users is 20. Marcello is a new added User with privilege level 10

By clicking on a user you get the following edit display which can be modified:



By clicking on **Add New User** on the previous User configuration display, you may add a new user.

Web GUI: Configuration > Security > Switch > Users

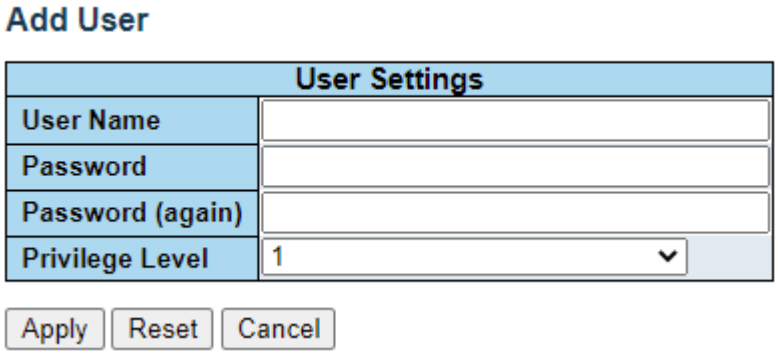


Figure 4-25: Add/Edit User Configurations

Table 4-21: Add/Edit User Configuration Parameters

Username	A string identifying the username that this entry should belong to. The allowed string length is 1 to 31. The valid username allows letters, numbers and underscores.
Password	The password of the user. The allowed string length is 0 to 31. Any printable characters including Space is accepted
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 other values must 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 etc.) need 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	**Delete User:** Delete the current user. This button is not available for new configurations (Add new user). Marcello is a new added User with privilege level 10

4.5.1.2 Privilege Level Configuration

This subsection provides an overview of the privilege levels.

Web GUI: Configuration > Security > Switch > Privilege Levels

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
Alarm	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
ERPS	5	10	5	10
ETH_LINK_OAM	5	10	5	10
Firmware	5	10	5	10
Green_Ethernet	5	10	5	10
IP	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
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

Apply Reset

Figure 4-26: Privilege Level Configuration

Table 4-22: Privilege Configuration Level Parameters

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 contains more than one. The following description defines these privilege level groups in detail: • **System**: Contact, Name, Location, Time zone, 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 Levels	The Privilege Levels can be configured between 0 to 15 (where 0 is lowest level and 15 is highest level) Every group has an authorization Privilege 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.

4.5.1.3 Authentication Method Configurations

This subsection allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces. The figure has one row for each client type and several columns.

Web GUI: Configuration > Security > Switch > Auth Method

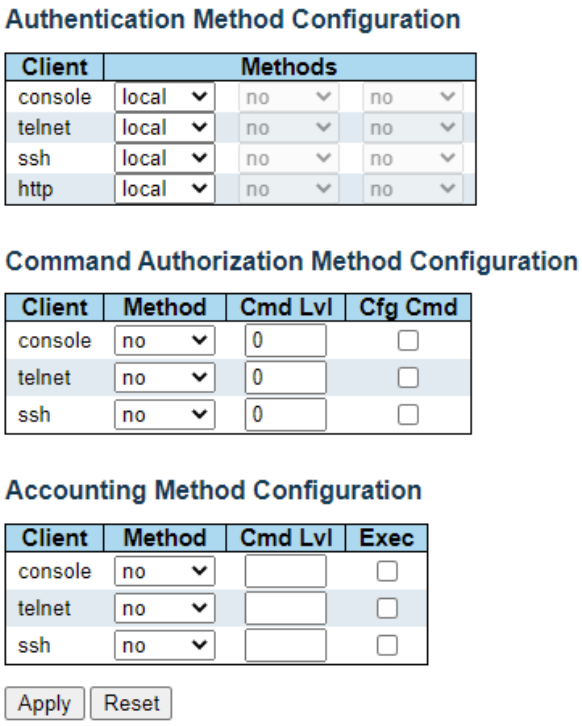


Figure 4-27: Authentication Method Configurations displays.

Table 4-23: Authentication Method Configurations Parameters

Authentication Method Configuration	
Client	The management client for which the configuration below applies.
Authentication Methods	Authentication 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 a remote RADIUS server for authentication. • **tacacs+**: use a remote TACACS+ server for authentication
Methods that involve 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 of 0 to 15.
Cfg Cmd	Also authorize configuration commands.
Accounting Method Configuration	
Client	The management client for which the configuration below applies.
Method	Method can be set to one of the following values: • **no**: Accounting is disabled. • **tacacs**: Use remote TACACS+ server(s) accounting.
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.
Exec	Enable exec (login) accounting.

4.5.1.4 SSH Configuration

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

Web GUI: Configuration > Security > Switch > SSH

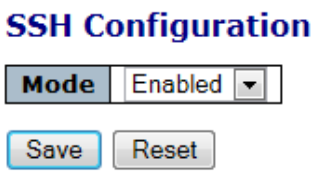


Figure 4-28: SSH Configuration

Table 4-24: Authentication Method Configuration Parameters

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

4.5.1.5 HTTPS Configuration

HTP 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 sends an HTTP command to the Web server directing 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.

Web GUI: Configuration > Security > Switch > HTTP

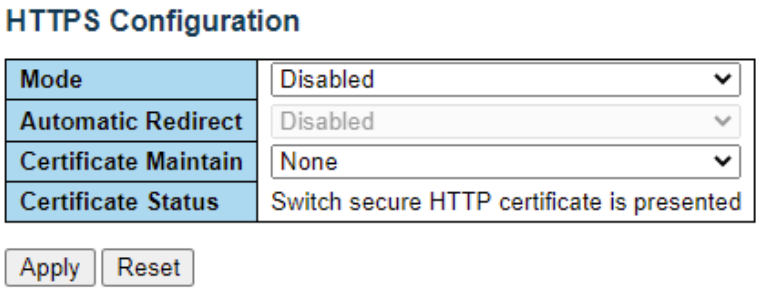
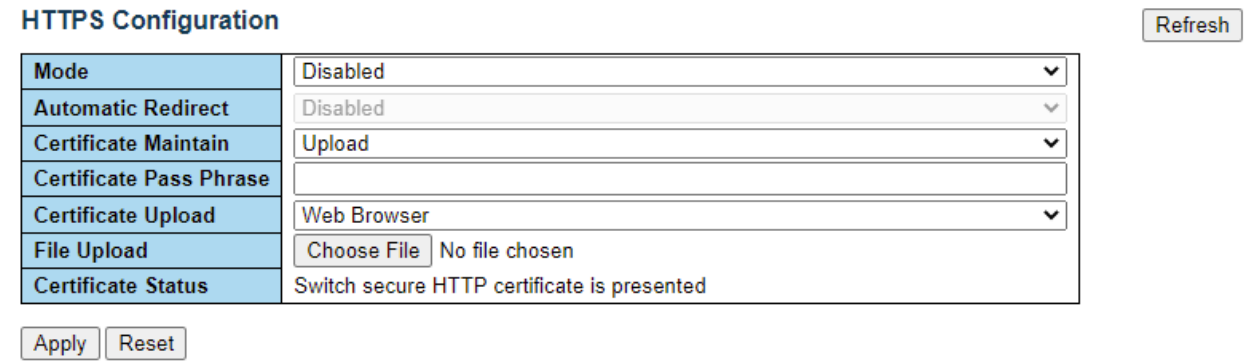


Figure 4-29: HTTPS Configuration

Table 4-25: HTTPS Configuration Parameters

Mode	Indicate the HTTPS mode operation. Possible modes are: **Enabled**: Enable HTTPS mode operation. **Disabled**: Disable HTTPS mode operation.
Automatic Redirect	Indicate the HTTPS redirect mode operation. It is only significant when "HTTPS Mode Enabled" is selected. When the redirect mode is enabled, the HTTP connection will be redirected to HTTPS connection automatically. Notice that the browser may not allow the redirect operation due to the security consideration unless the switch certificate is trusted to the browser. You need to initialize the HTTPS connection manually for this case. Possible modes are: **Enabled**: Enable HTTPS redirect mode operation. **Disabled**: Disable HTTPS redirect mode operation
Certificate Maintain	The operation of certificate maintenance. Possible operations are: 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.
By choosing the **Upload** option in the Certificate Maintain, the following display is shown, the parameters of which are explained below.	



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 (-), underscore (_). 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.

4.5.1.6 Access Management Configuration

In this subsection, you may configure the access management configuration.

The maximum number of entries is **16**. If the application type matches any one of the access management entries, it will allow access to the switch.

Web GUI: Configuration > Security > Switch > Access Management

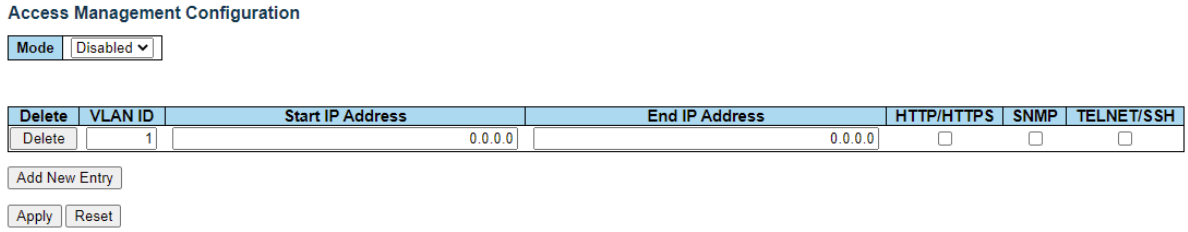


Figure 4-30: Access Management Configuration display

Table 4-26: Access Management Configuration parameters

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 save.
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 that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.
SNMP	Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry
TELNET/ SSH	Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.
Buttons	**Add New Entry:** Click to add a new access management entry.

4.5.1.7 Access Management Statistics

This sub-section provides statistics for selected access management.

Web GUI: Monitor > Security > Access Management Statistics

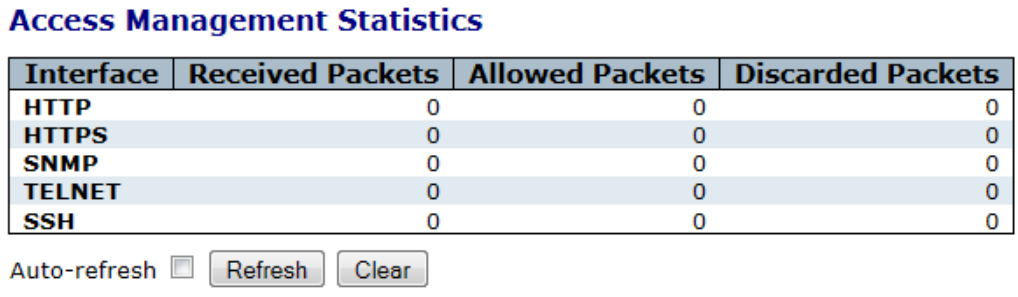


Figure 4-31: Access Management Statistics display

Table 4-27: Access Management Statistics Parameters

Interface	The interface type through which the remote host can access the switch.
Received Packets	Number of received packets from the interface when access management mode is enabled.
Allowed Packets	Number of allowed packets from the interface when access management mode is enabled.
Discarded Packets	Number of discarded packets from the interface when access management mode is enabled.

4.5.2 Network Security

Network Security includes the following subjects:

- MAC Limit
- Port Security switch and Port Security port status
- Network Access Server (NAS)
- Access Control List (ACL)
- IP Source Guard ARP Inspection

4.5.2.1 Port Security Configuration

This section describes the port security settings.

Web GUI: Configure > Security > Network > Port Security > Configuration

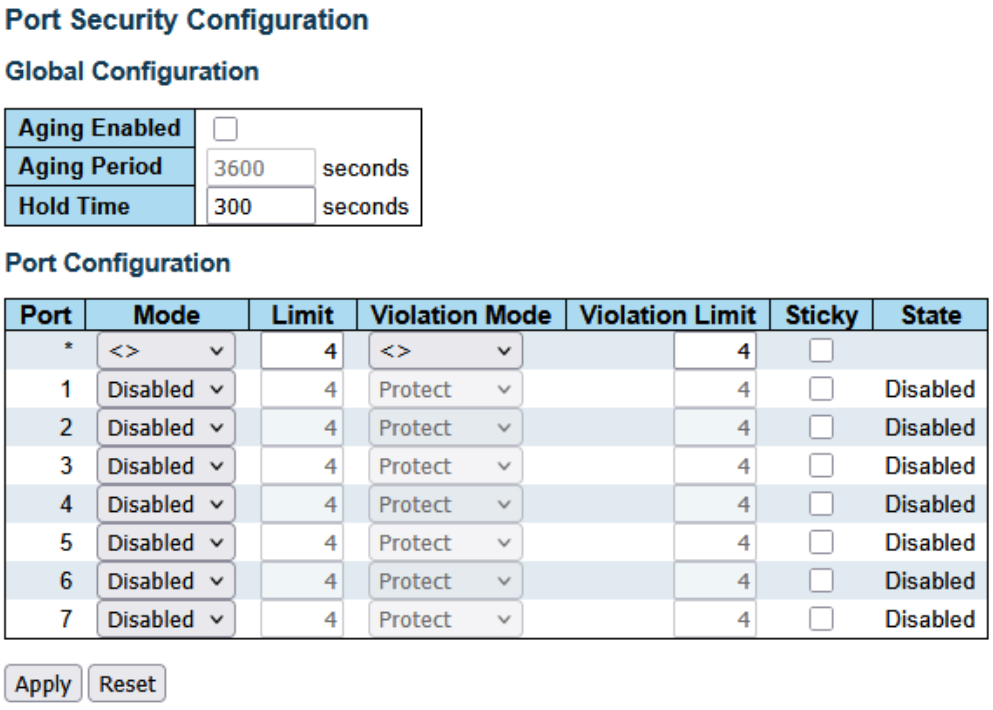


Figure 4-32: Port Security Configuration

Table 4-28: System and Port Configuration Parameters

Global Configuration	
Mode	Indicates if **Limit Control is globally enabled** or disabled on the switch. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.
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 were not 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).
The table has one row for each port on the selected switch and several columns.	
Port Configuration	
Port	The port number to 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 1023. Default is 4. If the limit is exceeded, an action is taken corresponding to the violation mode. 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 addresses 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 1023. Default is 4. It is only used when Violation Mode is **Restrict**.
Sticky	Enables sticky learning of MAC addresses on this port. When the port is in sticky mode, all MAC addresses that would otherwise have been learned as dynamic are learned as sticky. Sticky MAC addresses are part of the running-config and can therefore be saved to startup-config. Sticky MAC addresses survive link changes (in contrast to Dynamic, which will have to be learned again). They also survive reboots if running-config is saved to startup-config. 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 management-wise 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 Shut down or Trap & Shutdown.

Re-open Button	If a port is shut down by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to Shut down in the Action section. *Note that clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost.*

4.5.2.2 Port Security Switch Status

This section 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.

Web GUI: Monitor > Security > Network > Port Security > Overview

Port Security Switch Status

User Module Legend

User Module Name	Abbr
Port Security (Admin)	P
802.1X	8
Voice VLAN	V

Port Status

Clear	Port	Users	Violation Mode	State	MAC Count		
					Current	Violating	Limit
Clear	1	---	Disabled	Disabled	-	-	-
Clear	2	---	Disabled	Disabled	-	-	-
Clear	3	---	Disabled	Disabled	-	-	-
Clear	4	---	Disabled	Disabled	-	-	-
Clear	5	---	Disabled	Disabled	-	-	-
Clear	6	---	Disabled	Disabled	-	-	-
Clear	7	---	Disabled	Disabled	-	-	-

Figure 4-33: Port Security Switch Status

Table 4-29: System and Port Configuration Parameters

User Module Legend	
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 (see below).
Port Status	
The table has one row for each port on the selected switch and several columns.	
Clear	Click to remove all dynamic 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 to which the configuration below applies. Click the port number to see the status for this port. Refer to next page.
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 (see Abbr above) 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 the arrival of frames from unknown MAC addresses. • **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 Webpage.
Mac Count (Current, Violating Limit)	The three columns indicate the number of currently learned MAC addresses (forwarding as well as blocked), the number of violating MAC address (only counting in Restrict mode) 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 Port Security is not administratively enabled on the port, the Violating and Limit columns will show a dash (-).

4.5.2.3 Port Security Port Status

This section 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.

Notice that if you have added static or sticky MAC addresses, they will show up on this page only if Port Security is enabled on the interface to which they pertain.

Web GUI: Monitor > Security > Network > Port Security > Details

Figure 4-34: Port Security Port Status

Table 4-30: Port Security Port Status Parameters

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.
Time of Addition	Shows the date and time when this MAC address was first seen on the port.

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.

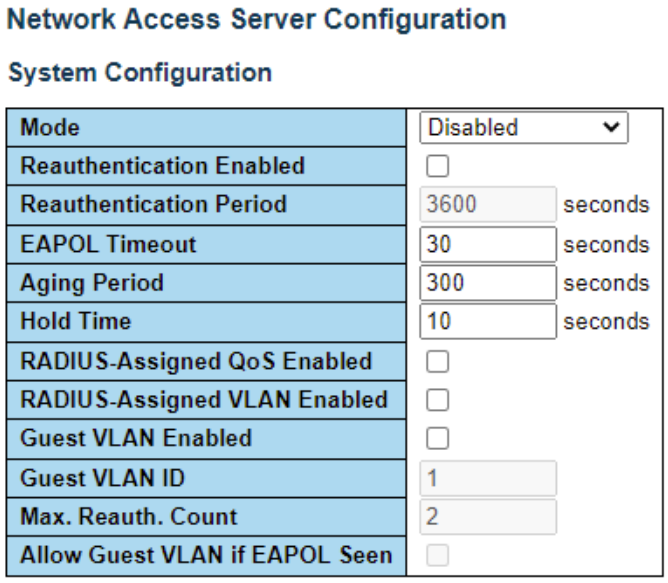
4.5.2.4 Network Access Server Configuration

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" section. 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 does not 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 802.1 X authentications

The NAS configuration consists of two sections, System and Port Configurations.



Web GUI: Monitor > Security > Network > NAS

Figure 4-35: Network Access Server Configuration

Table 4-31: Network Access Server Configuration Parameters

System Configuration	
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 (see **Aging Period** below)
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. 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 an 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 does not 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**") 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 (Refer to RADIUS-Assigned QoS Enabled within Port Configuration-see below) for a detailed description). 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 on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on 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 (see RADIUS-Assigned VLAN Enabled within Port Configuration below) for a detailed description. 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 on that port. When unchecked, RADIUS-server assigned VLAN is disabled on 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 on 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 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 lifetime 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 lifetime 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 lifetime of the port. The value can only be changed if the Guest VLAN option is globally enabled.
Port Configuration	
The table below has one row for each port on the switch several columns	
Port	The port number for which the configuration below applies.
Admin State	
If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:	
Force Authorized	In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication
Force Unauthorized	In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.

Port-based 802.1X	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 authenticator 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 PDUs (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, likeMD5-Challenge,PEAP, and TLS. The important thing is that the authenticator (the switch) does not 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 or block traffic on the switch port connected to the supplicant.
Single 802.1X	In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really are not authenticated. To overcome this security breach, use the Single 802.1X variant. Single 802.1X is not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant does not provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated

Multi 802.1X	Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module. In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

MAC-based Auth.	Unlike port-based 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-Challengeauthentication 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 the Port Security module. 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 port-based 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 do not need special supplicant software to authenticate. The advantage of MAC-based authentication over 802.1X-based authentication is that the clients do not 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. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

RADIUS-Assigned QoS Enabled	When RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e., • Port-based 802.1X • Single 802.1X RADIUS attributes used in identifying a QoS Class: The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet. Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule: • All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '7', which translates into the desired QoS Class in the range [0; 7].

RADIUS-Assigned VLAN Enabled	When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e., • Port-based 802.1X • Single 802.1X For troubleshooting VLAN assignments, use the " VLANs→VLAN Membership Status and VLAN Port Status pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration. RADIUS attributes used in identifying a VLAN ID: RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used: The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet. The switch looks for the first set of these attributes that have the same Tag value and fulfil the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag): - Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6). - Value of Tunnel-Type must be set to "VLAN" (ordinal 13). - Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].

Guest VLAN Enabled	When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below. This option is only available for EAPOL-based modes, i.e.: • Port-based 802.1X • Single 802.1X • Multi 802.1X For troubleshooting VLAN assignments, use the " → VLANs → VLAN Membership Status and VLAN Port Status" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration. Guest VLAN Operation: When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count (refer to System Configuration above) and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen (refer to System Configuration above) is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed -Refer to Port Configuration), and if not, the port will be placed in the Guest VLAN. Otherwise, it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout. Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN. While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.

Port State	The current state of the port. It can undertake one of the following values: • **Globally Disabled**: NAS is globally disabled. Link Down: NAS is globally enabled, but there is no link on the port. • **Authorized**: The port is in Force Authorized (Refer to Port Configuration above) or a single-supplicant mode and the supplicant is authorized. • **Unauthorized**: The port is in Force Unauthorized ((Refer to Port Configuration above) or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server. • **X Auth/Y Unauth**: The port is in a multi-supplicant mode. Currently X clients are authorized, and Y are unauthorized.
Restart	Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State (Refer to beginning of Port Configuration above) is in an EAPOL-based or MAC-based mode (Refer to f Port Configuration above). Clicking these buttons will not cause settings changed on the page to take effect. • **Reauthenticate**: Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized. • **Reinitialize**: Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

4.5.2.5 Network Access Server Switch Status

This section provides an overview of the current NAS port states for the selected switch.

Web GUI: Monitor > Security > Network > NAS > Switch

Network Access Server Switch Status

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			-	
5	Force Authorized	Globally Disabled			-	
6	Force Authorized	Globally Disabled			-	
7	Force Authorized	Globally Disabled			-	

Figure 4-36: Network Access Server Switch Status

Table 4-32: Network Access Server Switch Status Parameters

Port	The switch port number. Click to navigate to detailed NAS statistics for this port. Refer to next section.
Admin State	The port's current administrative state. Refer to NAS **Admin State** for a description of possible values Network Access Server Configuration.
Port State	The current state of the port. Refer to NAS **Port State** for a description of the individual states. Network Access Server Configuration.
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 username (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 at previous section. System Configuration). If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs (previous section System Configuration).

4.5.2.6 NAS Port Statistics

This section 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.

Web GUI: Monitor > Security > Network > NAS > Port

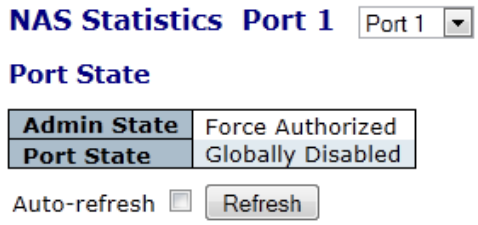


Figure 4-37: NAS Port Statistics

Table 4-33: NAS Port Parameters

Port State	
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	QoS Class assigned to the port 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 at previous section System Configuration. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs previous .System Configuration).
Port Counters	
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

EAPOL Counters			
Direction	Name	IEEE Name	Description
Rx	Total	dot1xAuthEapolFrames Rx	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	dot1xAuthEapLengthErrorFramesRx	The number of EAPOL 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

This backend (RADIUS) frame counters are available for the following administrative states:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based Auth

Backend Server Counters			
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 towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.

Last Supplicant/ Client Info

Last Supplicant/Client Info

Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states: (Refer to section 4.9.2.2 Port Configuration)

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based Auth

Last Supplicant/Client Info

Name	IEEE Name	Description
MAC Address	dot1xAuthLastEapolFrameSource	The MAC address of the last supplicant/client.
VLAN ID	-	The VLAN ID on which the last frame from the last supplicant/client was received.
Version	dot1xAuthLastEapolFrameVersion	**802.1X-based**: The protocol version number carried in the most recently received EAPOL frame. **MAC-based**: Not applicable.
Identity	-	**802.1X-based**: The username (supplicant identity) carried in the most recently received Response Identity EAPOL frame. **MAC-based**: Not applicable.

Selected Counters

The Selected Counters table is visible when the port is in one of the following administrative states:

- Multi 802.1X
- MAC-based Auth.

The table is identical to and is placed next to the above Port Counters table and will be empty if no MAC address is currently selected. To populate the table, select one of the **attached MAC Addresses** from the table below.

Attached MAC Addresses

Identity	Shows the identity of the supplicant, as received in the Response Identity EAPOL frame. Clicking the link causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it

	shows No supplicants attached. This column is not available for MAC-based Auth.
MAC Address	For Multi 802.1X, this column holds the MAC address of the attached supplicant. For MAC-based Auth., this column holds the MAC address of the attached client. Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows No clients attached.
VLAN ID	This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module
State	The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. If the backend server has not successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for **Hold Time** seconds.
Last Authentication	Shows the date and time of the last authentication of the client (successful as well as unsuccessful).
Buttons	The port select box determines which port is affected when clicking the buttons. **Clear**: This button is available in the following modes: • Force Authorized • Force Unauthorized • Port-based 802.1X • Single 802.1X **Clear All**: This button is available in the following modes: • Multi 802.1X • MAC-based Auth.X Click to clear the counters for the selected port. **Clear this**: This button is available in the following modes: • Multi 802.1X • MAC-based Auth.X

4.5.2.7 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.

Note: For a detailed explanation of ACL and ACE terms, refer to the Glossary of Terms at the end of this manual

Web GUI: Configuration > Security > Network > ACL > Ports

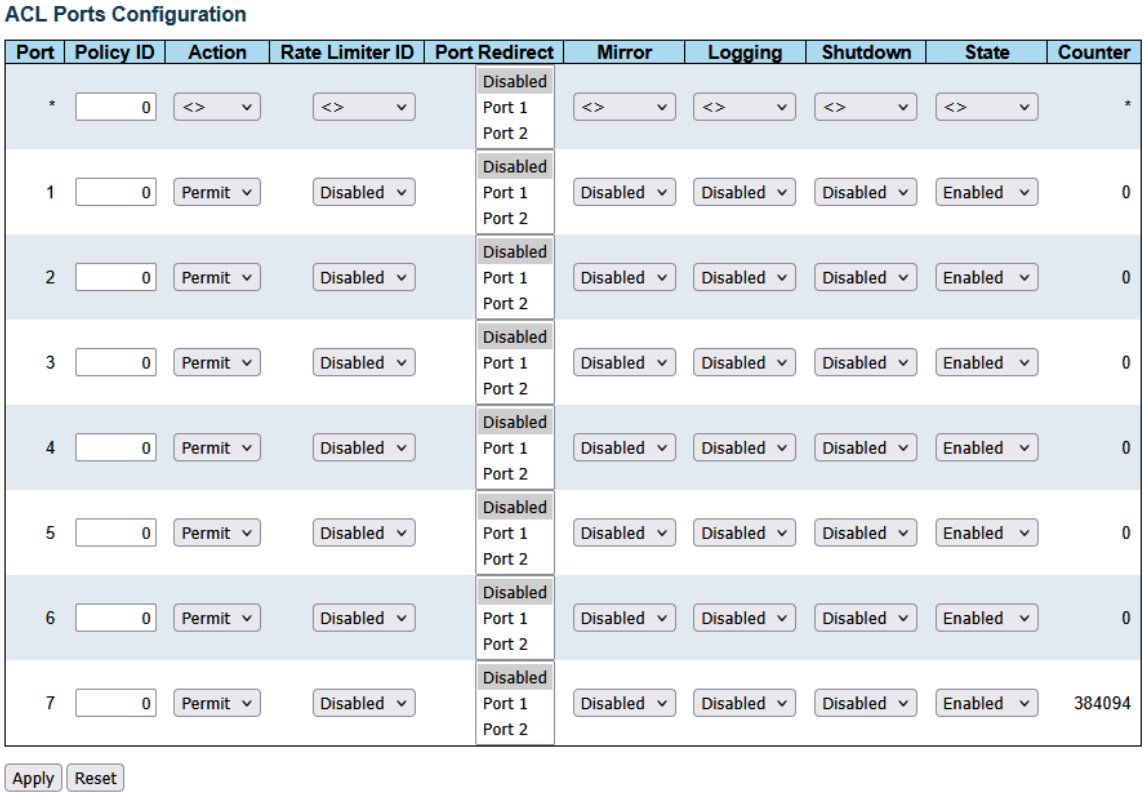


Figure 4-38: ACL Port Configuration

Table 4-34: ACL Port Configuration Parameters

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. 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 is 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**. *Note: The shutdown feature only works when the packet length is less than 1518(without VLAN tags).*
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.

4.5.2.8 Configuration

Configure the rate limiter for the ACL of the switch.

Web GUI: Monitor > Security > Network > ACL > Rate Limiters

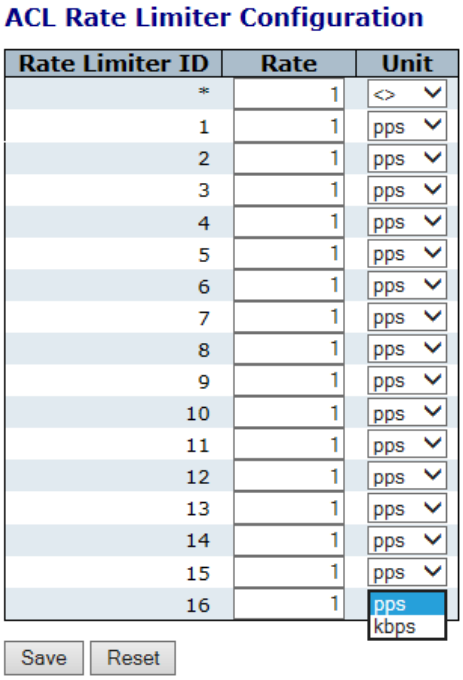


Figure 4-39: ACL Rate Limiter Configuration

Table 4-35: ACL Rate Limiter Parameters

Rate Limiter ID	The rate limiter ID for the settings contained in the same row. and its range is **1** to **16**.
Rate	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. • **LBPS**: Kbits per second.

4.5.2.9 Access Control List Configuration

This section 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 256 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.

Web GUI: Monitor > Security > Network > ACL > Access Control List

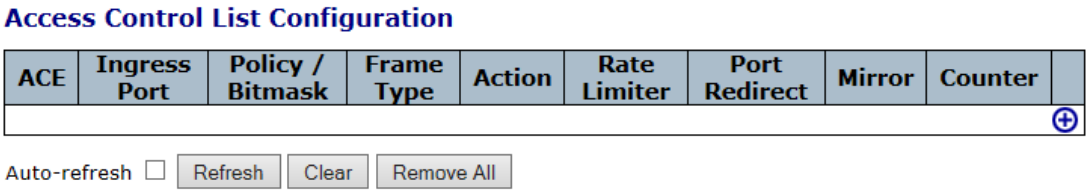


Figure 4-40: Access Control List Configuration

Table 4-36: ACL Configuration Parameters

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	Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are: • **Enabled**: Frames received on the port are mirrored. • **Disabled**: Frames received on the port are not mirrored. The default value is "Disabled.
Counter	The counter indicates the number of times the ACE was hit by a frame.
Modification Button	⊕: The lowest plus sign adds a new entry at the bottom of the ACE listings. By checking this box, you access additional displays (ACE configuration, VLAN Parameters).

Note: Refer to the Alphabetic Glossary of Terms for explanation of all underlined terms in the above section.

By clicking on the ⊕: The lowest plus sign adds a new entry at the bottom of the ACE listings. Refer to next page.

4.5.2.10 ACE Configuration

Configure an ACE (Access Control Entry) on this section. An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type selected.

A frame that hits this ACE matches the configuration that is defined here.

Web GUI: Configuration > Security > Network > ACL > Access Control List

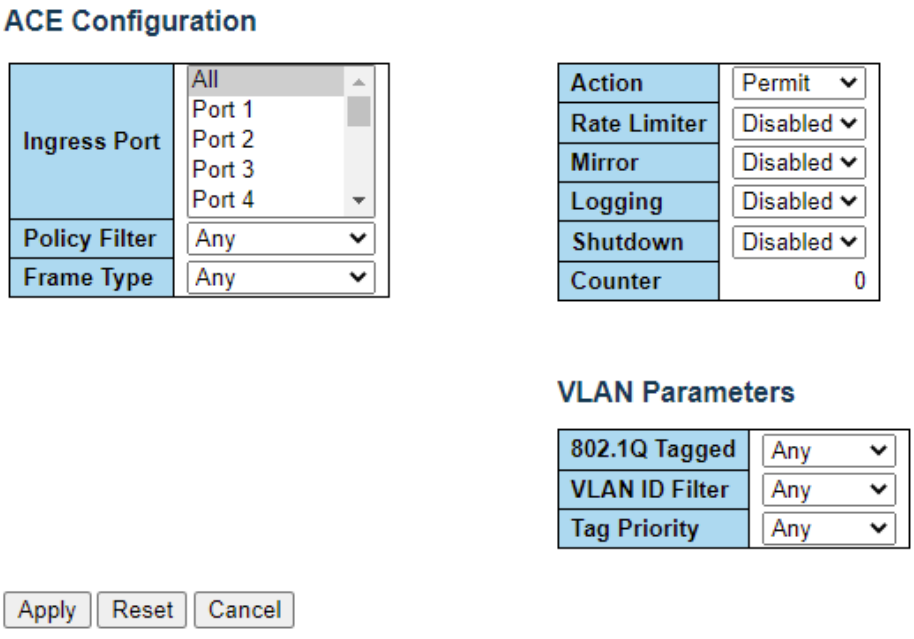


Figure 4-41: ACE Configuration displays

Table 4-37: ACL Configuration Parameters

ACE Configuration	
Second Lookup	Specify the second lookup operation of the ACE.
Ingress Port	Select the ingress port for which this ACE applies. • **All**: The ACE applies to all port. • **Port**: The ACE applies to this port number, where *n* is the number of the switch port.
Policy Filter	Specify the policy number filter for this ACE. • **Any**: No policy filter is specified. (Policy filter status is "don't-care".) • **Specific**: If you want to filter a specific policy with this ACE, choose this value. Two field for entering a policy value and bitmask appears.
Frame Type	Select the frame type for this ACE. These frames are mutually exclusive: • **Any**: Any frame can match this ACE. • **Ethernet Type**: Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal) and the value should not be equal to 0x800(IPv4), 0x806(ARP) or 0x86DD(IPv6). • **ARP**: Only ARP frames can match this ACE. Notice the ARP frames will not match the ACE with ethernet type. • **IPv4:** Only IPv4 frames can match this ACE. Notice the IPv4 frames will not match the ACE with ethernet type. • **IPv6:** Only IPv6 frames can match this ACE. Notice the IPv6 frames will not match the ACE with Ethernet type.
Action	Specify the action to take with a frame that hits this ACE. • **Permit**: The frame that hits this ACE is granted permission for the ACE operation. • **Deny**: The frame that hits this ACE is dropped. • **Filter**: Frames matching the ACE are filtered.
Rate Limiter	Select whether the rate limiter in number of base units. The allowed range is **1** to **16**. **Disabled** indicates that, the rate limiter operation is disabled
EVC Policer	Select whether EVC policer is enabled or disabled. The default value is **Disabled**. Note that the ACL rate limiter and EVC policer cannot both be enabled.

Mirror	Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The rate limiter will not affect frames on the 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".
Logging	Specify the logging operation of the ACE. Notice that the logging message does not include the 4 bytes CRC information. The allowed values are: • **Enabled**: Frames matching the ACE are stored in the System Log. • **Disabled**: Frames matching the ACE are not logged. *Note: The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited*
Shutdown	Specify the port shut down operation of the ACE. The allowed values are: • **Enabled**: If a frame matches the ACE, the ingress port will be disabled. • **Disabled**: Port shut down is disabled for the ACE. *Note: The shutdown feature only works when the packet length is less than 1518(without VLAN tags).*
Counter	The counter indicates the number of times the ACE was hit by a frame.
VLAN Parameters	
802.1Q Tagged	Specify whether frames can hit the action according to the 802.1Q tagged. The allowed values are: • **Any**: Any value is allowed ("don't-care"). • **Enabled**: Tagged frame only. • **Disabled**: Untagged frame only. The default value is "Any".

VLAN ID Filter	Specify the VLAN ID filter for this ACE. • **Any**: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".) • **Specific**: If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears.
Tag Priority	Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is **0** to **7** or range **0-1**, **2-3**, **4-5**, **6-7**, **0-3** and **4-7**. The value **Any** means that no tag priority is specified (tag priority is "don't-care".)

4.5.2.11 ACL Status

This section 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 256 on each switch.

Web GUI: Monitor > Security > Network > ACL Status

ACL Status combined Auto-refresh Refresh

User	ACE	Frame Type	Action	Rate Limiter	Mirror	CPU	Counter	Conflict
ptp	1	IPv4/UDP 319-320 DIP:192.168.3.94/32	Deny	Disabled	Disabled	Yes	0	No
ptp	2	IPv4/UDP 319-320 DIP:192.168.3.94/32	Deny	Disabled	Disabled	Yes	0	No
ptp	3	IPv4/UDP 319-320 DIP:192.168.3.94/32	Deny	Disabled	Disabled	Yes	0	No
ptp	4	IPv4/UDP 319-320 DIP:192.168.3.94/32	Deny	Disabled	Disabled	Yes	0	No
ptp	5	IPv4/UDP 319-320 DIP:192.168.3.94/32	Deny	Disabled	Disabled	Yes	0	No
ptp	6	IPv4/UDP 319-320 DIP:192.168.3.94/32	Deny	Disabled	Disabled	Yes	0	No
mep	3	EType	Filter	Disabled	Disabled	No	0	No
mep	1	EType	Deny	Disabled	Disabled	Yes	2503	No
mep	2	EType	Filter	Disabled	Disabled	No	12	No

Figure 4-42: ACL Status

Table 4-38: ACL Status Parameters

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**.** • **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.
Mirror	Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are: • **Enabled**: Frames received on the port are mirrored. • **Disabled**: Frames received on the port are not mirrored. The default value is "Disabled.
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	The select box determines which ACL user is affected by clicking the buttons. Combined combined static ipManagement ipSourceGuard ipmc evc mep arpInspection upnp ptp dhcp loopProtect ttLoop y1564 linkOam ztp conflict

4.5.2.12 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 section provides the related IP Source Guard configurations.

Web GUI: Configuration > Security > Network > IP Source Guard/Configuration

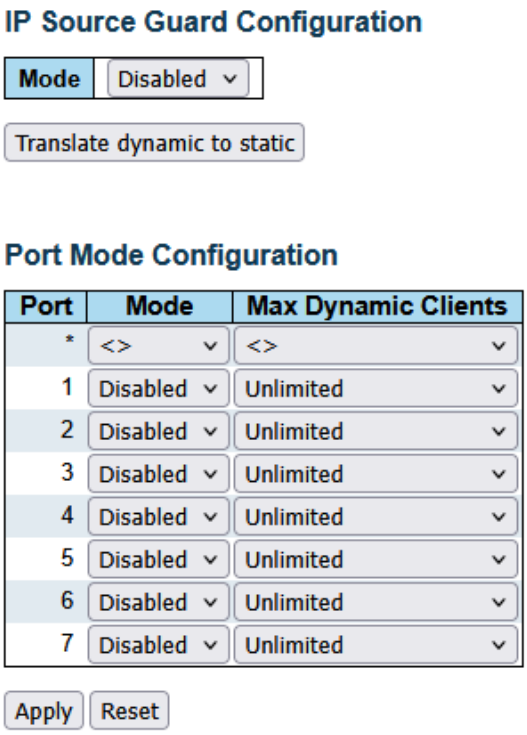


Figure 4-43: IP Source Guard Configuration

Table 4-39: IP Source Guard Configuration Parameters

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 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, 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.

4.5.2.13 Static IP Source Guard Table

Web GUI: Configuration > Security > Network > IP Source Guard > Static Table

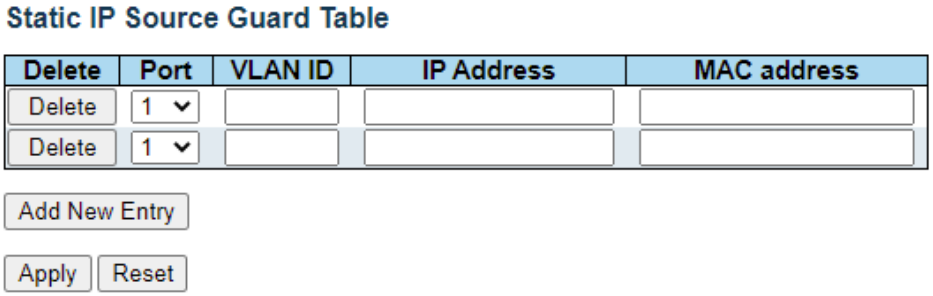


Figure 4-44: Static IP Source Guard Table

Table 4-40: IP Source Guard Table Parameters

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	**Add New Entry:** Click to add a new entry to the Static IP Source Guard table.

4.5.2.14 IPv6 Source Guard Configuration

IPv6 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 section provides the related IPv6 Source Guard configurations.

Web GUI: Configuration > Security > Network > IPv6 Source Guard > Configuration

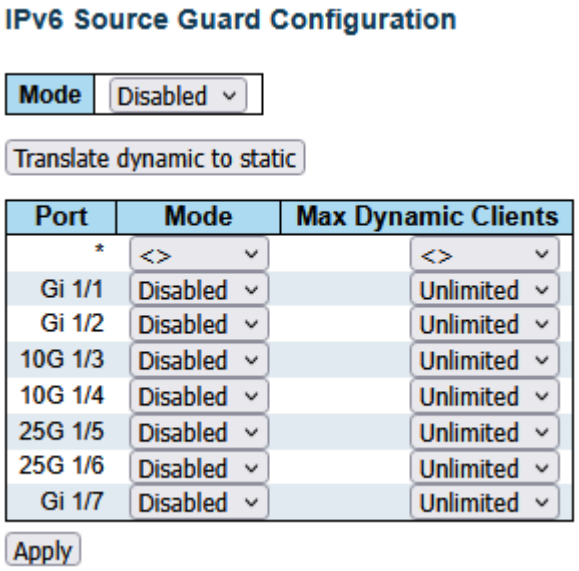


Figure 4-45: IPv6 Source Guard Configuration

Table 4-41: IPv6 Source Guard Configuration Parameters

Mode of IPv6 Source Guard Configuration	Enable or disable the Global IPv6 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 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, 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.

4.5.2.15 Static IPv6 Source Guard Table

Web GUI: Configuration > Security > Network > IP Source Guard/Static Table

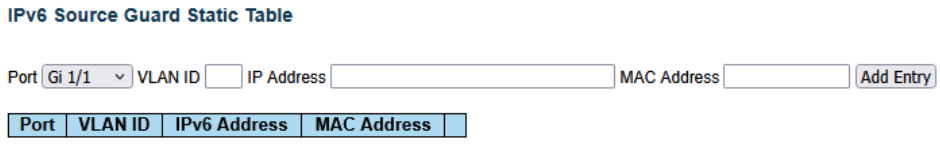


Figure 4-46: Static IP Source Guard Table

Table 4-42: IP Source Guard Table Parameters

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	**Add New Entry:** Click to add a new entry to the Static IP Source Guard table.

4.5.2.16 Dynamic IP Source Guard Table

Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address.

Each page shows up to 99 entries from the Dynamic IP Source Guard 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 IP Source Guard Table.

The "Start from port address", "VLAN" and "IP address" input fields allow the user to select the starting point in the Dynamic IP Source Guard Table.

Clicking the **Refresh** button will update the displayed table starting from that or the closest next Dynamic IP Source Guard 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 table 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.

Web GUI: Monitor > Security > Network > IP Source Guard

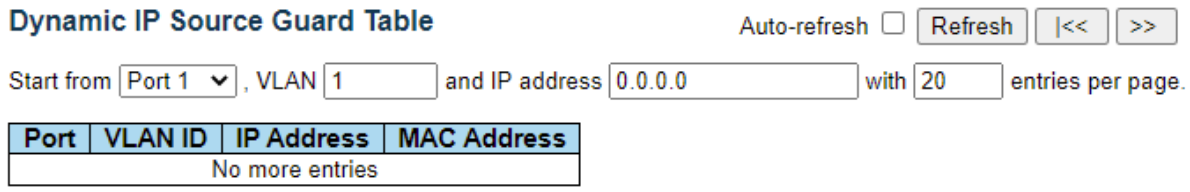


Figure 4-47: Dynamic IP Source Guard Table

Table 4-43: Dynamic IP Source Guard Table Parameters

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	**<<:** 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.

4.5.2.17 Dynamic IPv6 Source Guard Table

Entries in the Dynamic IPv6 Source Guard Table are shown on this page. The Dynamic IPv6 Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address.

Each page shows up to 99 entries from the Dynamic IPv6 Source Guard 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 IP Source Guard Table.

Clicking the **Refresh** button will update the displayed table starting from that or the closest next Dynamic IPv6 Source Guard Table match.

Web GUI: Monitor > Security > Network > IPv6 Source Guard

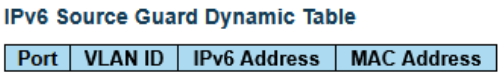


Figure 4-48: Dynamic IP Source Guard Table

Table 4-44: Dynamic IP Source Guard Table Parameters

Port	Switch Port Number for which the entries are displayed.
VLAN ID	VLAN-ID in which the IP traffic is permitted.
IPv6 Address	User IP address of the entry.
MAC address	Source MAC address.

4.5.3 Address Resolution Protocol

Address Resolution Protocol (ARP) 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.

The ARP subject is covered by the following displays:

- ARP Inspection Configuration
- Port Mode Configuration
- VLAN Mode Configuration
- Static ARP Inspection Table
- Dynamic ARP Inspection Table

4.5.3.1 ARP Inspection Configuration

This section provides ARP Inspection related configuration.

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.

Web GUI: Configuration > Security > ARP Inspection > Port Configuration

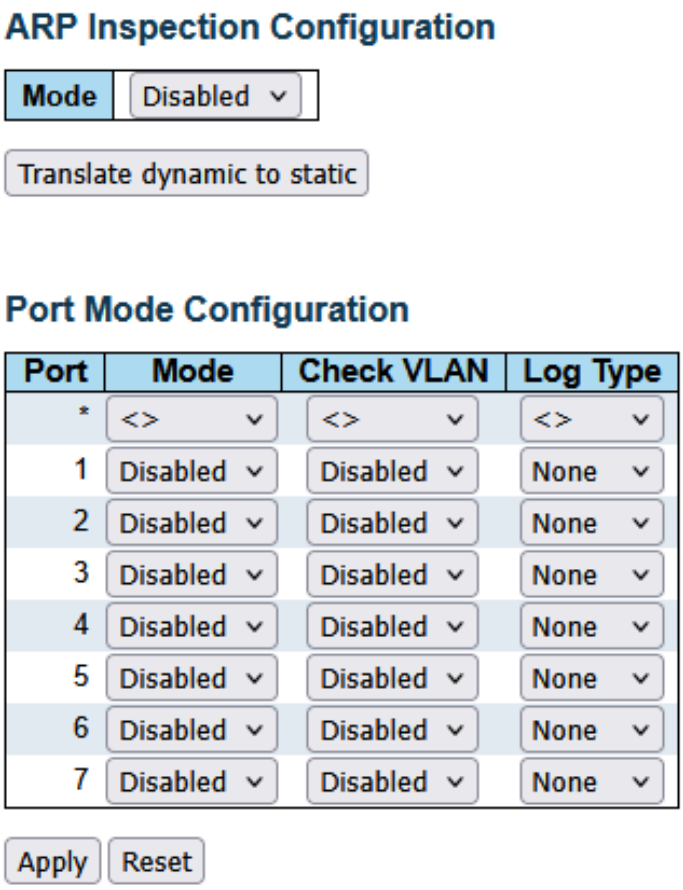


Figure 4-49: ARP Configurations displays

Table 4-45: ARP Configuration displays Parameters

ARP Inspection Configuration	
Mode of ARP Inspection Configuration	Enable the Global ARP Inspection or disable the Global ARP Inspection

Port Mode Configuration	
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 must 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 if 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 if 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 Type 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.

4.5.3.2 VLAN Configuration

This section provides information about enabling ARP on VLANs.

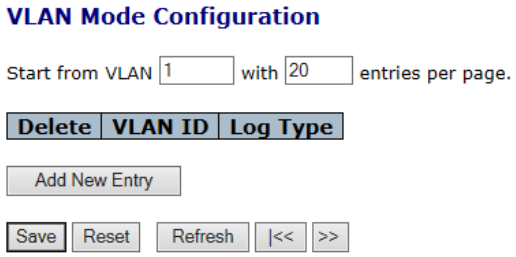


Figure 4-50: VLAN Mode Configurations display

Table 4-46: VLAN Mode Configuration Parameters

VLAN Mode Configuration	
Specify ARP Inspection is enabled on which VLANs. First, you must 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.
Navigating the VLAN 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 **Refresh** the 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.	

4.5.3.3 Static ARP Inspection Table

This page shows the static ARP Inspection rules. The maximum number of rules is **256** on the switch.

Web GUI: Monitor > Security > Network > ARP Inspection > Static Table

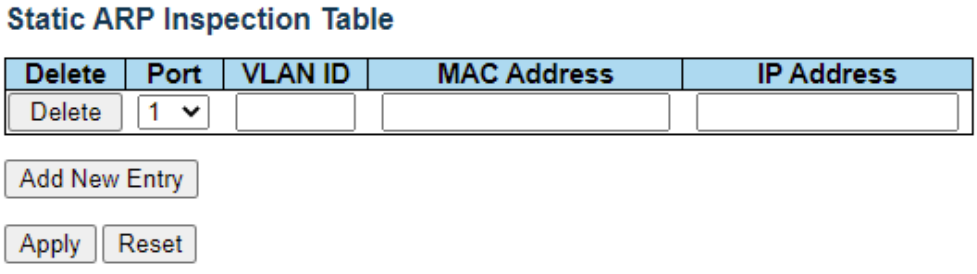


Figure 4-51: Static ARP Inspection Table display

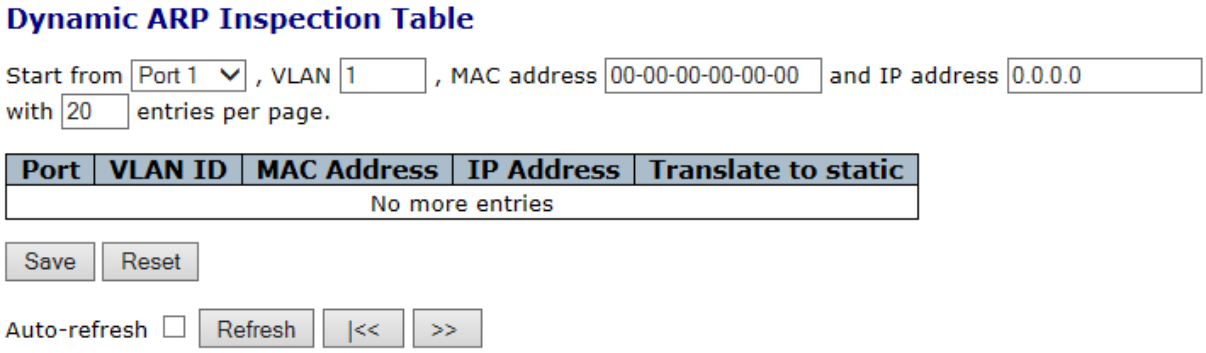
Table 4-47: Static ARP Inspection Table parameters

Static ARP Inspection Table	
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	**Add New Entry**: Click to add a new entry to the Static ARP Inspection table.

4.5.3.4 Dynamic ARP Inspection Table

Web GUI: Monitor > Security > Network > ARP Inspection > Dynamic Table



Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 256 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address. All dynamic entries are learning from DHCP Snooping.

Figure 4-52: Dynamic ARP Inspection Table display

Table 4-48: Dynamic ARP Inspection Table parameters

Dynamic ARP Inspection Table	
Port	Switch Port Number for which the entries are displayed
VLAN ID	VLAN-ID in which the ARP traffic is permitted.
MAC Address	User MAC address of the entry
IP Address	User IP address of the entry.
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 table 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.

4.5.4 Authentication Server Configuration (AAA)

This section allows the configuration of Authentication Servers.

4.5.4.1 Radius Server Configuration

This section allows you to configure the RADIUS servers.

Web GUI: Security > AAA > Radius

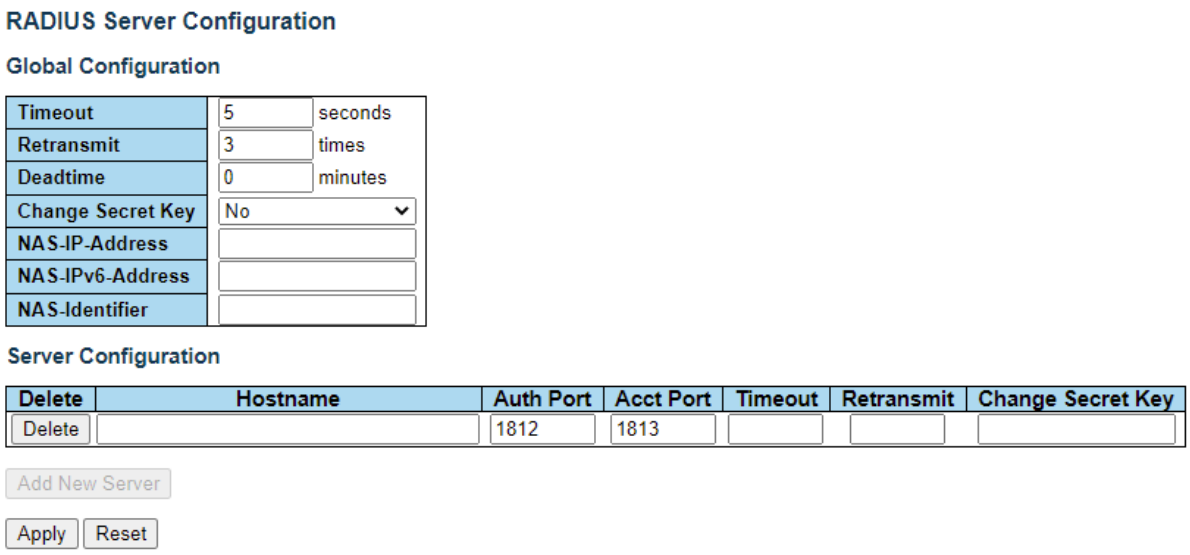


Figure 4-53: Radius: Server Configuration

Table 4-49: Radius: Server Configuration Parameters

Global Configuration	
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 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 dead.
Deadtime	Deadtime, 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 Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured
Change Secret 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 RADIUS server and the switch.
NAS IP Address (Attribute 4)	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 (Attribute 95)	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 (Attribute32)	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 IP address of the outgoing interface is used.
Server Configuration	
The table has one row for each RADIUS Server and several columns listed below.	
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. Set to 0 to disable authentication.
Acct Port	The UDP port to use on the RADIUS server for accounting. Set to 0 to disable 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.
Change Secret Key	Specify to change the secret key or not. When the checkbox is checked, you can change the setting overrides the global key. Leaving it blank will use the global key.
Adding a New Server	
Click **Add New Server** 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. The **Delete** button can be used to undo the addition of the new server.	

4.5.4.2 Radius Server Status Overview

This page provides an overview of the status of the RADIUS servers configurable on the Global and Server configurations

Web GUI: Monitor > Security > AAA > RADIUS Overview

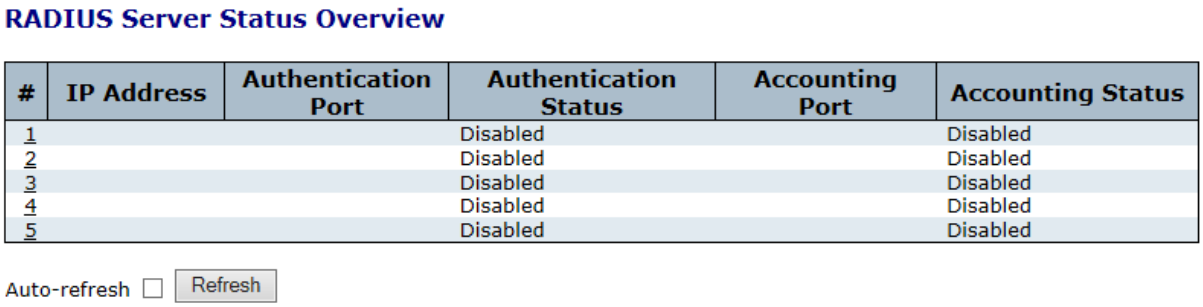


Figure 4-54: RADIUS: Server Status Overview

Table 4-50: RADIUS: Server Status Overview parameters

RADIUS Servers	
#The RADIUS server number. Click to navigate to detailed statistics for this server.	
IP Address	The IP address of the 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 for accounting
Accounting Status	The 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.

4.5.4.3 RADIUS Auth. Statistics for Server

This section provides detailed statistics for a particular RADIUS server.

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.

Web GUI: Monitor > Security > AAA > Radius Overview

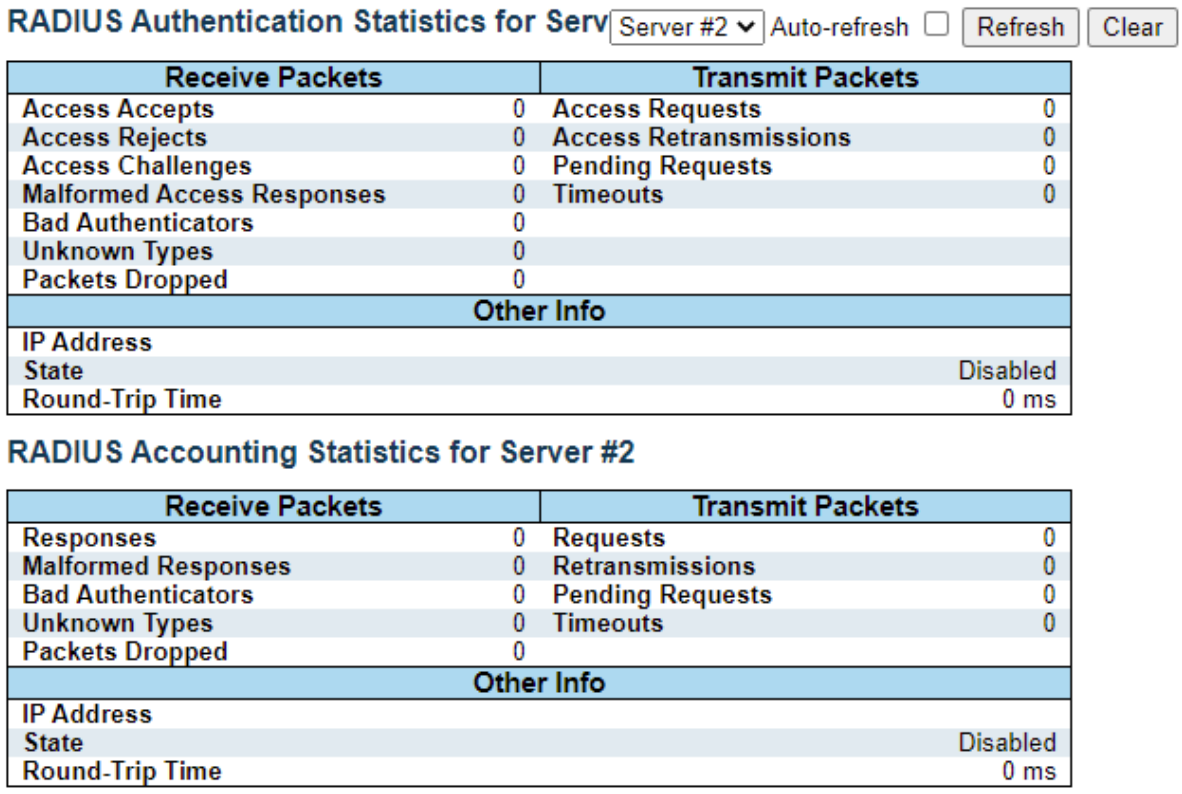


Figure 4-55: RADIUS Statistics for Server

Table 4-51: RADIUS Statistics for Server Parameters

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.	
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	radiusAuthClientExtMalformed AccessResponses	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 with unknown types from the server on the authentication port and dropped.
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	radiusAuthClientExtAccess Retransmissions	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	Rad+iusAuthClientExtRoundTripTime	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 has not 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.	
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	radiusAccClientExtRetransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.
Tx	Pending Requests	radiusAccClientExtPendingRequests	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	radiusAccClientExtTimeouts	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 has not been round-trip communication with the server yet.

4.5.4.4 TACACS+ Sever Configuration

This page allows you to configure the TACACS+ servers.

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.

Web GUI: Monitor > Security > AAA > TACACA+

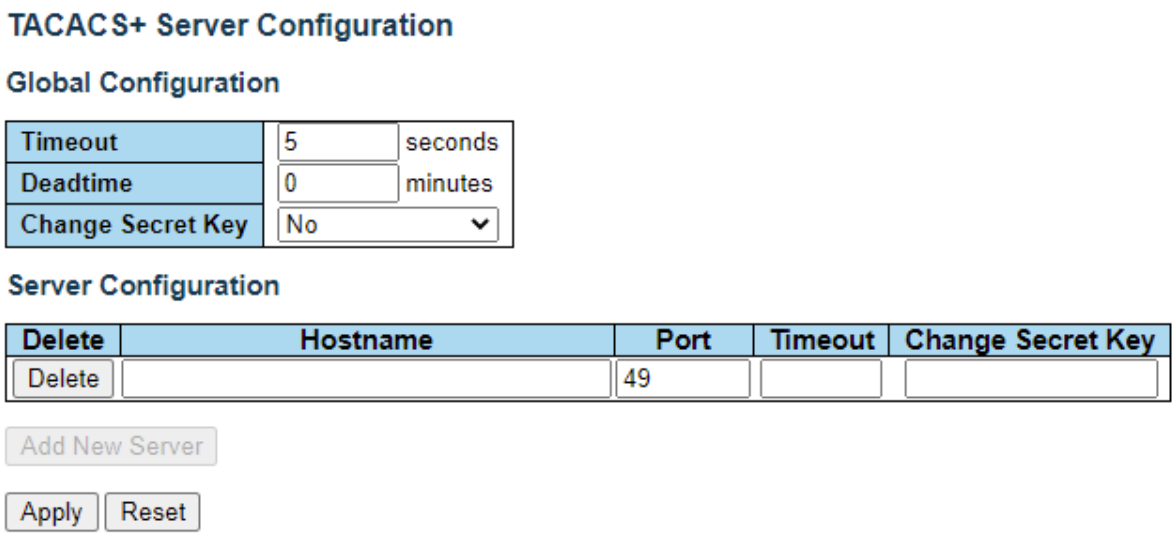


Figure 4-56: TACACS+ Server Configuration

Table 4-52: TACACS+ Server Configuration Parameters

Global Configuration	
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 dead.
Deadtime	Deadtime, 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 Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured
Change Secret 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 several columns listed below.	
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 UDP 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.
Change Secret Key	Specify to change the secret key or not. When the checkbox is checked, you can change the setting overrides the global key. Leaving it blank will use the global key.

Adding a New Server
Click **Add New Server** 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. The **Delete** button can be used to undo the addition of the new server

4.6 Clock Central Configuration

4.6.1 Overview

Clock Central visualizes the system's clocks and timing flows, allowing the high-level configuration and monitoring of inputs, outputs and behavior.

Each one of the different inputs and outputs (e.g. PTP, SyncE) is configured and monitored in their own respective detailed pages, but the overall control and relationship between them is handled by Clock Central.

Clock Central allows both General and Hybrid modes. In General mode all clocking domains (frequency, phase and ToD) are control by the same input(s) (e.g. GNSS), while the Hybrid mode allows each domain to operate independently of the others (e.g. as a BC, with both PTP and SyncE).

4.6.2 Mode Configuration

This section enables the configuration of the device's clocking system, with sync reference sources, outputs and overall state.

The possible clock reference inputs (sync source) to the Clock Central are: SyncE, PTP, NTP, GNSS, ToD, TDM and External (1PPS and 10MHz). The Clock Central will output the required sync clock according to reference quality and priority.

Web GUI: Configuration > Timing > Clock Central

Figure 4-57: Mode selection

When Clock Central mode is set to Hybrid, the split clocking domain option appears.

4.6.3 Sync Source Configuration

Sync Source						
ID	Ena	Type	Port	Status	Quality	
					Current	Qualified

Figure 4-58: Sync Source display

Up to 5 different Sync sources can be configured, including SyncE, PTP, NTP, GNSS, ToD, TDM and External. Source priority can be set according to ID (default) of quality level.

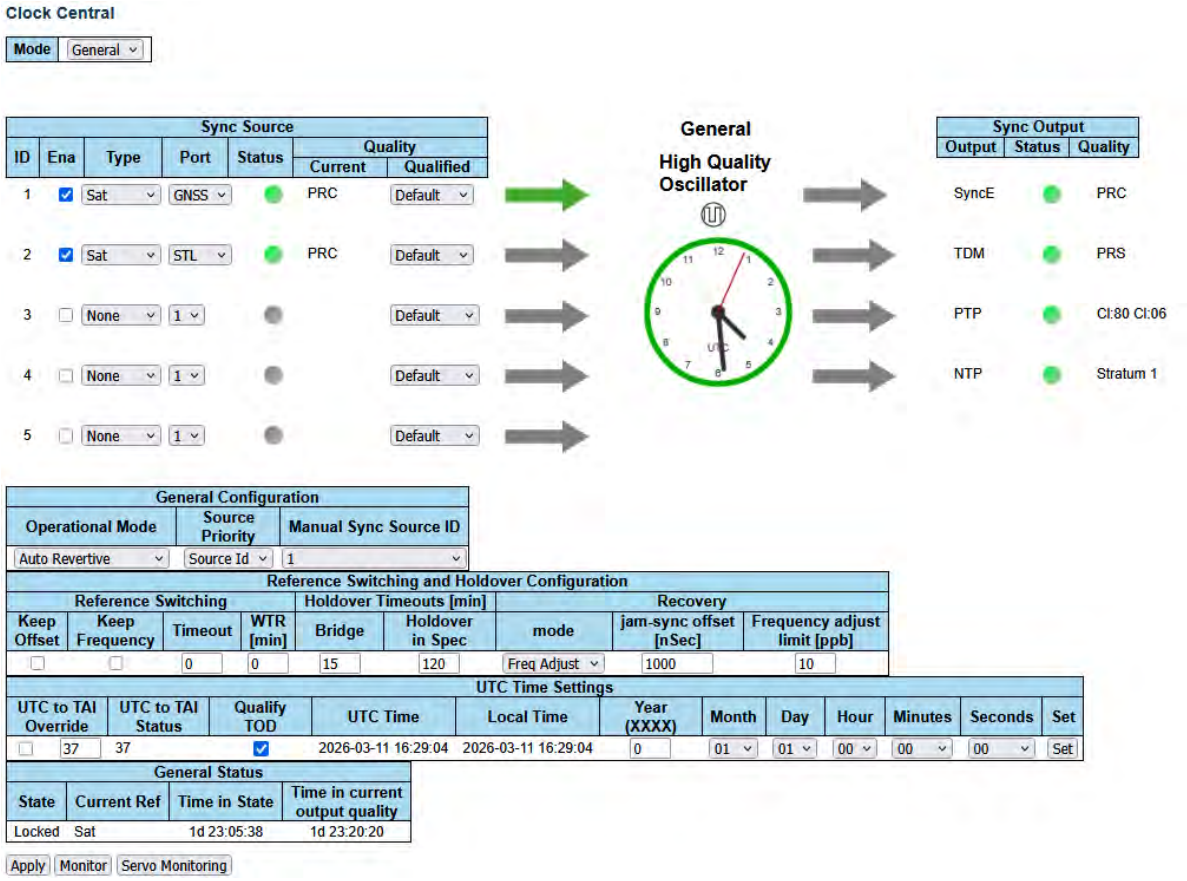


Figure 4-59: Clock Central configuration page

Table 4-53: Clock Central parameters

Sync Source	
ID	Indicates the sync source identification number.
Ena	Enable or disable the sync source.
Type	Select the type of sync source. Available options depend on model and may include: SyncE, PTP, GNSS, TDM and External.
Port	Select the port or instance of the selected sync source type. For example: for SyncE this will be Ethernet port numbers, for PTP the clock instance number, etc.

State	The status of the sync source. This indicator displays the following states: • **Green** - The source provides a valid reference clock. • **Red** – indicates failure of the source. • **Orange** – Source quality is unqualified • **Grey** - When a source is disabled or not applicable, indicator will be. The indicator is also a hyperlink to the detailed source's page.
Quality (Current)	Indicates the sync source's current (clock) quality (QL) as received from the source (e.g., via SSM). When there is no quality indication received from the source, a default quality value is shown with parentheses.
Quality (Qualified)	select the threshold quality, for which the source will be qualified as valid.

4.6.4 Clock Central Visual Indicators

Table 4-54: Clock Central parameters

Input arrows	Visualization of sources feeding the system. A **green** arrow indicates the source is currently selected.
General High Quality Oscillator	Provides a visual indication of the current oscillator status: • **Green** - system is locked to a sync source. • **Blue** - indicates the system is in Holdover state. • **Yellow** - indicates Free running (internal clock) state. • **Green/Yellow** (blinking) - Lock Acquisition. • **Blue/Green** (blinking) - Holdover Recovery.
Output arrows	Visualization of outputs (distributed from the system clock).

4.6.5 Sync Output

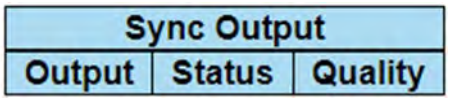


Figure 4-60: Sync Output

Table 4-55: Sync Output parameters

Sync Output	
Output	Indicates the type of output (e.g., SyncE, PTP, BITS, etc.).
Status	Indicates the clock output is active
Quality	Indicates the clock quality distributed on this type of output.

4.6.6 General Configuration

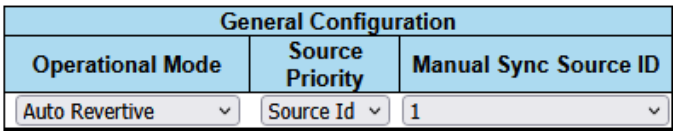


Figure 4-61: Clock Central General Configuration

Table 4-56: General configuration parameters

General Configuration	
Operational Mode	Allow selection of the required system's synchronization mode Available modes are: • **Manual:** source will the one configured in the manual source configuration fields, regardless of its state. • **Auto Revertive (default mode).:** clock source is automatically selected based on priority and state. When higher priority source that previously failed, is valid again, switchover will take place. This is the default mode and the most commonly used one. • **Auto Non-Revertive:** clock source is automatically selected based on priority and state. When higher priority source that previously failed, is valid again, no switchover will take place. • **Forced HoldOver:** the system will be synchronized to the last selected source but will go into holdover mode and ignore this source. • **Forced Free running:** the system will be synchronized to the local clock, ignoring all sync sources.
Priority Select Mode	The source will be selected based on its ID (the lower it is the higher its priority) or based on its Quality.
Manual Sync Source ID	Manually configure the sync source. Applicable only in Manual mode.

4.6.7 Reference Switching and Holdover Configuration

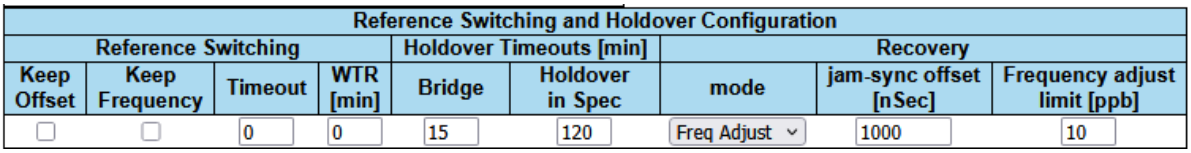


Figure 4-62: Holdover Configuration

Table 4-57: Holdover Configuration parameters

Reference Switching	
Keep Offset	Specify if the offset should be kept.
Keep Frequency	Specify if the Frequency should be kept.

Timeout	Set the Clock Central holdover duration in minutes
WTR [min]	Specifies the WTR time in minutes
Holdover Timeouts [min]	
Bridge	Specify the Bridge time in minutes
Holdover in Spec	Specify the Holdover in Spec time in minutes
Recovery	
Mode	Three options available: • Fast Locked • Keep Offset • Freq adjust
Jam-sync offset [nSec]	Default setting is 0
Frequency adjust limit	Default setting is 100 ppb

4.6.8 UTC Time Settings

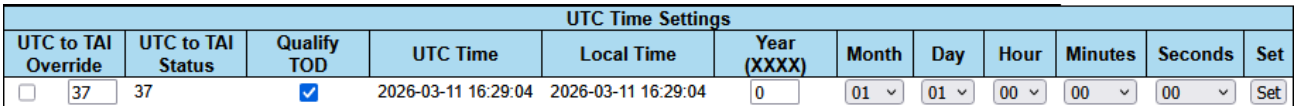


Figure 4-63: UTC Time Settings

Table 4-58: UTC Time Settings parameters

UTC to TAI Override	Override UTC with TAI. Specify the value in seconds of the difference between UTC and TAI
UTC to TAI Status	Displays the current TAI offset.
Qualify TOD	Qualify the Time of Day.
UTC Time	Specifies the current UTC time.
Local Time	Specifies the current local time.
Year (XXXX)	Specifies the current year.
Month	Specifies the current month.
Day	Specifies the current day.
Hours	Specifies the current hour of the day.
Minutes	Specifies the current minutes.
Seconds	Specifies the current seconds.
Set	Sets the time based on the configurations.

4.6.9 Clock Central General Status

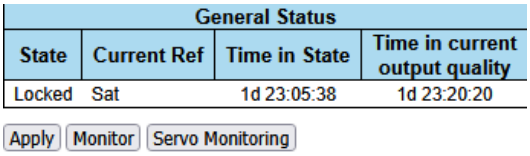


Figure 4-64: Clock Central General Status

Table 4-59: Clock Central General Status parameters

State	Shows the current Clock Central state, which includes: • Free Run: indicates Free running (internal clock) state. • Lock Acquisition: indicates the system locking on selected reference. • Locked: indicates the system locked to selected reference. • Holdover: reference was lost, system is maintaining clocked output • Holdover Recovery: reference rediscovered, system resyncs.
Current Ref	Indicates the sync source (type and port/instance) the system is currently locked to (e.g., PTP, GPS, etc.).
Time in State	The time that has passed since the last system sync state change.
Time in current output quality	The time that has passed since the last output QL change.
Buttons	Monitor Direct link to the Clock Central monitoring page. Other Buttons: Direct link to relevant pages.

4.7 Clock Central Monitoring

This page allows you to monitor and view the status of the Clock Central. The page automatically update in order to display the actual status.

Web GUI: Monitor > Timing > Clock Central > Status

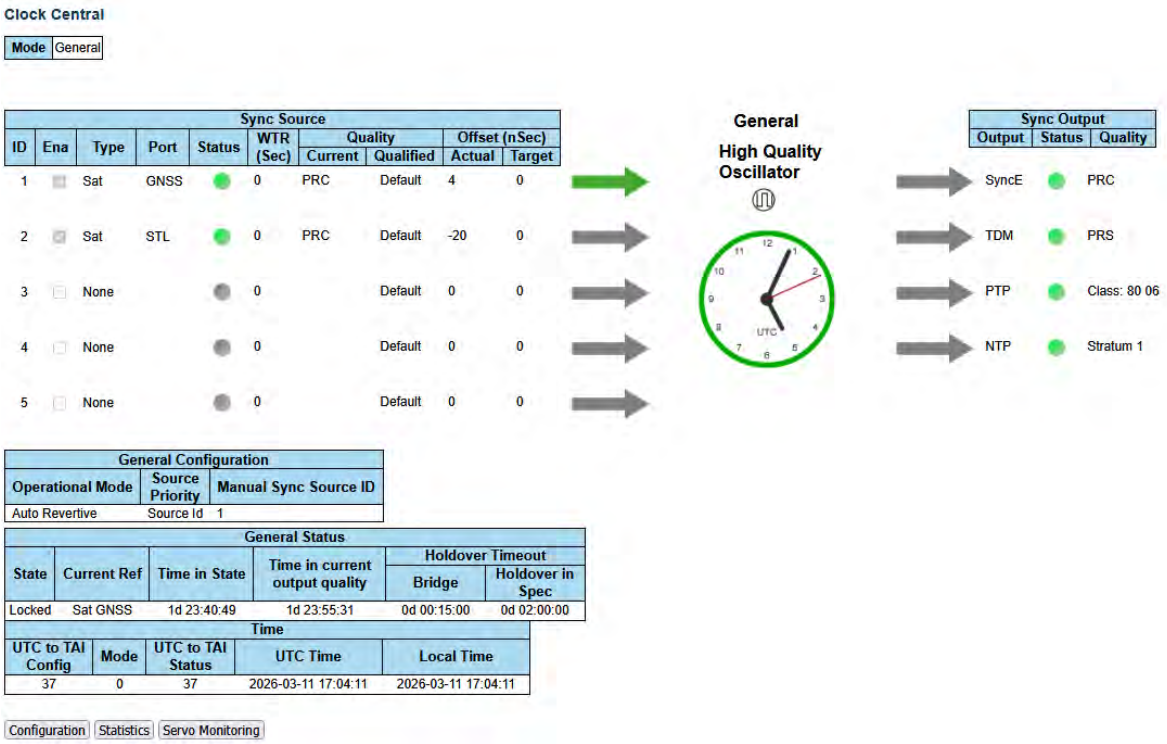


Figure 4-65: Monitoring Clock Central Status displays

The following displays allow us to monitor the Clock Central status and activity.

4.7.1 Sync Sources and Visual Indicators

For details refer to Table 4-53 and Table 4-54

4.7.2 Clock Central Source Status

The status table displays the current state of the system in reference to the selected Timing source.

Figure 4-66: General Status

General Status					
State	Current Ref	Time in State	Time in current output quality	Holdover Timeout	
				Bridge	Holdover in Spec
Locked	Sat GNSS	2d 00:00:35	2d 00:15:17	0d 00:15:00	0d 02:00:00

Table 4-60: General Status parameters

State	Shows the current system's overall synchronization state (e.g., Locked). The state is also evident in the color of the Clock Central main block diagram as described in Table 4-54 and Table 4-59
Current Ref	Indicates the sync source the system is currently locked to (e.g., Sat GNSS).
Time in State	The time that has passed since the last system sync state change.
Time in current output quality	The time that has passed since the last output QL change.
Holdover Timeout	Indicates the current Bridge and Holdover in Spec holdover timeouts.

4.7.3 Time

Time	
UTC to TAI Status	UTC Time
37	2021-04-09T13:07:44+00:00

UTC to TAI Status	Displays the configured difference between UTC and TAI, in seconds
Mode	Displays the current mode.
UTC to TAI Status	Displays the current difference between UTC and TAI, in seconds
UTC Time	Displays the current UTC time
Local Time	Displays the current local time

4.7.4 Sync Output

Sync Output		
Output	Status	Quality

Figure 4-67: Sync Output Status

Table 4-61: Sync Output parameters

Sync Output	
Output	Indicates the type of output (e.g., SyncE, PTP or TDM).
Status	Indicates the clock output which is used to synchronize the functional block in 'Output'.
Quality	Indicates the clock quality distributed on this type of output.
Buttons	**Configuration:** Direct link to the Clock Central configuration page. **Statistics:** Direct link to the Clock Central Statistics page

4.8 GNSS Module

This section displays the configuration and status info of the GNSS module.

Web GUI: Configuration > Timing > GNSS

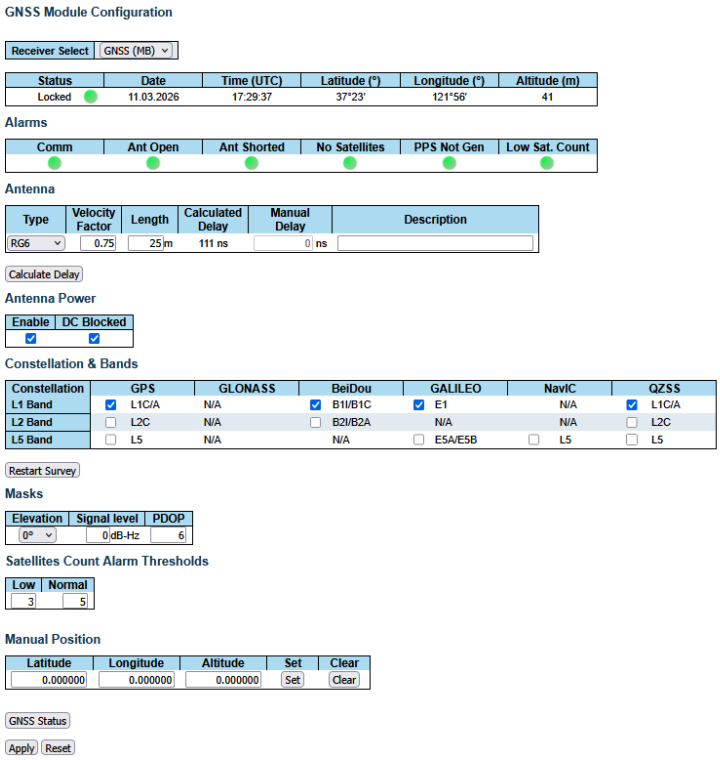


Figure 4-68: GNSS Module Configuration

4.8.1 Receiver

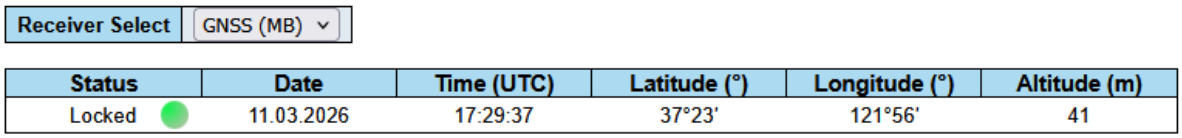


Figure 4-69: Receiver

Table 4-62: Receiver parameters

Receiver Select	Set the type of cable being used for the receiver type. The options are: • GNSS (MB) • STL (STL receiver) • GEOL (GEOL receiver)
Status	
Status	Displays the current GNSS Module status
Date	Displays the current date
Time (UTC)	Displays the current UTC time

Latitude (O)	Displays the current latitude, as received, in degrees
Longitude (O)	Displays the current longitude, as received, in degrees
Altitude (m)	Displays the current altitude, as received, in meters.

4.8.2 Alarms

The alarms parameters depend on the receiver type configured by the Receiver Select parameter.

4.8.2.1 GNSS Module

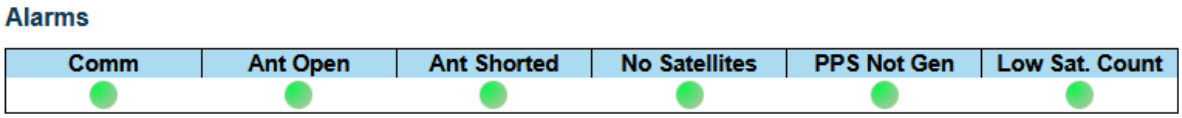


Figure 4-70: Alarms – GNSS Module

Table 4-63: Receiver Alarm parameters – GNSS Module

Comm	Display status of communication with the receiver
Ant Open	Signals the antenna is detected (green) by the receiver or not (red)
Ant Shorted	Signals a short circuit is detected (red) by the receiver or not (green)
No Satellites	When it lights red the receiver can see no satellites.
PPS Not Gen	When it lights red the receiver cannot generate 1PPS signal.
Low Sat. Count	When it lights red the receiver has a low satellite count

4.8.2.2 GEOL Module alarms

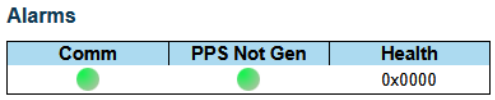


Figure 4-71: Alarms – STL Module

Table 4-64: Receiver Alarm parameters – GNSS Module

Comm	Display status of communication with the receiver
PPS Not Gen	When it lights red the receiver cannot generate 1PPS signal.
Health	Displays the health of the receiver

4.8.2.3 STL Module alarms

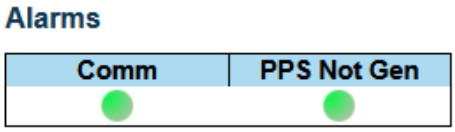


Figure 4-72: Alarms – STL Module

Table 4-65: Receiver Alarm parameters – GNSS Module

Comm	Display status of communication with the receiver
PPS Not Gen	When it lights red the receiver cannot generate 1PPS signal.

4.8.3 Satellite Selection (GEOL receiver)

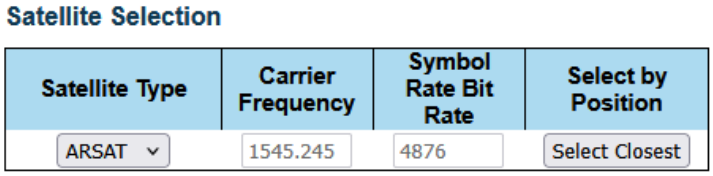


Figure 4-73: Satellite Selection

Table 4-66: Satellite Selection parameters

Satellite Type	Select the satellite type. The options are: • Manual • ARSAT • SASAT • ERSAT • EASAT • IRSAT • OCSAT
Carrier Frequency	Specify the carrier frequency of the satellite
Symbol Rate Bit Rate	Specify the bit rate for the Symbol Rate
Select by Position	Click the button to select the closest satellite.

4.8.4 Subscription Key (STL receiver)

Figure 4-74: Satellite Selection

Table 4-67: Satellite Selection parameters

Key	Enter the subscription key provided by the satellite subscription provider.
Update Key	Update the subscription key on the receiver

4.8.5 Antenna

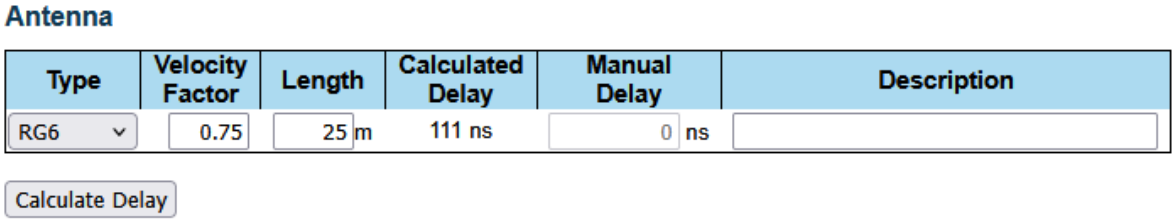


Figure 4-75: Antenna

Table 4-68: Antenna Configuration parameters

Type	Set the type of cable being used for the antenna. When Manual is selected, it is possible to directly configure the cable delay.
Velocity Factor	Set the Velocity Factor (VF) of the antenna cable.
Length	Set the length of the antenna cable in meters.
Calculated Delay	Indicates the cable delay in nsec as calculated based on VF and length.
Manual Delay	Set the cable delay in nsec manually (applicable when Type is **Manual**).
Description	Set a free text description of the cable (up to 63 characters).
Buttons	**Calculate Delay:** Click to calculate the cable delay based on current parameters.

4.8.6 Antenna Power

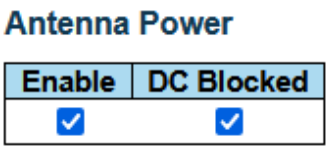


Figure 4-76: Antenna Power

Table 4-69: Antenna Power parameters

Enable	Enable antenna power
DC Blocked	Specify if DC is blocked

4.8.1 Manual Position (GNSS)

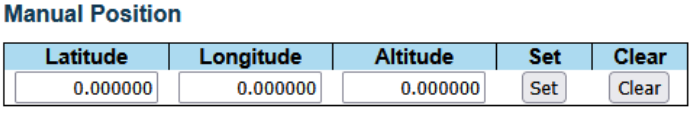


Figure 4-77: Manual Position

Table 4-70: Manual Position parameters

Latitude	Specify the latitude
Longitude	Specify the longitude
Altitude	Specify the altitude
Set	Set the configured latitude, longitude, and altitude
Clear	Clear all values

4.8.1 Manual Position (STL receiver)

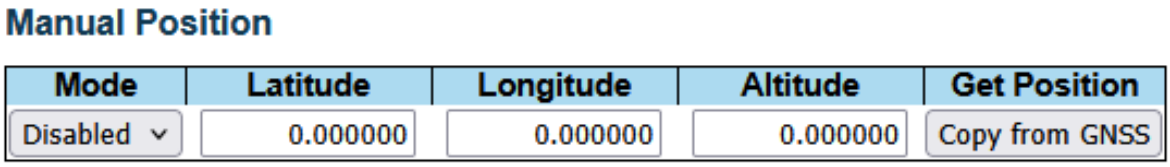


Figure 4-78: Manual Position

Table 4-71: Manual Position parameters

Mode	Specify the manual position mode. The options are: • Disabled – Manual positioning is disabled • Fixed – Position is fixed to the coordinates provided • Guess – Position is estimated based on coordinates provided
Latitude	Specifies the latitude of the receiver
Longitude	Specifies the longitude of the receiver
Altitude	Specifies the altitude of the receiver
Get Position	Click this button to obtain the latitude, longitude, and altitude from the GNSS module.

4.8.2 Manual Position (GEOL receiver)

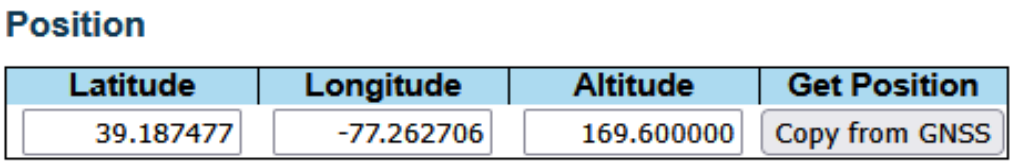


Figure 4-79: Position

Table 4-72: Manual Position parameters

Latitude	Specifies the latitude of the receiver
Longitude	Specifies the longitude of the receiver
Altitude	Specifies the altitude of the receiver

Get Position	Click this button to obtain the latitude, longitude, and altitude from the GNSS module.

4.8.3 Constellation & Bands

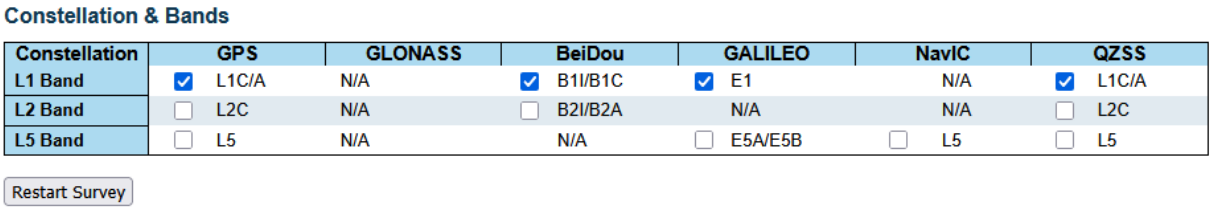


Figure 4-80 Constellation & Bands

Table 4-73: GNSS Constellation L1 Band Configuration Options

Band	Constellation
L1 band	GPS – L1C/A, GLONASS – G1, BEIDOU – (B1I, B1C), GALILEO – E1, QZSS – L1C/A
L2 band	GPS – L2C, GLONASS – G2, BEIDOU – B2i, GALILEO – E5a, NavIC – N/A QZSS – L2C
L5 band	GPS – L5, BEIDOU – B2a, GALILEO – E5a, NavIC – L5, QZSS – L5

4.8.4 Masks

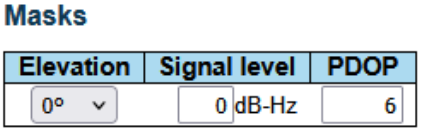


Figure 4-81 Masks

Table 4-74: Mask Configuration Options

Elevation	Specify the elevation
Signal Level	Specify the signal level in dB-Hz
PDOP	Specify the Position Dilution of Precision (PDOP)

4.8.5 Satellites Count Alarm Thresholds

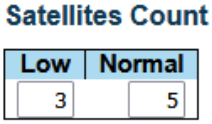


Figure 4-82 Satellites Count Alarm Thresholds

Table 4-75: Satellites Count Alarm Thresholds Options

Low	Specify the low satellite count alarm threshold
Normal	Specify the normal satellite count

4.8.1 GNSS Module Status

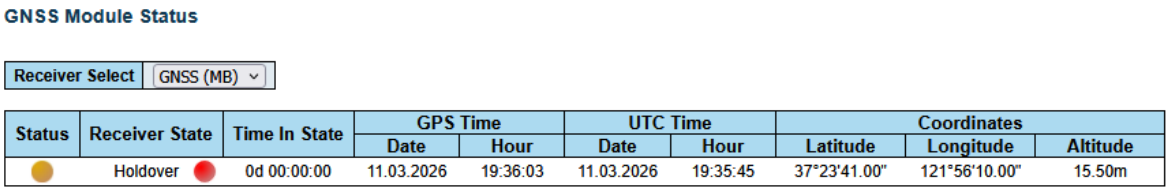


Figure 4-83: GNSS Module Status

Table 4-76: Receiver parameters

Receiver Select	Select the type of receiver. The options are: • GNSS (MB) • STL
Status	
Status	Displays the current GNSS Module status
Receiver State	Displays the Receiver State
Time In State	Displays the length of time the receiver has been in the current state
GPS Time	Displays the current GPS Date and Hour
UTC	Displays the current UTC time
Coordinates	Displays the current Latitude, Longitude, and altitude of the GNSS module

4.8.1 Satellite Status

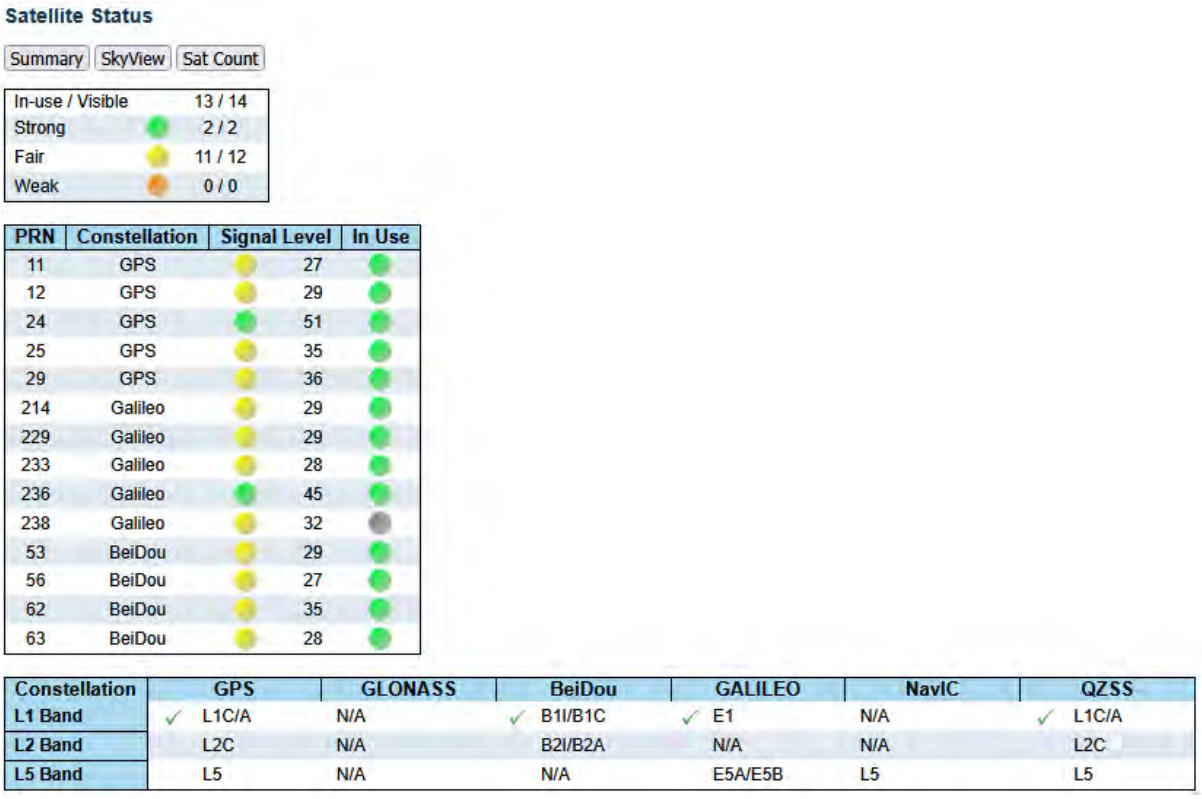


Figure 4-84: Satellite Status

Table 4-77: Satellite Status parameters

PNR	The PRN (satellite number) of the tracked satellites.
Constellation	The satellite constellation type. The options are: • GPS • GLONASS • BeiDou • GALILEO • NavIC • QZSS
Signal Level	The satellite's received signal level in terms of Carrier to Noise ratio [dB-Hz]. The accompanying LED indicates whether the satellite receive level is good (green) or fair (**orange**).
In Use	Shows when a satellite is In use **(green)** by the device
Summary Table	Shows the number of total tracked satellites and good satellites.
Details/Summary Button	Toggle detailed satellite table on/off

4.8.1 Antenna Cable Status

Antenna Cable Status

Type	Length	Delay (ns)	Ant. pwr	Description
RG6	25	111		

Figure 4-85: GNSS Antenna Cable Status

Table 4-78: GNSS Antenna Cable parameters

Type	The type of cable being used for the antenna.
Length	The length of the antenna cable in meters.
Delay	Indicates the cable delay in nsec.
Description	A textual description of the cable.

4.8.2 Sky View

This section displays the current sky map of the GNSS receiver tracked satellites.

Web GUI: Monitor > Timing > GNSS > SkyView

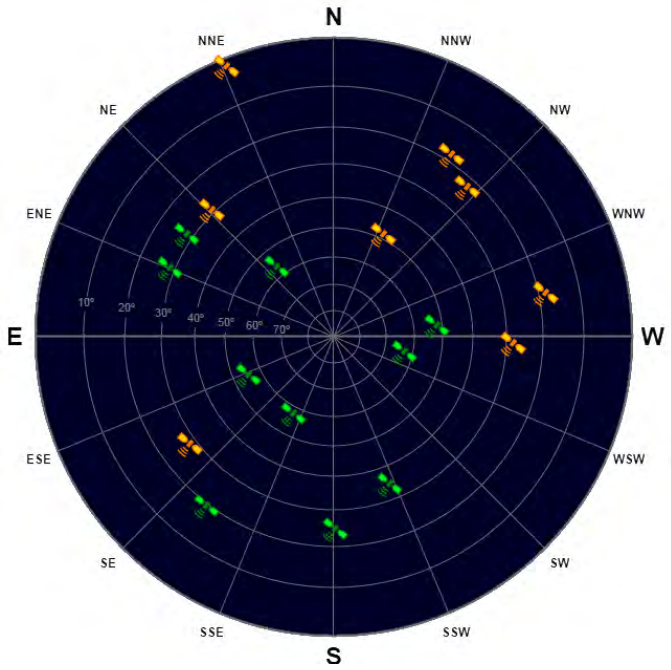


Figure 4-86: Sky view display

Table 4-79: Sky View parameters

Displays the sky view of the tracked satellites. The azimuth angle is the angle between the North ('N') and radial on which the satellite is displayed. The elevation angle is represented by the distance from the center (90 degrees) to the edge of the sky map circle (0 degrees). Each satellite icon is positioned according to status and displayed in green (strong receive signa) or orange (fair signal). When pointing on a satellite a text box balloon will automatically open, showing satellite info highlights.

4.8.3 Satellite Count

This section displays a graph of the tracked satellites count.

Web GUI: Monitor > Timing > GNSS > Sat Count

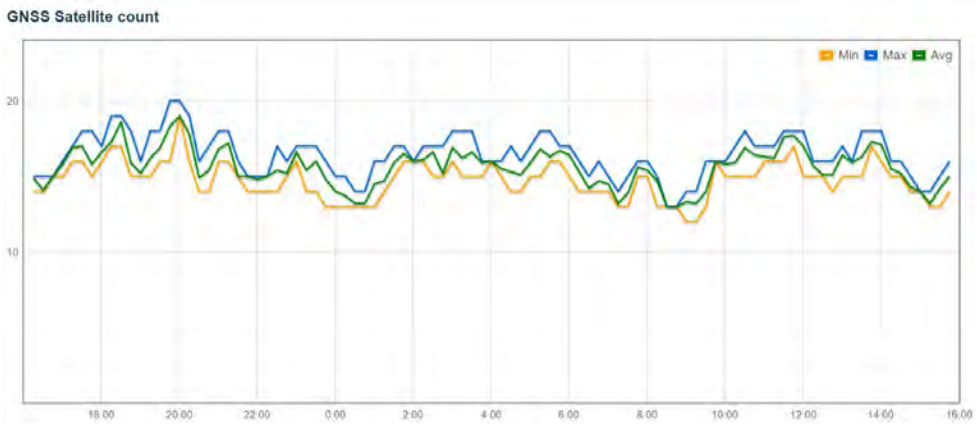


Figure 4-87: Satellite Count display

Table 4-80 Satellite Count parameters

Satellite Count	The type of cable being used for the GNSS antenna.
Graph type	Selection of type of graph to show: Time axis duration can be 15 minutes (1 minute resolution) or 24 hours (15 minutes resolution- Show only good (above threshold) satellites or all visible (tracked)ones.
Common Buttons	**Send Report**: send report to your computer if you have set the required parameter in the EdgeGM 7000 report Configuration. **Other Buttons**: GNSS Config. Sky View. Sat Counts are direct links to the respective pages.

4.8.4 Interference Status

Web GUI: Monitor > Timing > GNSS > Interference

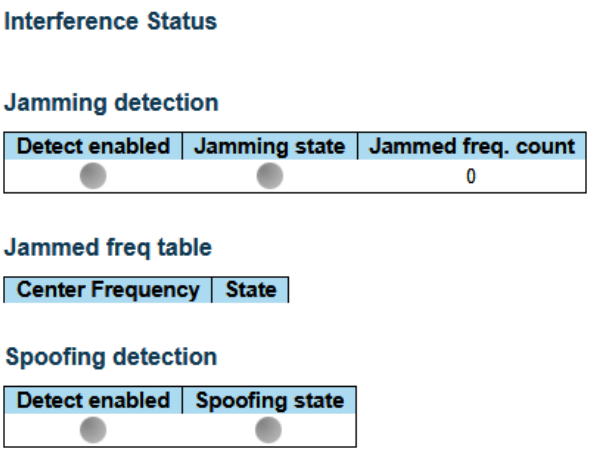


Figure 4-88: Interference Status parameters

Table 4-81 Interference Status parameters

Jamming detection	The type of cable being used for the GNSS antenna.

Detect enabled	Displays whether detection is enabled
Jamming state	Displays the current jamming state of the device.
Jammed freq. count	Displays a count of all jammed frequencies.

4.9 IEEE1588 Precision Time Protocol

PTP is an acronym for **P**recision **T**ime **P**rotocol, a network protocol for synchronizing the clocks of Network systems. Regarding Ethernet Backhaul, PTP is considered the technology of choice to deliver clock synchronization to remote telecom base stations. PTP defines synchronization message used between a Master and Slave clock. The Master provides the time, and the slave synchronizes to the Master

Multiple slaves can synchronize to a single Master. The Master clock provides synchronization message that the slaves use to correct their local clocks. This section allows the user to configure and inspect the current PTP Clock settings. In Synchronous mode of operation, the Synchronous Ethernet interface processes the SSM (**Synchronization Status Messages)** and recovers the clock quality level information. The ESMC channel is a logical communication channel which transmits SSM information that is the quality level of the transmitting synchronous Ethernet equipment clock.

When a Synchronous Ethernet port is selected, the SSM are transmitted through this port, indicating the quality level of the clock it can drive. The messages are received (if the other remote unit supports SyncE) with the quality level of the transmitting clock. The remote end unit receiving the messages on its configured Synchronous Ethernet port extracts the clock quality level and transmits it to the Clock Master Unit. The Clock Master Unit receives the SSM data from many Synchronous Ethernet ports and establishes the clock sources. The device internal state logic (clock selector) monitors all reference clocks and automatically selects the best available reference clock based on configured priority and revertive priorities. There are different synchronization methods as described below

The Auto-Revertive is the default mode of operation. This mode includes two functions: automatic reference clock selection (the highest priority qualified clock is selected) and the occurrence of the Revertive function when needed.

The clock selection process supports revertive and non-revertive modes of operation. If the Auto- revertive mode is enabled: when the clock selection process has selected -a primary clock, and the active primary clock source has failed o degraded over a certain period and then is later recovered, this primary clock source becomes again the active clock source. If Auto non-revertive mode is selected and a secondary clock source is active (due to a previous degradation of the primary clock source), the primary clock source is not reactivated even after its quality has been improved.

Methods of Operation

Note: the following modes of operation can be selected under Clock Central Configuration.

Auto Revertive: In this mode, the highest priority qualified reference clock is selected. If this selected clock fails or it is degraded, the next priority qualified clock is selected, and the lock acquisition will begin. If the previous primary clock is restored and qualified, then the revertive function will compel the previous primary clock to become again the active clock source.

Auto Non Revertive: Clock Selection of the best clock source is only done when the selected clock fails. The primary clock source is not reactivated in this case.

Free-Run mode: The free-run mode occurs immediately, after a reset, or when the timing synchronization logic has not yet been synchronized to a reference clock input. In this mode the frequency accuracy of the clock outputs is equal to the frequency accuracy of the input master clock.

Manual: The user may select the clock source (None, SyncE, PTP, TDM, External) If this manually selected clock source is failing, the clock selector will go into holdover state.

Normal (Locked mode): The input clock references are monitored for frequency accuracy and phase correctness. If at least one is of the clock reference inputs is qualified, then the logic will start the lock acquisition of that clock input. And the device logic will enter the normal locked mode. During the normal locked operation, the time synchronization logic phase locks to the qualified reference clock and generates output clocks and frame pulses with a frequency accuracy equal to the frequency accuracy of the input reference clock. The generated clock and frames pulse outputs comply with specifications as described in Telcordia and ITU-T Telecommunication standard.

Holdover state: When the timing synchronization logic loses its reference input clock or becomes degraded, and no other qualified clock references are available, it will enter in holdover mode and continue to create output clocks based on the reference frequency data collected during the synchronization process.

PTP Messages

PTP defines the following messages for synchronization and control between devices:

Event message (timing message): Types of event messages: Sync, Delay_Req, Pdelay_Req, Pdelay_Req.

General messages: Announce, Follow-Up. Delay_Resp, Pdelay_Resp_Follow_Up, Management, Signaling. (Pdelay=Peer delay)

4.9.1 PTP Clock Configuration

This section describes the PTP clock configuration settings.

Note: By clicking on PTP Config "Add New PTP Clock" you get the following additional display

Web GUI: Configuration > Timing > PTP

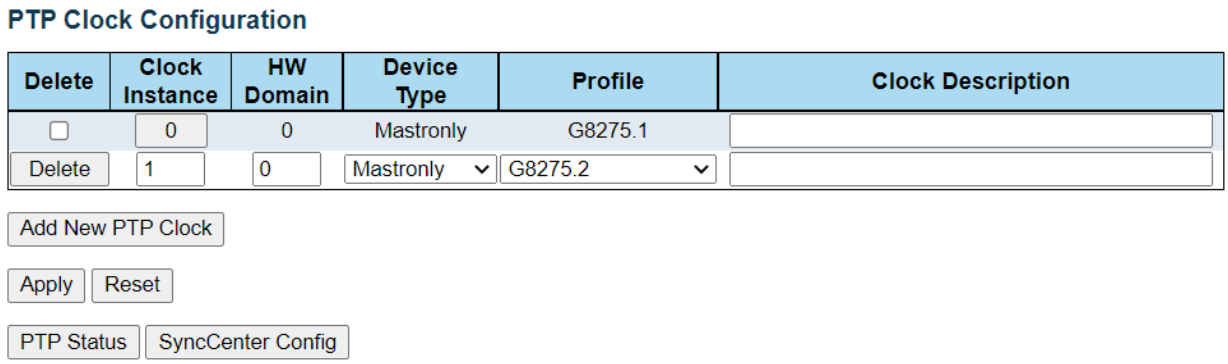


Figure 4-89: PTP Clock Configuration

Note: After applying the Clock configuration hit the button with the clock instance number to continue to the instance detailed configuration

Table 4-82: PTP Clock Configuration Parameters (for both displays)

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.
Device Type	Indicates the Type of the Clock Instance. There are five Device Types. 1. Ord-Bound – clock's Device Type is Ordinary-Boundary Clock. 2. P2p Transp – clock's Device Type is Peer to Peer Transparent Clock. 3. E2e Transp – clock's Device Type is End to End Transparent Clock. 4. Master Only – clock's Device Type is Master Only. 5. Slave Only – clock's Device Type is Slave Only. **Definitions:** **Master & Slave clock**: has only one physical port to the network and can be implemented as a master or slave clock. The OC sends and receive PTP messages. It supports the synchronization mechanism. **Boundary clock**: has multiple physical ports to the network and can be used as an intermediate stage/device. The BC performs the functionality of the Ordinary clock and can be connected to multiple sub-networks: normally it is synchronized to one Master reference clock and provides synchronization to various clients.

	End to End Transparent clock: there are multiple ports and do not behave or perform a Master and slave relationship. These ports forward all PTP messages and correct the timing. **Peer to peer Transparent clock:** there are multiple ports and do not behave or perform a Master and slave relationship. Each port supports the Pdelay mechanism
Profile	Indicates the profile used by the clock.
Clock Description	User defined free text (64 characters)
Buttons	**Add New PTP Clock**: Hit to add a PTP clock instance entry to the table. **Apply**: Hit to apply the clock instance settings to the running-config. **Reset**: Hit to reset the new clock instance parameters to previous values. **PTP Status**: Click on it to go to PTP Status display. **Clock Central config**: Click on it to go to Clock Central config. display

4.9.2 PTP Clock's Configuration and Status

This page allows the user to inspect and configure the current PTP clock settings. It contains the following configuration and status tables:

Web GUI: Configuration > Timing > PTP > (Hit Clock Inst. Number)

4.9.2.1 Clock Type and Profile

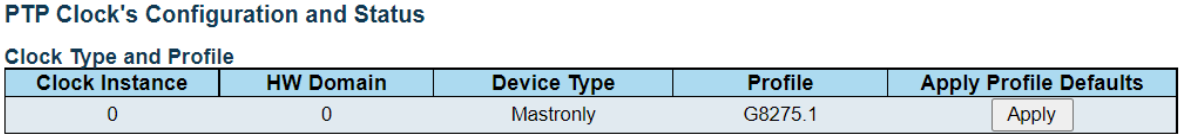


Figure 4-90: Clock Type and Profile

Table 4-83: Clock Type and Profile

Clock Instance	Indicates the Instance 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 five Device Types. 1. Ord-Bound – clock's Device Type is Ordinary-Boundary Clock. 2. P2p Transp – clock's Device Type is Peer to Peer Transparent Clock. 3. E2e Transp – clock's Device Type is End to End Transparent Clock. 4. Master Only – clock's Device Type is Master Only. 5. Slave Only – clock's Device Type is Slave Only.
Profile	Indicates the profile used by the clock.

Apply Profile Defaults	If the clock has been configured to use a profile, clicking the 'Apply' button will reset configured values to profile defaults.

4.9.2.2 Port Enable and Configuration

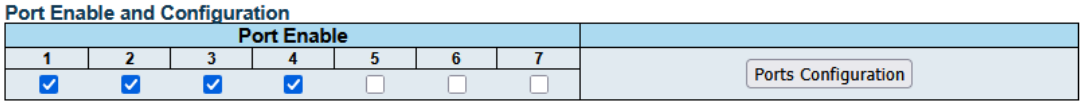


Figure 4-91: Port Enable and Configuration

Table 4-84: Port Enable and Configuration

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.

4.9.2.3 PTP Clock's Port Data Set configuration

This page allows the user to configure the PTP port data settings. Configuring the ports data set is accessible form the "Port Enable and Configuration" page by hitting **Ports Configuration.**

Web GUI: Configuration > Timing > PTP > Port Enable and Configuration > (Hit Clock Ports Configuration)

It contains the following configuration and status tables:

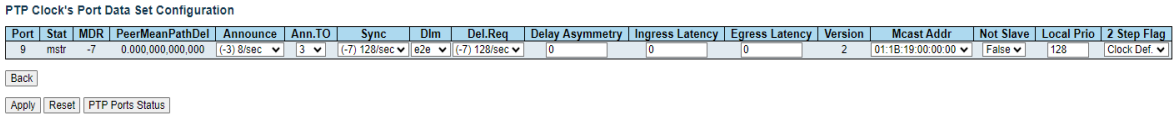


Figure 4-92: PTP Clocks Port Data set

Table 4-85: PTP Clocks Port Data set

Port	Static member port Identity: Port number [1..max port no]
Stat	Dynamic member portState: Current state of the port.
Peer Mean Path Del	The path delay measured by the port in P2P mode. In E2E mode this value is 0.
Announce	The interval for issuing announce messages in master state. Range is 8PPS to 1/16PPS.
Ann.TO	The timeout for receiving announce messages on the port. Range is 1 to 10
Sync	he interval for issuing sync messages in master. Range is 128PPS to 1/16PPS.

Dlm	Configurable member delayMechanism: The delay mechanism used for the port: • e2e - End to end delay measurement • p2p - Peer to peer delay measurement. • cp2p - Common Peer to peer delay measurement used in 802.1AS. There will be single instance of common peer to peer delay measurement per port. 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.
Del.Req	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 128PPS to 1/32PPS.
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.
Mcast Addr	Configured destination address for L2 multicast packets. The options are 01:1B:19:00:00:00 (default, forwardable MAC address) and 01:80:C2:00:00:0E (link-local, non-forwardable MAC).
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

4.9.2.4 Local Clock Current Time

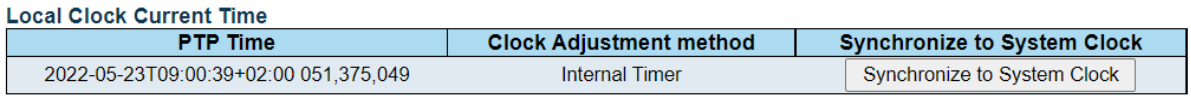


Figure 4-93: Local Clock Current time

Table 4-86: Local Clock Current time

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.

4.9.2.5 Clock Current DataSet

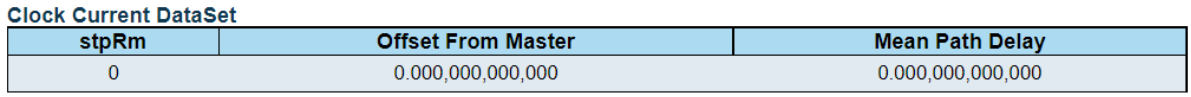


Figure 4-94: Clock Type and Profile

Table 4-87: Clock Type and Profile

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.

4.9.2.6 Clock Parent Data Set

The clock parent data set is defined in the IEEE 1588 standard. The parent data set is dynamic.

Figure 4-95: Clock Type and Profile

Table 4-88: Clock Type and Profile

Parent Port ID	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.
PStat	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 DataSet:Clock Quality)
Pri1	Clock priority 1 announced by the grand master.
Pri2	Clock priority 2 announced by the grand master.

4.9.2.7 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.

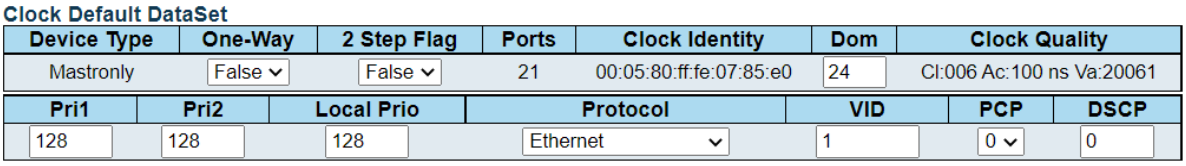


Figure 4-96: Clock Default DataSet

Table 4-89: Clock Default DataSet

Device Type	Indicates the Type of the Clock Instance. There are five Device Types. 1. Ord-Bound – clock's Device Type is Ordinary-Boundary Clock. 2. P2p Transp – clock's Device Type is Peer to Peer Transparent Clock. 3. E2e Transp – clock's Device Type is End to End Transparent Clock. 4. Master Only – clock's Device Type is Master Only. 5. Slave Only – clock's Device Type is Slave Only.
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	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 IPv6Mixed PTP using a combination of IPv6 multicast and unicast. Currently, this is supported for only One step E2E Transparent clock. EthIPv4IPv6Combo PTP using any one of Ethernet, IPv4 or IPv6. This is supported for only one step E2E Transparent clocks.
VID	VLAN Identifier used for tagging the VLAN packets.
PCP	Priority Code Point value used for PTP frames.
DSCP	DSCP value used when transmitting IPv4 encapsulated packets.

4.9.2.8 Master Enable on State

The Master Enable on State allow the user to control the PTP instance message transmission based on the Clock Central operational state. PTP transmission can be set to one of the following modes per Clock Central state:

- Disabled – PTP transmission deactivated
- Enabled - PTP transmission activated
- Rule 0 - PTP transmission activation is conditioned to Instance 0 state

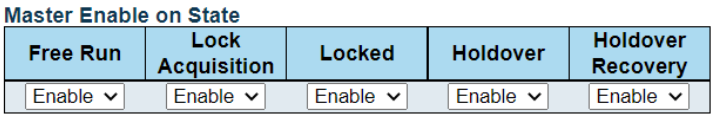


Figure 4-97: Master Enable on State

Table 4-90: Master Enable on State

Free Run	In Free Run state PTP can be set to: Disable, Enable, Rule 0.
Lock Acquisition	In Lock Acquisition state PTP can be set to: Disable, Enable, Rule 0.
Locked	In Locked state PTP can be set to: Disable, Enable, Rule 0.
Holdover	In Holdover state PTP can be set to: Disable, Enable, Rule 0.

Holdover Recovery	In Holdover Recovery state PTP can be set to: Disable, Enable, Rule 0.

4.9.2.9 Quality Override

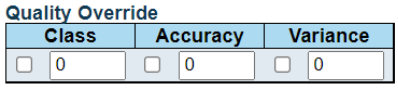


Figure 4-98: Quality Override

Class	Tick checkbox to enable Clock Class override, then set the desired value.
Accuracy	Tick checkbox to enable Accuracy override, then set the desired value.
Variance	Tick checkbox to enable Variance override, then set the desired value.

Table 4-91: Quality Override

4.9.2.10 Clock Default DataSet

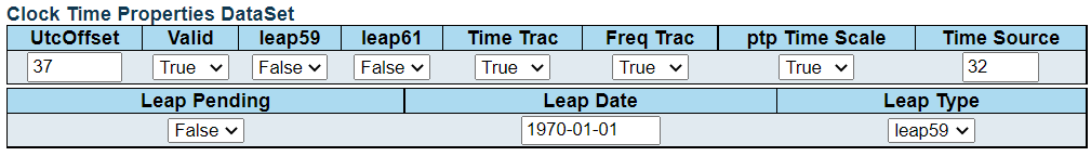


Figure 4-99: Clock Type and Profile

Table 4-92: Clock Type and Profile

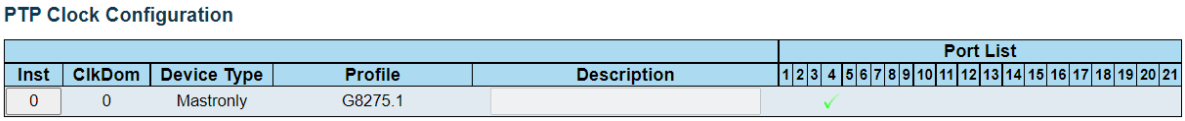
UtcOffset	In systems whose epoch is UTC, it is the offset between TAI and UTC
Valid	When true, the value of currentUtcOffset is valid
leap59	When true, this field indicates that last minute of the current UTC day has only 59 seconds.
leap61	When true, this field indicates that last minute of the current UTC day has 61 seconds.
Time Trac	True if the timescale and the value of currentUtcOffset are traceable to a primary reference.
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.

Buttons	**Apply**: Hit to apply the clock instance settings to the running-config. **Reset**: Hit to reset the new clock instance parameters to previous values. **PTP Global**: Hit to return to PTP Global configuration screen. **PTP Clock Status**: Click on it to go to PTP Clock Status screen.

4.9.3 PTP Monitoring

This section allows the user to inspect the current PTP clock settings

Web GUI: Monitor > Timing > PTP > Clocks


PTP Clock Configuration

					Port List
Inst	ClkDom	Device Type	Profile	Description	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21
0	0	Mastronly	G8275.1		✓

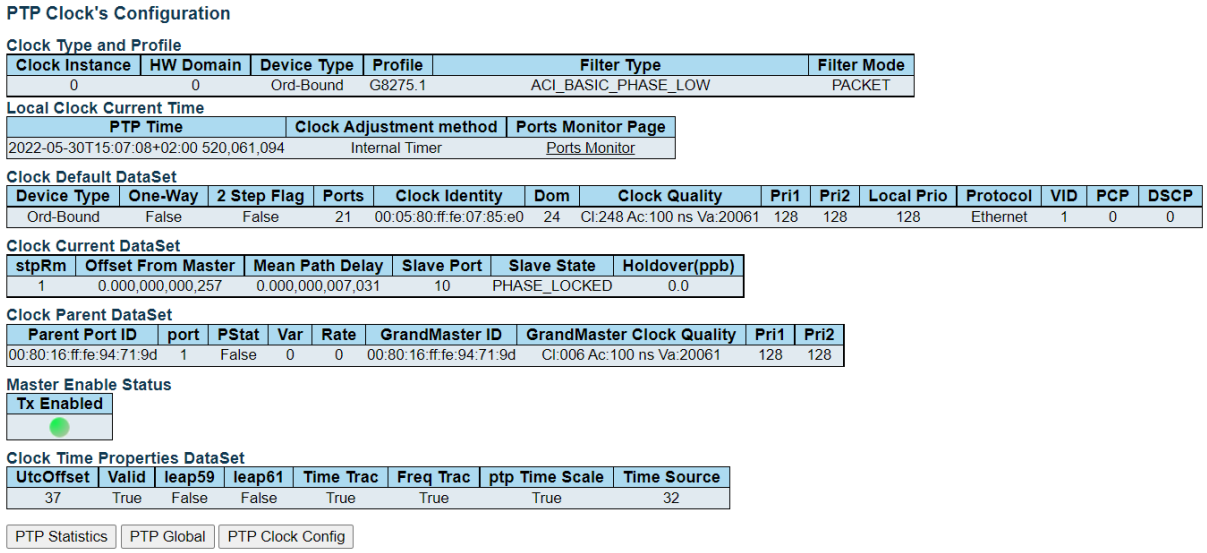
Figure 4-100: PTP Clock Status

Table 4-93: PTP Clock Status Parameters

Inst	Indicates the Instance of a particular Clock Instance [0...3]. Click on the Clock Instance number to monitor the Clock details.
ClkDom	Refers to Clock HW Domain
Device Type	Indicates the Type of the Clock Instance. There are five Clock Types: • **Boundary** – clock's Type is Ordinary-Boundary Clock. • **Transparent (P2P)** – Clock's Type is Peer to Peer Transparent Clock. • **Transparent (E2E)** – Clock's Type is End to End Transparent Clock • **Master Only** - Clock's e Type is Master Only. • **Slave Only** - Clock's Type is Slave Only.
Profile	Indicates the profile used by the clock.
Description	User defined free text (64 characters)
Port List	It shows the configured ports for the specified Clock Instance.
Buttons	**Instance number:** Hit to access detailed Clock Instance Status page **PTP Config**: Click on it to go to PTP Configuration display. **Clock Central config**: Click on it to go to Clock Central config. display

4.9.3.1 PTP Clock Instance Status

Web GUI: Monitor > Timing > PTP > Clocks > (Hit Clock Inst. Number)


PTP Clock's Configuration

Clock Type and Profile

Clock Instance	HW Domain	Device Type	Profile	Filter Type	Filter Mode
0	0	Ord-Bound	G8275.1	ACI_BASIC_PHASE_LOW	PACKET

Local Clock Current Time

PTP Time	Clock Adjustment method	Ports Monitor Page
2022-05-30T15:07:08+02:00 520,061,094	Internal Timer	Ports Monitor

Clock Default DataSet

Device Type	One-Way	2 Step Flag	Ports	Clock Identity	Dom	Clock Quality	Pri1	Pri2	Local Prio	Protocol	VID	PCP	DSCP
Ord-Bound	False	False	21	00:05:80:ff:fe:07:85:e0	24	Cl:248 Ac:100 ns Va:20061	128	128	128	Ethernet	1	0	0

Clock Current DataSet

stpRm	Offset From Master	Mean Path Delay	Slave Port	Slave State	Holdover(ppb)
1	0.000,000,000,257	0.000,000,007,031	10	PHASE_LOCKED	0.0

Clock Parent DataSet

Parent Port ID	port	PStat	Var	Rate	GrandMaster ID	GrandMaster Clock Quality	Pri1	Pri2
00:80:16:ff:fe:94:71:9d	1	False	0	0	00:80:16:ff:fe:94:71:9d	Cl:006 Ac:100 ns Va:20061	128	128

Master Enable Status

Tx Enabled

Clock Time Properties DataSet

UtcOffset	Valid	leap59	leap61	Time Trac	Freq Trac	ptp Time Scale	Time Source
37	True	False	False	True	True	True	32

PTP Statistics | PTP Global | PTP Clock Config

Figure 4-101: PTP Clock Instance Status

Table 4-94: PTP Clock Instance Status Parameters

Clock Instance	Indicates the Instance of a particular Clock Instance [0...3]
ClkDom HW Domain	Refers to Clock HW Domain
Device Type	Indicates the Type of the Clock Instance. There are five Clock Types: • **Boundary** – clock's Type is Ordinary-Boundary Clock. • **Transparent (P2P)** – Clock's Type is Peer to Peer Transparent Clock. • **Transparent (E2E)** – Clock's Type is End to End Transparent Clock • **Master Only** - Clock's e Type is Master Only. • **Slave Only** - Clock's Type is Slave Only.
Profile	Indicates the profile used by the clock.
PTP Time	Shows the actual PTP time with nanosecond resolution.
Clock Adjust. Method	Shows the actual clock adjustment method. The method depends on the available hardware.
Ports Monitor Page	Click to monitor the port data set for the ports assigned to this clock instance.
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	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	Local priority for G8275.1 BMC algorithm (1 is highest priority).
Protocol	• Transport protocol used by the PTP protocol engine • Ethernet PTP over Ethernet multicast • ip4multi PTP over IPv4 multicast • ip4uni PTP over IPv4 unicast
VID	VLAN Identifier used for tagging the PTP frames. Note: Packets are tagged if the port is configured for vlan tagging for the configured VID.
PCP	Priority Code Point value used for PTP frames.
DSCP	Priority Code Point value used for PTP frames.
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.
Slave Port	Shows which port is in slave mode. The value is 0 if no ports are in slave mode.
Slave State	Shows synchronization state of the slave (Slave only/Boundary): FREERUN, FREQ_LOCKING, PHASE_LOCKING, PHASE_LOCKED, HOLDOVER.
Holdover(pbb)	After the slave has been in Locked mode during the stabilization period, this value shows the actual clock offset between the free run and the actual holdover frequency, the value is shown in parts pr billion (ppb). During the stabilization period, the value is shown as N.A. The stabilization period is 60 sec as default, it can be changed from the CLI interface.
Parent Port ID	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.
PStat	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).

GrandMaster ID	Clock identity for the grand master clock, if the local clock is not a slave, the value is the clocks own id.
GrandMaster Clock Quality	The clock quality announced by the grand master (See description of Clock Default DataSet:Clock Quality).
Pri1	Clock priority 1 announced by the grand master.
Pri2	Clock priority 2 announced by the grand master.
Tx Enabled	Green – Indicates Master is enabled for PTP transmission. Red – Indicates Master is NOT enabled for PTP transmission.
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.
Buttons	**PTP Config**: Click on it to go to PTP Configuration display. **Clock Central config**: Click on it to go to Clock Central config. Display.

4.9.3.2 PTP Clock Statistics

This page allows the user to view the **PTP Clock Statistic**.

Web GUI: Monitor > Timing > PTP > Clocks > PTP Clock Instance Status > (Hit PTP Statistic)

It contains the following status tables:

PTP Clock Statistics

Clock Instance	0
Statistics Type	All

Slave Packet Statistics

Time since last reset		13d 02:38:00
Messages		
Announce	RX	8420000
Sync	RX	138265222
Follow-Up	RX	0
Delay Request	TX	138208104
Delay Response	RX	138207938
P Delay Response	RX	0
P Delay Response Follow-Up	RX	0
Management	RX	0
Errors		
Unknown Domain	RX	137
Unknown	RX	0
Lost Delay Response	RX	178
Lost Delay Response Follow-Up	RX	0
Unknown Signalling	RX	0
Signalling		
Total	RX	44639
Total	TX	45155
Announce Request	TX	15983
Announce Grant	RX	15467
Announce Grant Timer		22 sec
Announce Cancel Request	TX	0
Sync Request	TX	14586
Sync Grants	RX	14586
Sync Grant Timer		22 sec
Sync Cancel Request	TX	0
Delay Response Request	TX	14586
Delay Response Grants	RX	14586
Response Grant Timer		22 sec
Ack Cancel	RX	0
Ack Cancel	TX	0
General Deny Grants	RX	0
Cancel request	TX	0
General		
Master Select Changes (BMCA)		3

Clear

Figure 4-102: PTP Clock Statistic

Slave Delay Statistics (sec)

Time since last reset	13d 02:39:05
Master to slave	
Max	0.000,000,031,773
Min	-0.000,000,019,203
Mean	0.000,000,009,497
Current	-0.000,000,003,136
Slave to master	
Max	0.000,000,031,792
Min	-0.000,000,019,082
Mean	0.000,000,003,271
Current	0.000,000,015,210
Path delay	
Max	0.000,000,006,421
Min	-0.000,000,798,242
Mean	-0.000,000,346,447
Current	0.000,000,005,642

Clear

Figure 4-103: slaves delay Statistics (sec)

Slave Servo Statistics

Time since last reset	13d 02:39:54
Servo count	0
Last offset from referense	-8 nsec
Filter Dispersion	0 nsec

Clear

Figure 4-104: Slave Servo Statistic

Master Packet Statistics

Time since last reset		13d 02:40:27
Messages		
Announce	TX	3949444
Sync	TX	3949451
Follow Up	TX	0
Delay Request (CPU)	RX	0 (0)
Delay Response (CPU)	TX	0 (0)
P Delay Request	RX	0
Management	RX	0
Errors		
Unknown Domain	RX	137
Unknown	RX	0
Unknown cancel	RX	2
Unknown Signalling	RX	0
Signalling		
Total	RX	20600
Total	TX	20598
Announce Request	RX	6920
Announce Grant	TX	6920
Deny Announce Request (No resource available)	TX	0
Announce Cancel Request	RX	2
Sync Request	RX	6838
Sync Grant	TX	6838
Deny Sync Request (No resource available)	TX	0
Sync Cancel Request	RX	0
Delay Response Request	RX	6838
Delay Response Grant	TX	6838
Delay Response Cancel Request	RX	0
Ack Cancel	TX	2
General Deny Request	TX	0
Cancel Request	RX	4

Clear

Figure 4-105: Master Packet Statistics

4.9.4 PTP Slave Table

This section shows the PTP Slave Table (Relevant for Unicast profiles only).

Web GUI: Monitor > Timing > PTP > Slave Table

PTP Slave Table

#	Clock Instance	IPv4 Address	IPv6 Address	Port #	MAC Address	Status		Message rate (FPS)		
						Sync	Ann	Sync	DelReq	Announce
1	0	192.168.5.163	::	1	00-05-80-05-00-03			8/sec	8/sec	1/sec

Figure 4-106: PTP Slave Table

Table 4-95: PTP Slave Table

#	Index of slave (has no functional impact).

Clock Instance	The master's clock instance.
IP Address	The slave's IP address.
Port #	The master's port number.
MAC Address	The MAC address of the slave (or the gateway's).
Status	**Sync** - Indicates Sync messages are transmitted to the slave. **Ann** - Indicates Announce messages are transmitted to the slave.
Message rate (FPS)	**Sync** - The current rate of Sync messages to the slave (as negotiated with the master). **DelReq** - The current rate of Delay Request messages from the slave (as negotiated with the master). **Announce** - The current rate of Announce messages to the slave (as negotiated with the master)

The slave device must collect 4 timestamps when PTP Sync and Del.Req messages are transmitted and received in order to calculate the offset from master clock.

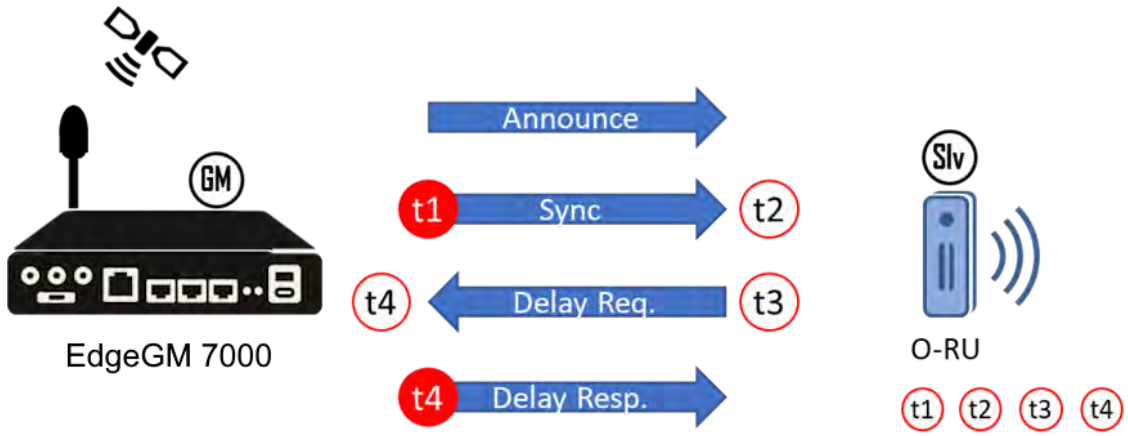


Figure 4-107: Basic working principle of IEEE 1588v2

4.10 Synchronous Ethernet (SyncE)

4.10.1 Overview

This section allows the user to inspect and configure the current SyncE port settings. SyncE is used to make an Ethernet network 'clock frequency' synchronized. Mobile network operators have started to deploy 4G/LTE networks. Ethernet has become the logical choice for mobile backhaul. These operators would like to deploy voice over Ethernet. Ethernet networks must provide timing and synchronization to enable proper operation of the mobile services. **The EdgeGM 7000 devices** are offered with complete precision timing support based on Synchronous Ethernet and 1588-2008 (PTP) for LTE mobile backhaul applications.

The aim of Synchronous Ethernet is to provide a synchronous signal to network resources that may need such frequency synchronization signal. SyncE was standardized by the ITU-T and supports the following recommendations:

ITU-T G8261 standard that defines aspects regarding the architecture and performance of SyncE networks.

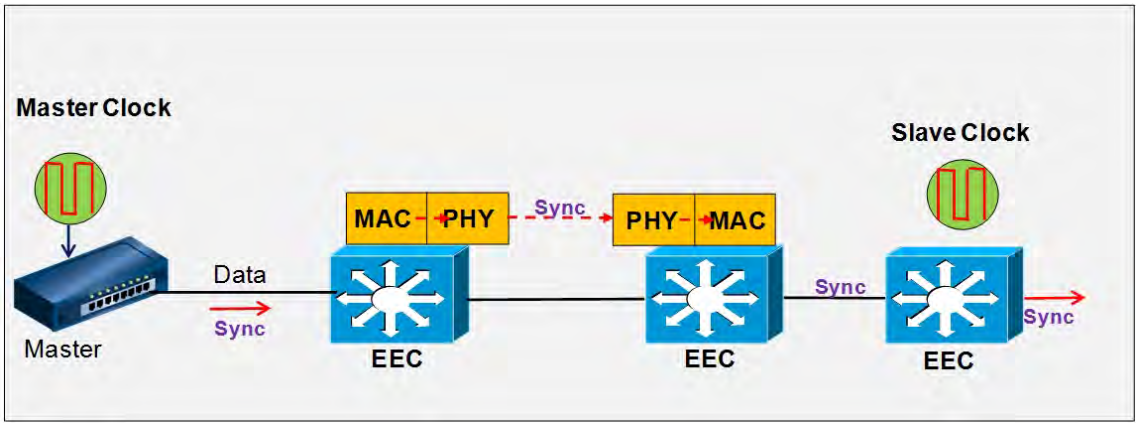
ITU-T G8262 standard which specifies SyncE slave clocks.

ITU-T G8264 standard that describes the specifications of Ethernet Synchronization Messaging Channel (ESMC)

In Synchronous mode of operation, the Synchronous Ethernet interface processes the SSM (**Synchronization Status Messages)** and recovers the clock quality level information. The ESMC channel is a logical communication channel which transmits SSM information, that is the quality level of the transmitting synchronous Ethernet equipment clock.

When a Synchronous Ethernet port is selected, the SSM are transmitted through this port, indicating the quality level of the clock it can drive. The messages are received (if the other remote unit supports SyncE) with the quality level of the transmitting clock. The remote end unit receiving the messages on its configured Synchronous Ethernet port extracts the clock quality level and transmits it to the Clock Master Unit. The Clock Master Unit receives the SSM data from many Synchronous Ethernet ports and establishes the clock sources. The device internal state logic (clock selector) monitors all reference clocks and automatically selects the best available reference clock based on configured priority and revertive priorities.

SyncE Basic mechanism



The master switch receives the external clock which is a high precision clock. In a synchronous Ethernet network, Ethernet data is carried over layer 2 whereas the sync timing signals over physical layer 1. All internal clocks should be synchronized by the external reference clock.

The Ethernet interfaces are designed with an internal clock which is synchronized by the master external clock. SyncE enables the transport of slave synchronization signals within the entire network.

The EEC devices are defined as Ethernet Equipment Slave clocks. Ethernet interfaces are also able to generate their own synchronization clock in case they lose the master reference clock (this situation is defined as holdover state**).**

The SyncE Configuration procedure for the EdgeGM 7000 es includes the following display:

4.10.2 SyncE Port Configuration

This section displays and allows configuration of the SyncE configuration of the applicable Ethernet ports.

Web GUI: Configuration > Timing > SyncE

Figure 4-108: SyncE SSM Configuration

Table 4-96: SyncE configuration

SyncE Configuration	
SSM Option Select	Select the system network region option: • SSM Option 1 - refers to synchronization networks designed for Europe. • SSM Option 2 - refers to synchronization networks designed for US.
SSM Free Run	Set the SSM output quality level in Free Run state: PRC, SSUB, SSUA, EEC1, DNU
SSM Holdover	Set the SSM output quality level in Holdover state: PRC, SSUB, SSUA, EEC1, DNU

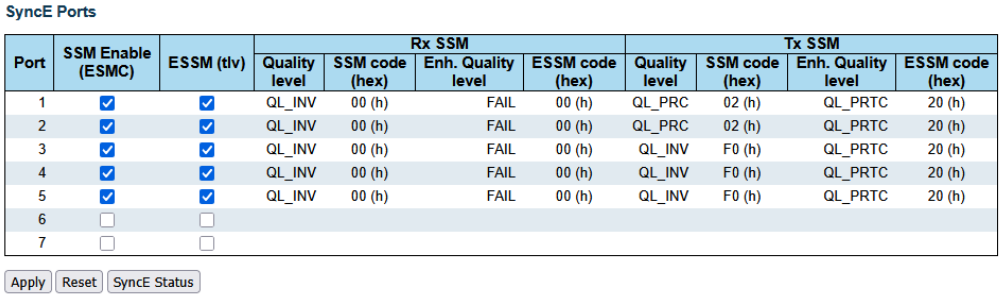


Figure 4-109: SyncE Port Configuration

Table 4-97: SyncE Port Configuration Parameters

SyncE Ports	
Port	The port number to configure.
SSM Enable	Enable and disable of SSM functionality on this port.
Tx SSM: Quality Level	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.
Tx SSM: SSM code (hex)	Displaying the actual hex code used to indicate the transmitted Quality.
Rx SSM: Quality Level	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.
Rx SSM: SSM code (hex)	Displaying the actual hex code used to indicate the received Quality.
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.

4.10.3 SyncE Port Monitoring

This section displays and allows configuration of the SyncE configuration of the applicable Ethernet ports.

Web GUI: Monitor > Timing > SyncE

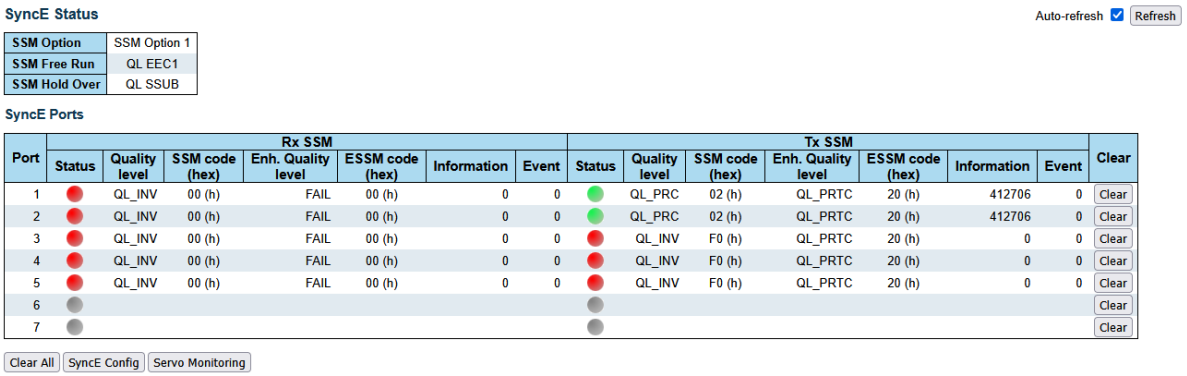


Figure 4-110: SyncE Status

Table 4-98: SyncE Status Parameters

SyncE Status	
SSM Option Select	Display the system network region option: • SSM Option 1 - refers to synchronization networks designed for Europe. • SSM Option 2 - refers to synchronization networks designed for US.
SSM Free Run	Display SSM output quality level in Free Run state: PRC, SSUB, SSUA, EEC1, DNU
SSM Holdover	Display SSM output quality level in Holdover state: PRC, SSUB, SSUA, EEC1, DNU

Table 4-99: SyncE Port Status Parameters

SyncE Ports Status	
Port	The port number to configure.
Tx SSM: Status	Enable and disable of SSM functionality on this port.
Tx SSM: Quality Level	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
Tx SSM: code (hex)	Displaying the actual hex code used to indicate the transmitted Quality
Tx SSM: Information	Counter displaying the number of transmitted SSM Information messages
Tx SSM: Event	Counter displaying the number of transmitted SSM Event messages
Rx SSM: Status	Enable and disable of SSM functionality on this port.
Rx SSM: Quality Level	Monitoring of the received SSM QL on this port.
Rx SSM: code (hex)	Displaying the actual hex code indicating the received Quality per port

Rx SSM: Information	Counter displaying the number of received SSM Information messages
Rx SSM: Event	Counter displaying the number of received SSM Event messages
Clear	Hit **Clear** button to reset counters per port
Buttons	**SyncE Config**: Click on it to go to PTP Configuration display. **Clear All**: Click to reset all ports counters

4.11 External Sync Ports Configuration

Web GUI: Configuration > Timing > External

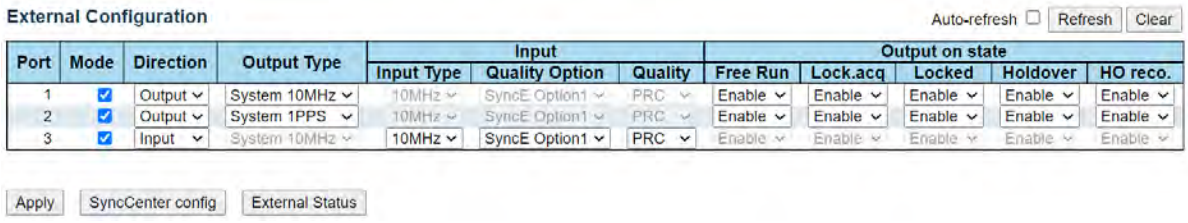


Figure 4-111: External Clock Configuration

Table 4-100: External Clock Configuration parameters

Port	Indicates sync port number.
Mode	Enable or disable the sync port.
Direction	Set the port to either input or output.
Output Type	Set the port's output type and frequency. Applicable when the port is set to **Output**
Input Type	Set the port's input type and frequency. Applicable when the port is set to **Input**
Quality Option	Set the input signal Quality Option
Quality	Set the input signal Quality level
Buttons	**Clock Central config:** click to go to Clock Central Configuration page. **External Status:** click to go to External Clock Status page.

4.11.1 External Status

Web GUI: Monitor > Timing > External

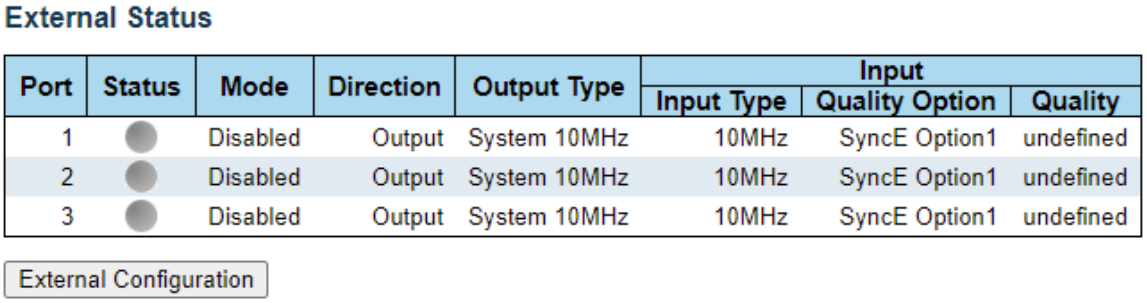


Figure 4-112: External Status

Table 4-101: External Status parameters

Port	Indicates sync port number.
Mode	Indicates whether the Sync port's state is Enabled or Disabled.
Direction	Indicates whether the Sync port's direction is Input or Output.
Output Type	Indicates the Sync port's Output type.
Input	Indicates the Sync port's Input type.
Quality Option	Indicates the Sync port's Input Quality Option
Input Quality	Indicates the Sync port's Input Quality level
Buttons	**External Configuration:** click to go to External Clock Configuration page.

Note: When connecting cables to any of the coaxial interfaces, TNC or SMA (e.g. GNSS, 1PPS), the coax cable connector should be properly screwed to the connector of the port to achieve best performance. However, caution should be used when connecting or removing these cables. Avoid applying excessive force doing so, to prevent port connector damage. It is recommended to perform these actions without any tools.

4.12 Spanning Tree

Spanning Tree Protocol was developed to protect Ethernet networks from the bad effects of network loops: a loop is a circular path in the network which causes frame storms that overloads the Ethernet network.

Spanning Tree Protocol creates a spanning tree within a mesh network of connected Ethernet bridges and disables the links which are not part of that tree, leaving a single active path between any two network nodes.

Note: Spanning Tree is available in all EdgeGM 7000 devices

Spanning Tree Versions:

- 802.1d Legacy Spanning Tree
- 802.1w Rapid Spanning Tree

Faster topology conversion by:

A faster method for temporary loop prevention: STP waits for the new topology to stabilize while RSTP makes the new root port forwarding immediately once all prior root ports have been made blocking, and then uses handshaking (on point-to-point links) to make designated ports forwarding as well.

Improvements in topology change detection, notification, and flushing of the learn tables.

- 802.1s Multiple-Instance Spanning Tree

A newer version supporting more than a single topology: each instance (group of VLANs) can have its own topology.

4.12.1 Understanding RSTP and MSTP

STP provides basic loop prevention functionality with slow network convergence when topology changes occur.

RSTP converges faster because a handshake mechanism is deployed, based on P2P links instead of the timer-based process used by STP.

Under RTSP, port assignments change through exchanged messages RSTP device generates configuration messages once every hello time interval.

An RTSP device will respond to BPDUs sent from the root bridge. The RSTP device will propose its spanning tree information to its designated ports.

If another RSTP device receives this information and determines that this is the superior root information, it starts a synchronizing operation to ensure all its ports are in sync with the new information. This device may send an “agreement” to the first RSTP device confirming its superior spanning tree information.

The first RSTP device, upon receiving this agreement, knows now that it can rapidly change that port to the forwarding state.

Similar proposal agreement handshake messages propagate within the network, restoring the connectivity very quickly after a topology change, bypassing the traditional listening/learning state transition process.

Therefore, a cascading effect is created away from the RSTP root where each designated port proposes to its neighbors to determine if a rapid transition is possible. In this way RSTP achieves faster convergence times than STP.

RSTP device port roles:

Root – A forwarding port that is the best port from no root-bridge to Root bridge.

Designated –A forwarding port for every LAN segment.

Alternate – An alternate port to the root bridge.

Disabled – A network administrator can manually disable a port.

Backup – provides an alternate designated port.

4.12.1.1 Understanding MSTP

RSTP does not solve the problem inherent in STP: all VLANs within a LAN must share the same spanning tree topology. An STP or RSTP network has only one spanning tree instance for the entire network and includes all VLANs in the network. EdgeGM 7000 switches utilize the Multiple Spanning Tree protocol (MSTP, 802.1s) to ensure that only one active path exists between any two nodes in a spanning tree instance. An instance includes a unique set of VLANs, belongs to a specific spanning tree region and creates a separate per instance forwarding topology.

A region may comprise multiple spanning tree instances (each with a different set of VLANs). Each spanning tree instance is independent of other instances. Each region can support up to 16 spanning tree instances.

MSTP region: a group of interconnected switches that share the same attributes is defined as an MST region. An MST region includes multiple spanning tree instances (MSTI) which provide different paths for different VLAN. Each MSTI can have its own independent topology. Note that MSTP recognizes an STP or RSTP LAN as a distinct spanning tree region.

A region can include two types of STP instances:

- Internal Spanning Tree Instance (IST instance). This is the default spanning tree instance in any MST region. IST provides the root switch for the region and by default comprises all VLANs in the region except those VLANs assigned to MSTI.
- Multiple Spanning Tree Instance (MSTI). This type of configurable STP instance includes assigned VLANs which operate as part of the same single spanning tree topology. IST instance is defined as Instance 0 whereas all other MST instances are numbered from 1 to 15.
- All MST instances within the same region share the same protocol timers, each MST instance has its own topology Parameters, such root switch ID, root path cost and additional selected Parameters.

4.12.2 Common and Internal Spanning Tree (CSTI):

CSTI is a collection of the IST in each region and the Common Spanning Tree (CST) which interconnects the various MST regions and STP LANs, and RSTP LANs in a switched network.

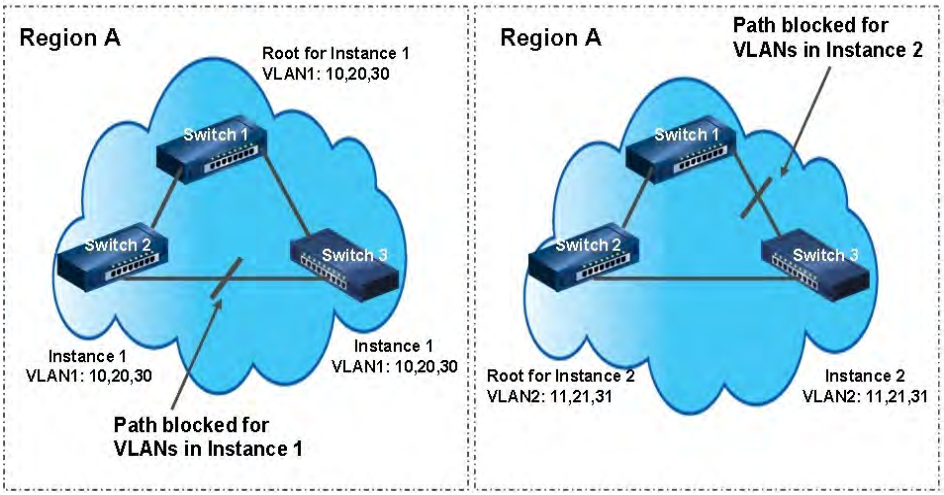
The CIST is created as a result of the STP algorithm running between switches that support the 802.1w, and the 802.ID protocols. MSTP allows for rapid port state transition just like RSTP. MSTP is compatible to STP and RSTP.

4.12.3 Example of a Multiple Spanning Tree Application

Assume we have tree switches in a region configured with VLANs grouped in two instances, as follows:

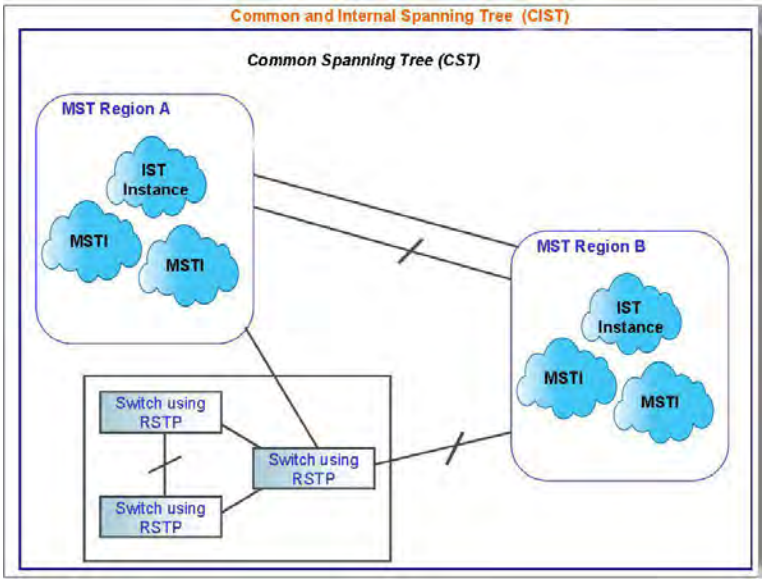
VLAN1 (10, 20, 30) mapped to Instance 1; VLAN2 (11, 21, 31) mapped to Instance 2. The logical topologies shown in the below drawing are the result from these VLAN/Instance grouping resulting on different blocked links for different VLANs as shown.

The MSTP configuration commands operate exactly like RSTP commands and MSTP is compatible with the RSTP and STP enable switches in our network.



MSTP Network

MSTP interconnects between various MST regions and maps active and separate paths through separate spanning tree instances. The below drawing depicts an MSTP network MSTP distinguish an STP or RSTP LAN as a distinct separate STP region.



4.12.4 Bridge settings

Spanning Tree protocol version (STP, RSTP or MSTP) is selected according to the networking environment. EdgeGM 7000 devices allows STP, RSTP, MSTP system settings configuration as detailed below.

Web GUI: Configuration > Advanced > L2 & Switching > Spanning Tree > Bridge Settings

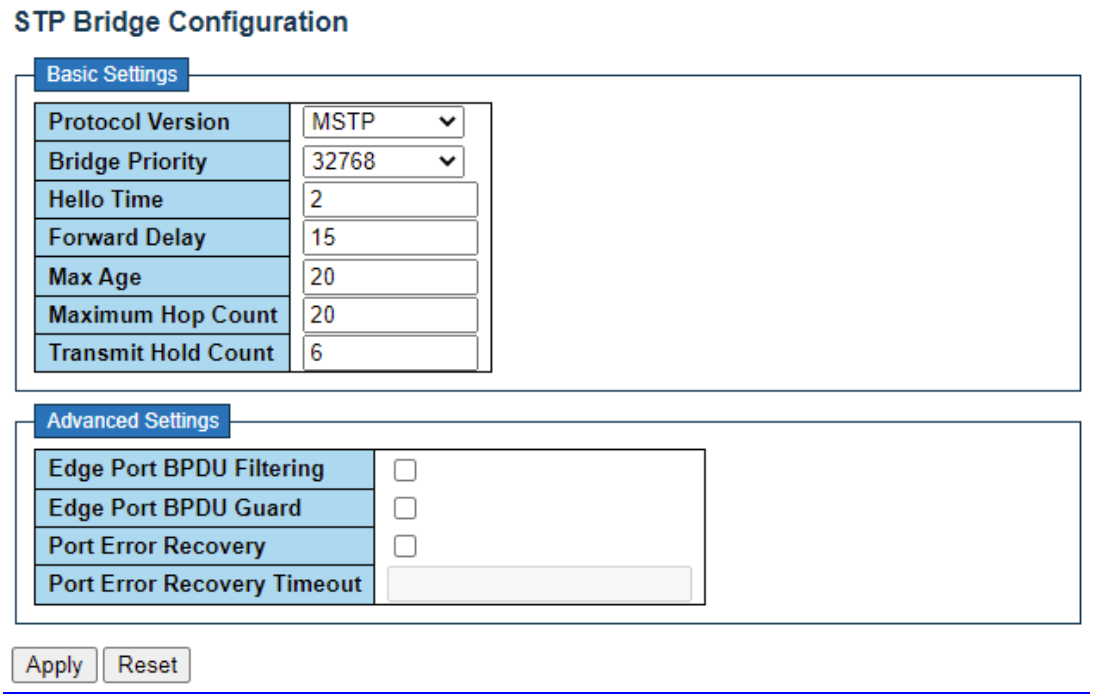


Figure 4-113: STP Bridge Configuration

Table 4-102: STP Bridge Configuration Parameters

Basic Settings	
Protocol version	The MSTP / RSTP / STP protocol version setting. Valid values are **STP**, **RSTP** and **MSTP**.
Bridge Priority	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.
Hello Time	The interval between sending STP BPDU's. Valid values are in the range 1 to 10 seconds, default is 2 seconds. *Note: Changing this parameter from the default value is not recommended and may have adverse effects on your network.*
Forward Delay	The delay used by STP Bridges to transition Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

Max Age	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, *and* Max Age must be <= (FwdDelay-1) *2.
Maximum Hop Count	This defines the initial value of remaining Hops for MSTI information generated at the boundary of a MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.
Transmit Hold Count	The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.
Advanced Settings	
Edge Port BDPU Filtering	Controls 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 must be disabled and re-enabled for normal STP operation. This condition is also cleared by a system reboot.
Port Error Recovery Timeout	The time that must pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

4.12.5 MSTI Configuration

This section allows the user to inspect and change the current STP MSTI bridge instance (group of VLANs) priority configurations.

Add VLANs separated by spaces or comma.

Web GUI: Configuration > Advanced > L2 & Switching > Spanning Tree > MSTI Mapping

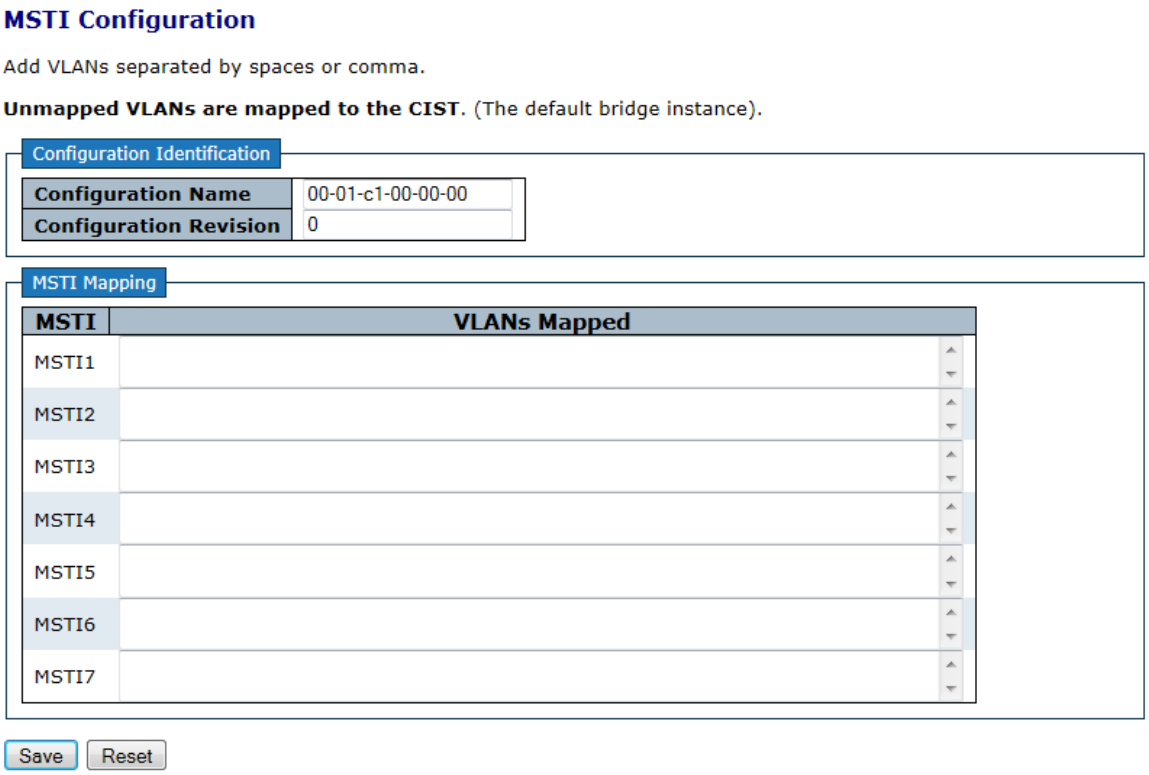


Figure 4-114: MSTI Configuration

Table 4-103: MSTI Configuration Parameters

Configuration Identification	
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	
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 can be given as a single (xx, xx being between 1 and 4094) VLAN, or a range (xx-yy), each of which must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e., not having any VLANs mapped to it.) Example: 2,5,20-40.

4.12.6 MSTI Priority Configuration

The user is allowed to inspect the current STP MSTP bridge instance priority configurations and possibly change them as well

Web GUI: Configuration > Advanced > L2 & Switching > Spanning Tree > MSTI Mapping

Figure 4-115: STP MSTI Priority Configuration.

Table 4-104: STP MSTI Priority Configuration Parameters

MSTI	The bridge instance (group of VLANs). The CIST is the *default* instance, which is always active.
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.**

4.12.7 CIST Port Configuration

The user is allowed to inspect the current STP CIST port configurations, and possibly change them as well. This section contains settings **for physical and aggregated ports**.

Web GUI: Configuration > Advanced > L2 & Switching > Spanning Tree > CIST Ports

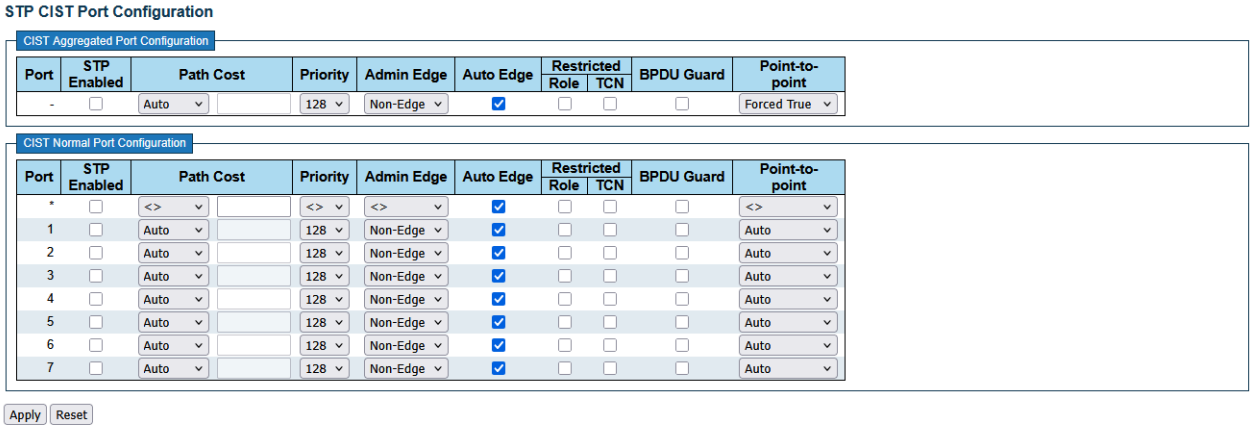


Figure 4-116: CIST Port Configuration displays

Table 4-105: CIST Port Configuration displays Parameters

CIST Aggregated and Normal Port Configurations	
Port	The switch port number of the logical STP port.
STP Enabled	Controls whether STP is enabled on this switch port.
Path Cost	Controls the path cost incurred by the port. The **Auto** setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the **Specific** setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in 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).
OperEdge (state flag)	Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transitioning to the forwarding state is faster for edge ports (having *operEdge* true) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in **Monitor**->**Spanning Tree** -> **STP Detailed Bridge Status**.
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.

CIST Aggregated and Normal Port Configurations	
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 influencing 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 trees active topology as a result of persistent incorrectly 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 is the physical link state for the attached LANs changing 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 affect this setting. A port entering error-disabled state due to this setting is subject to the bridge **Port Error Recovery** setting as well, located at STP Bridge Setting
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. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

4.12.8 MSTI Port Configuration

This section 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.**

By clicking on **Get** we get the below display for the selected MSTI.

Web GUI: Configuration > Advanced > L2 & Switching > Spanning Tree > MSTI Ports

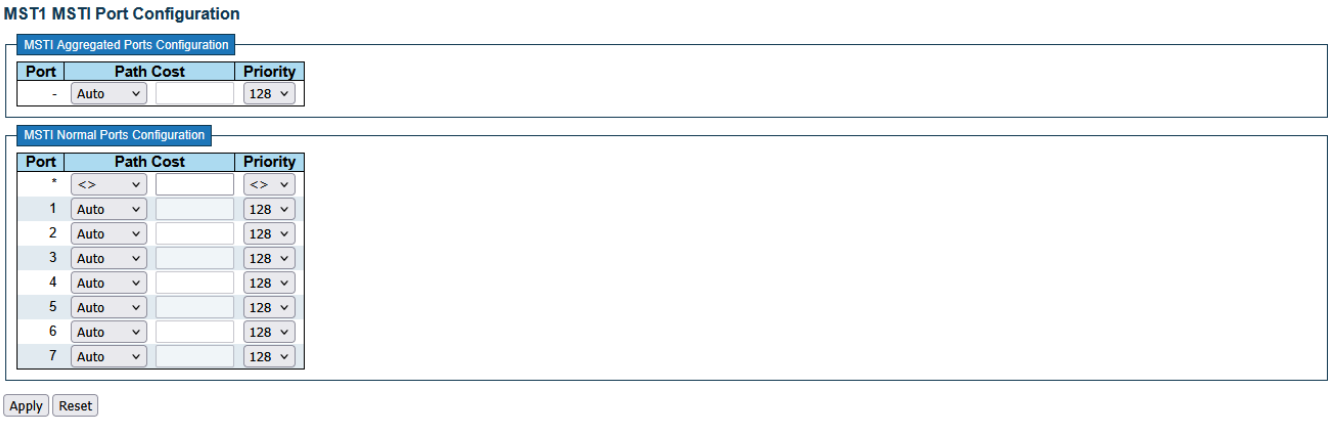


Figure 4-117: MSTI Port Configuration

Table 4-106: MSTI Port Configuration Parameters

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. (See above). Lower priority is better.
Buttons	**Get**: Click to retrieve settings for a specific MSTI.

4.12.9 Spanning Tree Monitoring

This section provides various STP monitoring displays.

4.12.9.1 STP Bridges Status

This display provides a status overview of all STP bridge instances.

Web GUI: Monitor > Advanced > L2 & Switching > Spanning Tree > Bridge Status

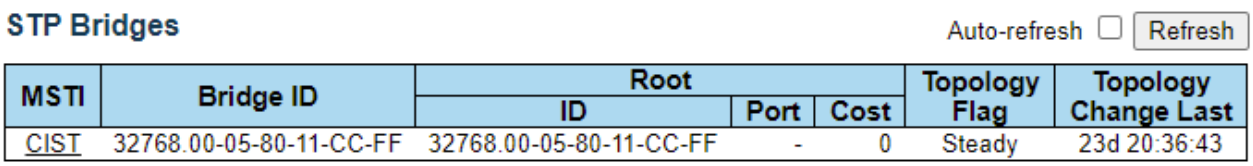


Figure 4-118: STP Bridges

Table 4-107: STP Bridges Parameters

MSTI	The Bridge Instance. CIST 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 it 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 of this Bridge instance.
Topology Change Last	The time since last Topology Change occurred.

By clicking on CIST on above display, an additional display is shown below (STP Detailed Bridge Status). This display provides detailed information on a single STP bridge instance, along with port state for all active associated ports. Refer to next sub-section for more details.

4.12.9.2 STP Detailed Bridge Status

This section provides detailed information on a single **STP** bridge instance, along with port state for all active ports associated.

Web GUI: Monitor > Advanced > L2 & Switching > Spanning Tree > Bridge Status | CIST

STP Detailed Bridge Status

STP Bridge Status	
Bridge Instance	CIST
Bridge ID	32768.00-05-80-08-87-AA
Root ID	32768.00-05-80-08-87-AA
Root Cost	0
Root Port	-
Regional Root	32768.00-05-80-08-87-AA
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	0
Topology Change Last	-

CIST Ports & Aggregations State

Port	Port ID	Role	State	Path Cost	Edge	Point-to-Point	Uptime
No ports or aggregations active							

Figure 4-119: STP Detailed Bridge Status

Table 4-108: STP Detailed Bridge Status Parameters

STP Bridge Status	
Bridge Instance	The Bridge instance -**CIST**, **MSTI**...
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 it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge
Regional Root	The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge. *(For the CIST instance only)*.
Internal Root Cost	The Regional Root Path Cost. For the Regional Root Bridge this is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge. *(For the CIST instance only)*.
Topology Flag	The current state of the Topology Change Flag of this Bridge instance.
Topology Change Count	The number of times where the topology change flag has been set (during a one-second interval).
Topology Change Last	The time passed since last Topology Flag was last set
CIST Ports & Aggregations State	
Port	The switch port number of the logical STP port
Port ID	The port id as used by the STP protocol. This is the priority part and the logical port index of the bridge port.
Role	The current STP port role. The port role can be one of the following values: **Alternate Port** **BackupPortRootPort** **Designated Port**
State	The current STP port state. The port state can be one of the following values: **Discarding** **Learning** **Forwarding**
Path Cost	The current STP port path cost. This will either be a value computed from the **Auto** setting, or any explicitly configured value
Edge	The current STP port (operational) Edge Flag. An Edge Port is a switch port to which no Bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transits directly to the Forwarding Port State, since there is no possibility of it participating in a loop.

Point-to-Point	The current STP port point-to-point flag. A point-to-point port connects to a non-shared LAN media. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transit to STP state.
Uptime	The time since the bridge port was last initialized.

4.12.9.3 STP Port Status

This section displays the STP CIST port status for physical ports switch.

Web GUI: Monitor > Advanced > L2 & Switching > Spanning Tree > Port Status

STP Port Status

Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Forwarding	-

Figure 4-120: STP Port Status

Table 4-109: STP Port Status Parameters

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

4.12.9.4 STP Port Statistics

This page displays the STP port statistics counters of bridge ports in the switch.

Web GUI: Monitor > Advanced > L2 & Switching > Spanning Tree > Port Statistics

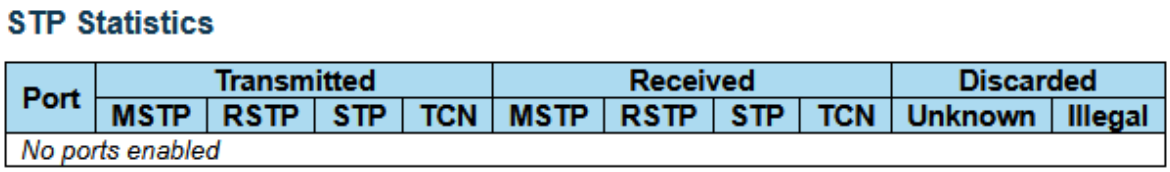


Figure 4-121: STP Statistics

Table 4-110: STP Statistics Parameters

Port	The switch port number of the logical STP port.
MSTP	The number of MSTP BPDU's received/transmitted on the port.
RSTP	The number of RSTP 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.

4.13 IP Multicast

Multicast is the delivery of information to a group of destinations simultaneously using the most efficient strategy to deliver the messages over each link of the network only once, creating copies only when the links to the destinations split.

Internet Group Management Protocol (IGMP) is an IP (Layer 3) protocol used for signaling of multicast group membership (adding or removing clients to/from a multicast group).

IGMP snooping analyze all IGMP packets between hosts connected to the EdgeGM 7000 and multicast routers in the network. When the EdgeGM 7000 snoops an IGMP Join or IGMP Report from a host for a given multicast group, it adds the host's port number to the multicast list for that group. When the EdgeGM 7000 snoops an IGMP Leave, it removes the host's port from the table entry.

The following sections explain and demonstrate in detail IGMP snooping support using the Web screens description.

4.13.1 IGMP Snooping Configuration

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.

IPMC is an acronym for **IP** **M**ulti**C**ast.

IPMC supports IPv4 and IPv6 multicasting. IPMCv4 denotes multicast for IPv4. IPMCv6 denotes multicast for IPv6.

This section enables IGMP Snooping related configuration.

Web GUI: Configuration > Advanced > L2 & Switching > IP & Routing > IPMC > IGMP Snooping > Basic Configuration

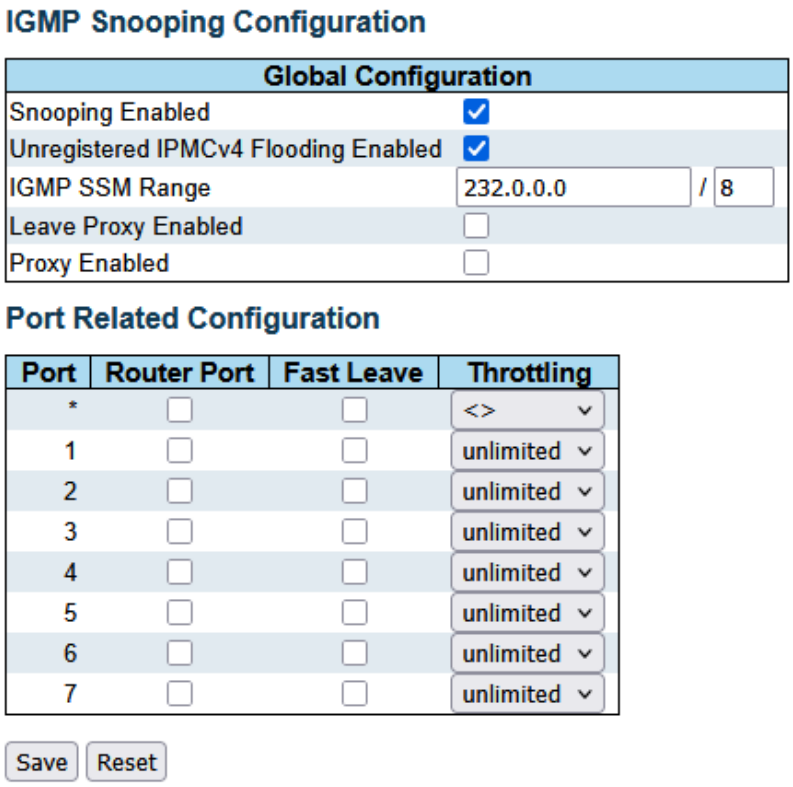


Figure 4-122: IGMP Snooping Configurations

Table 4-111: IGMP Snooping Configuration Parameters

Global Configuration	
Snooping Enabled	Enables the Global IGMP Snooping.
Unregistered IPMCv4 Flooding enabled	Enables 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 despite 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 Enabled	Enables IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
Proxy Enabled	Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.
Port Related Configuration	
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast Leave	Enables the fast leave on the port. Multicast 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. This processing applies to IGMP and MLD.
Throttling	Enable to limit the number of multicast groups to which a switch port can belong.

4.13.2 IGMP Snooping VLAN Configuration

Navigating the IGMP Snooping VLAN Table

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. Clicking the **Refresh** button will update the displayed table starting from that or the next closest VLAN Table match.

The **>>** will use the last entry of the currently displayed entry 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.

Web GUI: Configuration > Advanced > L2 & Switching > IP & Routing > IPMC > IGMP Snooping > VLAN Configuration

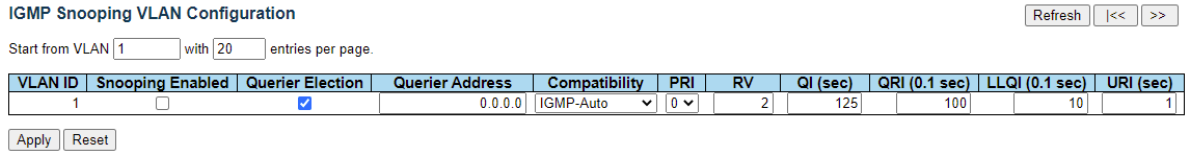


Figure 4-123: IGMP Snooping VLAN Configuration

Table 4-112: IGMP Snooping VLAN Configuration Parameters

VLAN ID	The VLAN ID of the entry.
Snooping Enabled	Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.
Querier Election	Enable to join IGMP Querier election in the VLAN. A router sends IGMP Query messages onto a particular link. This router is called the 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	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 Maximum Response Delay used to calculate the Maximum Response 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	**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.

4.13.3 IGMP Snooping Port Group Filtering Configuration

Web GUI: Configuration > Advanced > L2 & Switching > IP & Routing > IPMC > IGMP Snooping > Port Filtering Profile

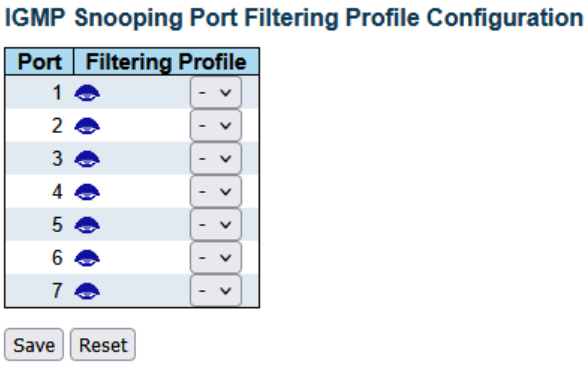


Figure 4-124: IGMP Snooping Port Group Filtering Configuration

Table 4-113: IGMP Snooping Port Group Filtering Configuration Parameters

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. IP Multicast Profile is an acronym for **IP MultiCast** Profile. IP Multicast Profile is used to deploy the access control on IP multicast streams.
Profile Management Button	You can inspect the rules of the designated profile by using the following button:  : List the rules associated with the designated profile.

4.13.4 IGMP Snooping Status

This section provides IGMP Snooping status.

Web GUI: Monitoring > Advanced > L2 & Switching > IPMC > IGMP Snooping > Status

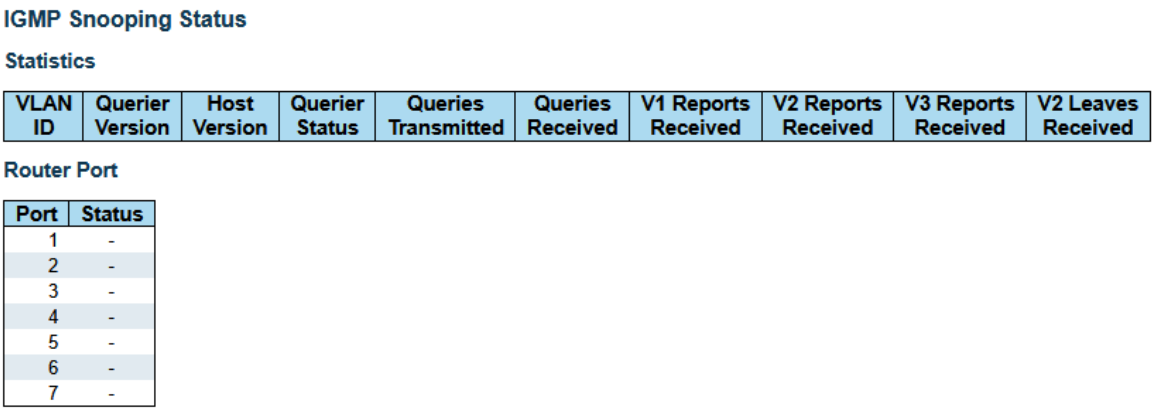


Figure 4-125: IGMP Snooping Status

Table 4-114: IGMP Snooping Status Parameters

Statistics	
VLAN ID	The VLAN ID of the entry.
Querier Version	Currently Working Querier Version.
Host Version	Currently Working Host Version.
Querier Status	Shows the Querier status is "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.
Querier Transmitted	The number of Transmitted Queries.
Querier Received	The number of Received Queries.
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 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 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.

4.13.5 IGMP Snooping Groups Information

Entries in the IGMP Group Table are shown on this section. The IGMP Group Table is sorted first by VLAN ID, and then by group.

Navigating the IGMP Group Table

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. Clicking the **Refresh** button will update the displayed table starting from that or the closest next IGMP Group Table match. In addition, the two input fields will – upon a 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 table 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.

Web GUI: Configuration > Advanced > IP & Routing > IPMC > IGMP Snooping > Groups Information

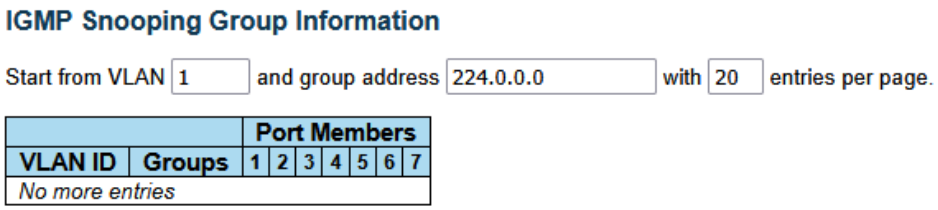


Figure 4-126: IGMP Snooping Groups Information

Table 4-115: IGMP Snooping Groups Parameters

VLAN ID	VLAN ID of the group.
Groups	Group address of the group displayed.
Port Members	Ports under this group.

4.13.6 IGMP SFM Information

Entries in the IGMP SFM Information Table are shown on this section. The IGMP 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 belonging to the same group are treated as single entry.

Navigating the IGMP SFM Information Table

Each page shows up to 99 entries from the IGMP 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 IGMP SFM Information Table. The "Start from VLAN", and "group" input fields allow the user to select the starting point in the IGMP SFM Information Table. Clicking **Refresh** the button will update the displayed table starting from that or the closest next IGMP SFM Information Table match. In addition, the two input fields will - upon a 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 table 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**.**

Web GUI: Configuration > Advanced > IP & Routing > IPMC > IGMP Snooping > IPv4 SFM Information

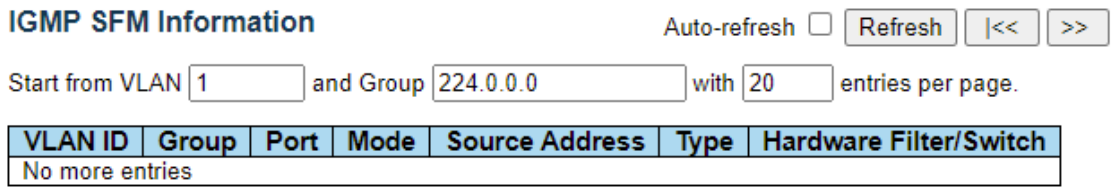


Figure 4-127: IGMP SFM Information

Table 4-116: IGMP SFM Information Parameters

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 IPv4 source addresses for filtering (per group) is 8. 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 address could be handled by chip or not.

4.13.7 MLD Snooping Configuration

This section provides MLD Snooping related configuration.

MLD is an acronym for Multicast Listener Discovery 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.

Web GUI: Configuration > Advanced > IP & Routing > IPMC > IPMC > MLD Snooping > Basic Configuration

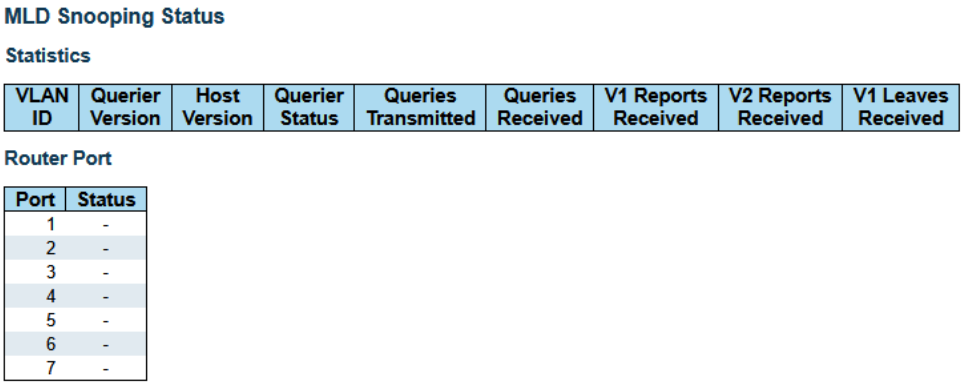


Figure 4-128: MLD Snooping Configurations

Table 4-117: MLD Snooping Configurations Parameters

MLD Snooping Configuration	
Snooping Enabled	Enables the Global MLD Snooping.
Unregistered IPMCv6 Flooding enabled	Enables 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 despite 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 Enabled	Enables MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
Proxy Enabled	Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Port Related Configuration	
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast Leave	Enable the fast leave on the port. System will remove group record and stop forwarding data upon receiving the MLDv1 leave message without sending last member query messages. It is recommended to enable this feature only when a single MLDv1 host is connected to the specific port.
Throttling	Enable to limit the number of multicast groups to which a switch port can belong.

4.13.8 MLD Snooping VLAN Configuration

Navigating the MLD Snooping VLAN Table

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. Clicking the **Refresh** button will update the displayed table starting from that or the next closest VLAN Table match.

The **>>** will use the last entry of the currently displayed entry 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.

Web GUI: Configuration > Advanced > IP & Routing > IPMC > MLD Snooping > VLAN Configuration

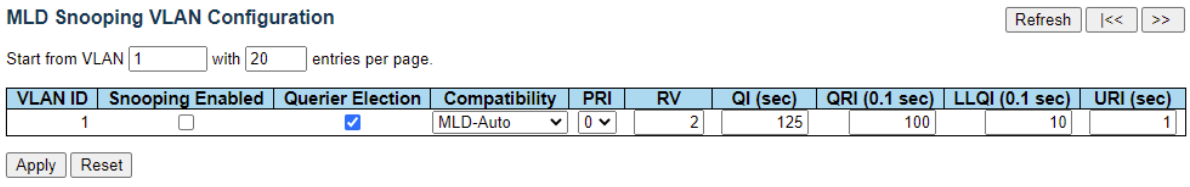


Figure 4-129: MLD Snooping VLAN Configurations

Table 4-118: MLD Snooping VLAN Configuration Parameters

VLAN ID	The VLAN ID of the entry.
MLD Snooping Enabled	Enable the per-VLAN MLD Snooping. Up to **511** VLANs can be selected for MLD Snooping.
Querier Election	Enable the 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 MLD v1, Forced MLD v2.** Default compatibility value is **MLD-Auto**.
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 LINK. 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 Maximum Response Delay used to calculate the Maximum Response 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	**Last Listener Query Interval**. The Last Listener Query Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages. The allowed range is **0** to **31744** in tenths of seconds, default last listener 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 node's initial report of interest in a multicast address. The allowed range is **0** to **31744** seconds, default unsolicited report interval is 1 second.

Web GUI: Configuration > Advanced > IP & Routing > IPMC > MLD Snooping > Port Filtering Profile

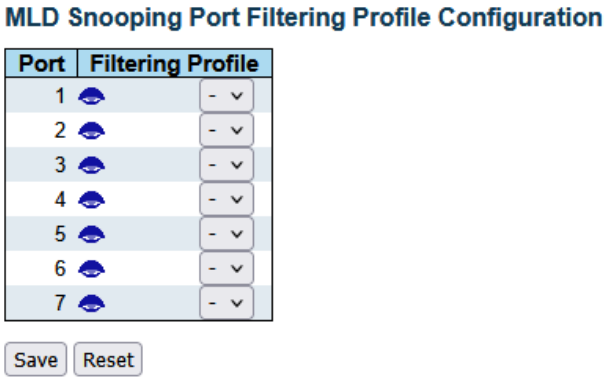


Figure 4-130: MLD Snooping Port Group Filtering Configuration

Table 4-119: MLD Snooping Port Group Filtering Configuration Parameters

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.
Profile Management Button	You can inspect the rules of the designated profile by using the following button: : List the rules associated with the designated profile.

4.13.9 MLD Snooping Status

This section provides MLD Snooping status.

Web GUI: Configuration > Advanced > IP & Routing > IPMC > MLD Snooping > VLAN Configuration

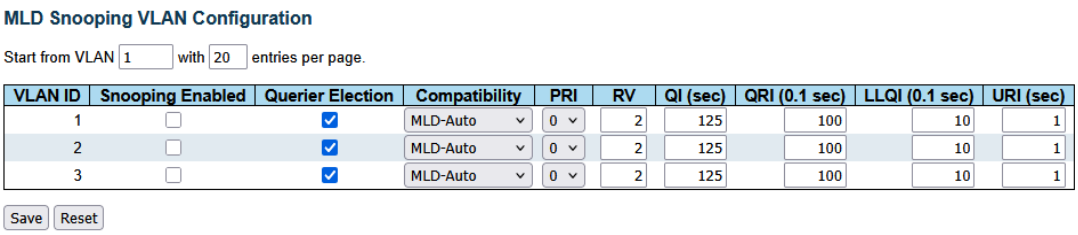


Figure 4-131: MLD Snooping Port Group Filtering Configuration

Table 4-120 MLD Snooping Status Parameters

Statistics	
VLAN ID	The VLAN ID of the entry.
Querier Version	Working Querier Version.
Host Version	Working Host Version.
Querier Status	Shows the Querier status is **ACTIVE** or **IDLE**. **DISABLE** denotes the specific interface is administratively disabled.
Querier Transmitted	The number of Transmitted Queries.
Querier Received	The number of Received Queries.
V1 Reports Received	The number of Received V1 Reports.
V2 Reports Received	The number of Received V2 Reports.
V1 Leaves Receive	The number of Received V1 Reports.
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	Indicate whether specific port is a router port or not.

4.13.10 MLD Snooping Groups Information

Entries in the MLD Group Table are shown on this section

Navigating the MLD Group Table.

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. Clicking the Refresh button will update the displayed table starting from that or the closest next MLD Group 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 table 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.

Web GUI: Monitor > Advanced > IPMC > MLD Snooping > Group Information

Figure 4-132: MLD Snooping Groups Information.

Table 4-121: MLD Snooping Groups Information Parameters

VLAN ID	VLAN ID of the group.
Groups	Group address of the group displayed.
Port Members	Ports under this group.

4.13.11 MLD 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.

Navigating the MLD SFM Information Table

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. Clicking the Refresh button will update the displayed table starting from that or the closest next MLD SFM Information 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 table 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.

Web GUI: Configuration > Advanced > L2 & Switching > IPMC > MLD Snooping > IPv6 SFM Information

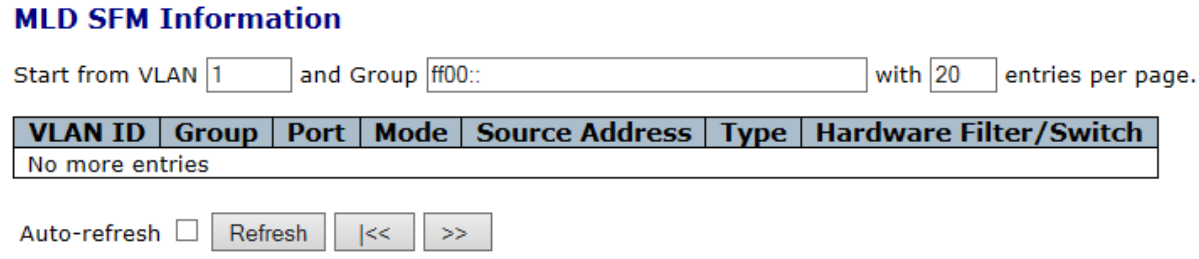


Figure 4-133: MLD SFM Information

Table 4-122: MLD SFM Information Parameters

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 IPv6 source addresses for filtering (per group) is 8.
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.

4.14 Link Aggregation

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.

Link aggregation bundles multiple ports (member ports) together into a single logical link. It is primarily used to increase available bandwidth without introducing loops in the network and to improve resiliency against faults. A link aggregation group (LAG) can be established with individual links being added or removed. This enables bandwidth to be incrementally scaled based on changing requirements. A link aggregation group can be quickly reconfigured if faults are identified.

Link aggregation (or IEEE 802.3ad) uses multiple Ethernet network links/ports in parallel to increase the link speed beyond the limits of any one single port, and to increase the redundancy for higher availability.

Two switches directly connected over several links can negotiate as to which ports should be selected as active members of an aggregation group.

A group of ports is selected to belong to a specific group ID (trunk) in order to generate an aggregated link.

Typically, the ports used in an aggregated link should be of the same type.

Link aggregation configuration is performed in two variants.

- Static – This mode is used to manually select the ports of the group.
- Link Aggregation Control Protocol (LACP) – In this mode two switches which are directly connected over several physical links, can negotiate which ports should be selected as active members of a group.

LACP works by sending frames (LACPDUs) down all links which have the protocol enabled. If it finds a device on the other end of the link which has also the LACP enabled, it

will also independently send frames along the same links enabling the two devices to detect multiple links between themselves and the combine them into a single logical link.

4.14.1 Common Aggregation Configuration

The aggregation hash code contributor settings are global (hashes are calculated when the first connection is established and then kept in the device memory for the session lifetime).

Web GUI: Configuration > Advanced > L2 & Switching > Aggregation > Common

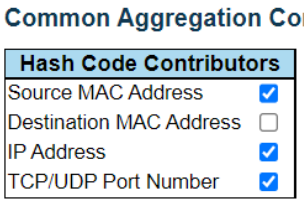


Figure 4-134: Common Aggregation Configuration

Table 4-123: Common Aggregation Configuration Parameters

Aggregation Mode Configuration	
Hash Code Contributors	
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	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 port number or uncheck to disable. By default, the port number is “Enabled”.

4.14.2 Aggregation Group and Mode Configuration

EdgeGM 7000 allows set up of the Aggregation Mode Configuration and the Aggregation Group.

This section is used to configure the Aggregation hash mode and the aggregation group.

Web GUI: Configuration > Advanced > Aggregation > Groups

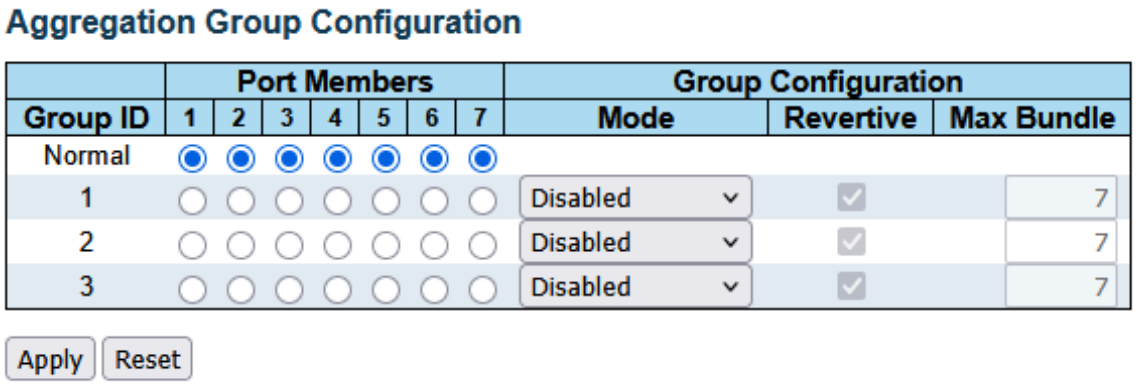


Figure 4-135: Aggregation Group and Mode Configuration

Aggregation Group Configuration	
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. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.
Mode	This parameter determines the mode for the aggregation group. • **Disabled**: The group is disabled. • **Static**: The group operates in static aggregation mode. • **LACP** (**Active**): The group operates in LACP active aggregation mode. See IEEE 801.AX-2014, section 6.4.1 for details. • **LACP** (**Passive**): The group operates in LACP passive aggregation mode. See IEEE 801.AX-2014, section 6.4.1 for details.
Revertive	This parameter only applies to LACP-enabled groups. It determines if the group will perform automatic link (re-)calculation when links with higher priority becomes available.
Max Bundle	This parameter only applies to LACP-enabled groups. It determines the maximum number of active bundled LACP ports allowed in an aggregation.

4.14.3 LACP Configuration

Web GUI: Configuration > Advanced > Aggregation > LACP

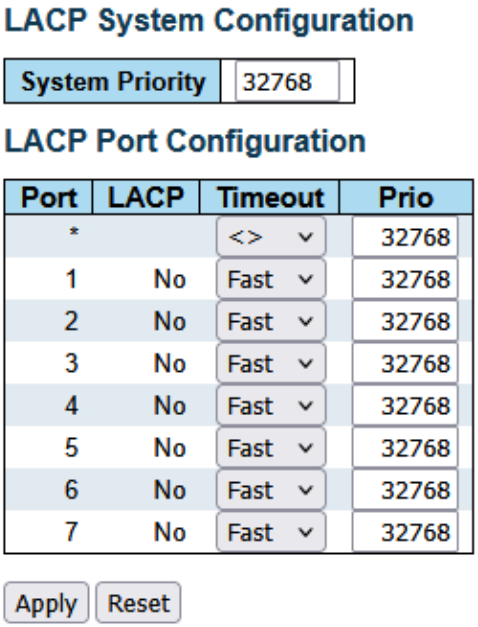


Figure 4-136: LACP Configuration

Table 4-124: LACP Port Parameters

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

4.14.4 Aggregation Status

Web GUI: Monitor > Advanced > Aggregation > Status

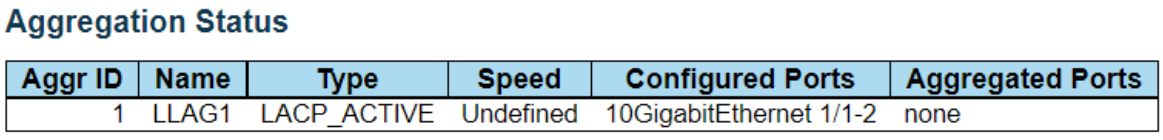


Figure 4-137: Aggregation Status

Table 4-125: Aggregation Status Parameters

Aggregation Status	
Aggr ID	The Aggregation ID associated with this aggregation instance.
Name	Name of the Aggregation group ID.
Type	Type of the Aggregation group (Static or LACP).
Speed	Speed of the Aggregation group.
Configured ports	Configured member ports of the Aggregation group.
Aggregated ports	Aggregated member ports of the Aggregation group.

4.14.5 LACP Monitoring

4.14.5.1 System Status

Web GUI: Monitor > Advanced > Aggregation > LACP > System Status

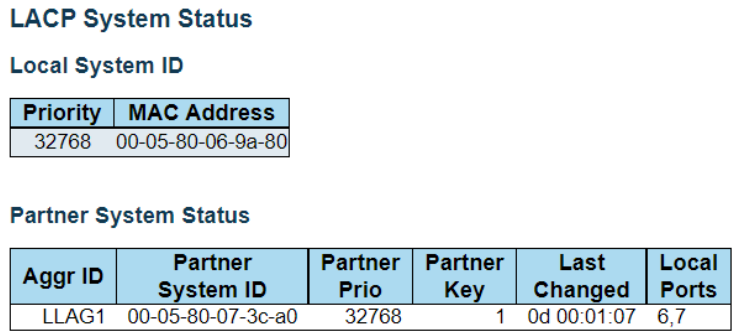


Figure 4-138: LACP System Status

Table 4-126: LACP System ID

Local System ID
This table display both the local system priority and the local system MAC address which forms the local LACP System ID.

Table 4-127: Partner System Status Parameters

Partner System Status	
This table display the partner system information for each LACP aggregation group.	
Aggr ID	The Aggregation ID associated with this aggregation instance.
Partner System ID	The system ID (MAC address) of the aggregation partner.
Partner Prio	The priority that the partner has assigned to this aggregation ID.

Partner Key	The Key that the partner has assigned to this aggregation ID.
Last changed	The time since this aggregation changed.
Local Ports	Shows which ports are a part of this aggregation for this switch.

4.14.5.2 Internal Status

Web GUI: Monitor > Advanced > Aggregation > LACP > Internal Status

LACP Internal Port Status

Port	State	Key	Priority	Activity	Timeout	Aggregation	Synchronization	Collecting	Distributing	Defaulted	Expired
6	Active	1	32768	Active	Fast	Yes	Yes	Yes	Yes	No	No
7	Active	1	32768	Active	Fast	Yes	Yes	Yes	Yes	No	No

Figure 4-139: LACP Internal Status

Table 4-128: LACP Internal Status Parameters

Internal Status	
This page provides a status overview for the LACP internal (i.e. local system) status for all ports. Only ports that are part of an LACP group are shown. For details on the shown parameters please refer to IEEE 801.AX-2014.	
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 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.

4.14.5.3 Neighbor Status

Web GUI: Monitor > Advanced > Aggregation > LACP > Neighbor Status

LACP Neighbor Port Status

Port	State	Aggr ID	Partner Key	Partner Port	Partner Port Prio	Activity	Timeout	Aggregation	Synchronization	Collecting	Distributing	Defaulted	Expired
6	Active	1	1	6	32768	Active	Fast	Yes	Yes	Yes	Yes	No	No
7	Active	1	1	7	32768	Active	Fast	Yes	Yes	Yes	Yes	No	No

Figure 4-140: LACP Neighbor Status

Table 4-129: LACP Neighbor Status Parameters

Neighbor Status	
This page provides a status overview for the LACP neighbor status for all ports. Only ports that are part of an LACP group are shown. For details on the shown parameters please refer to IEEE 801.AX-2014.	
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 Port	The partner port number associated with this link.
Partner Port 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 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.

4.14.5.4 Port Statistics

Web GUI: Monitor > Advanced > Aggregation > LACP > Neighbor Status

LACP Statistics

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
6	3282	3282	0	0
7	3281	3282	0	0

Figure 4-141: LACP Neighbor Status

Table 4-130: LACP Neighbor Status Parameters

Neighbor Status	
This page provides an overview for LACP statistics for all ports.	
Port	The switch port number.
LACP Received	Shows how many LACP frames have been received at each port.
LACP Transmitted	Shows how many LACP frames have been sent from each port.
Discarded	Shows how many unknown or illegal LACP frames have been discarded at each port.

4.15 LLDP-Link Discovery

LLDP is an IEEE 802.1ab standard protocol. The **L**ink **L**ayer **D**iscovery **P**rotocol is used for network discovery and works by having the units in the network exchanging information with their neighbors using LLDP frames.

Link discovery specifies a method and associated procedures that automatically discover transmission links and paths between network devices.

Unlike more traditional centralized polling techniques rooted in a management plane, autonomous link discovery procedures are rooted in and triggered by network elements composing the transport plane. As such, autonomous link discovery procedures may be event driven and executed in a coordinated, distributed fashion to automatically detect new

link connectivity associations and correlate link endpoint attributes between these network elements.

Once successful link correlations have been determined, autonomous notifications of these correlated link associations are sent to management elements and/or control elements residing in their respective management and control plane domains.

Link Layer Discovery Protocol (LLDP) is a media independent protocol allowing the LLDP agent to learn higher-level management reachability and connection and point information from neighboring devices. Each configured device is an active LLDP agent that sends periodic messages to all physical interfaces that listen for LLDP messages.

LLDP monitoring is implemented by collecting both LLDP neighbor information and LLDP statistics.

4.15.1 LLDP Configuration

This section allows the user to inspect and configure the current LLDP port settings.

Web GUI: Configuration > Advanced > L2 & Switching > LLDP > LLDP

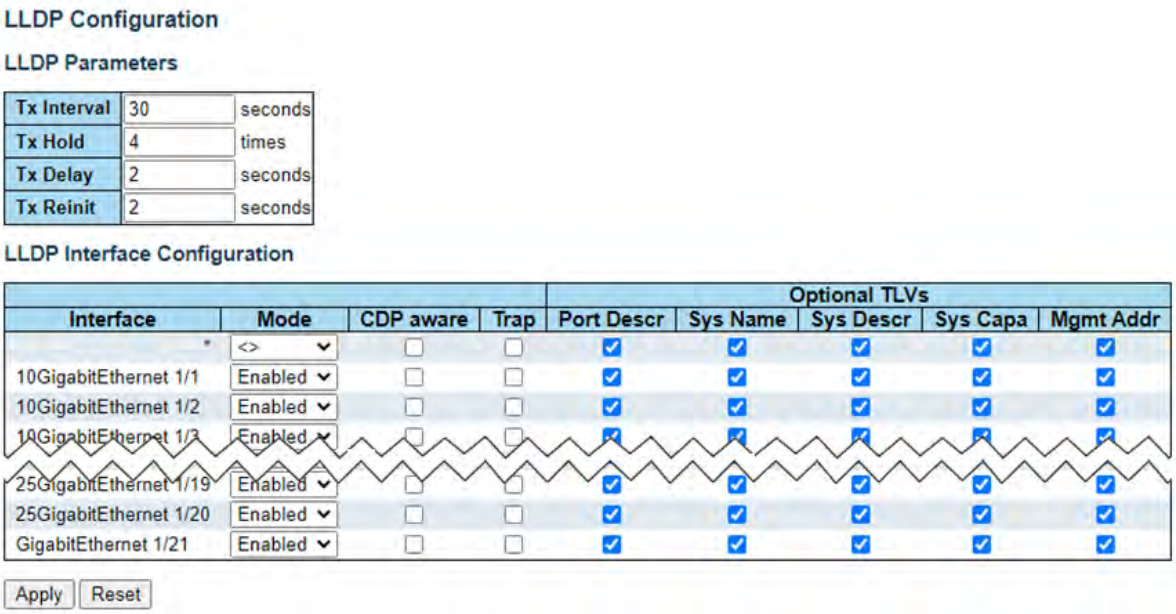


Figure 4-142: LLDP Configuration

Table 4-131: LLDP Configuration Parameters

LLDP Parameters	
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.
Tx Hold	Each LLDP frame contains information about the length of time 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.
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** in seconds. Tx Delay cannot be larger than a 1/4 of the **Tx Interval** value. Valid values are restricted to 1 - 8192 seconds.
Tx Reinit	When a port is disabled, LLDP is disabled or if the switch is rebooted, a LLDP shutdown frame is transmitted to the neighbor units for signaling that the LLDP information is not valid anymore. **Tx Reinit** controls the number of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 – 10 seconds.

LLDP Interface Configuration	
Interface	The switch interface name of the logical LLDP interface.
Mode	Select the 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 does not transmit CDP frames). CDP frames are only decoded if LLDP for the port is enabled. Only CDP TLVs that can be mapped into a corresponding field in the LLDP neighbors table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frame are not shown in the LLDP statistic). CDP TLVs are mapped into LLDP neighbors table as shown below. CDP TLV "Device ID" is mapped into the LLDP "Chassis ID" field. CDP TLV "Address" is mapped into the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors table. CDP TLV "Port ID" is mapped into the LLDP "Port ID" field. CDP TLV "Version and Platform" is mapped into the LLDP "System Description" field. Both the CDP and LLDP supports "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors table. If all ports have CDP awareness disabled, the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch. *Notes:* *When CDP awareness for a port is disabled the CDP information isn't removed immediately but will be removed when the hold time is exceeded. CDP is an acronym for Cisco Discovery Protocol.*

Optional TLVs	
TLV is an acronym for Type Length Value. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV.	
Port Descr	Optional TLV: When checked the "port description" is included in LLDP information transmitted.
Sys Name	Optional TLV: When checked the "system name" is included in LLDP information transmitted.
Sys Descr	Optional TLV: When checked the "system description" is included in LLDP information transmitted**.**
Sys Capa	Optional TLV: When checked the "system capability" is included in LLDP information transmitted**.**
Mgmt Addr	Optional TLV: When checked the "management address" is included in LLDP information transmitted.

4.15.2 LLDP Media Configuration

This section allows you to configure the LLDP-MED. This function applies to VoIP devices which support LLDP-MED.

Web GUI: Configuration > Advanced > L2 & Switching > LLDP > LLDP-MED

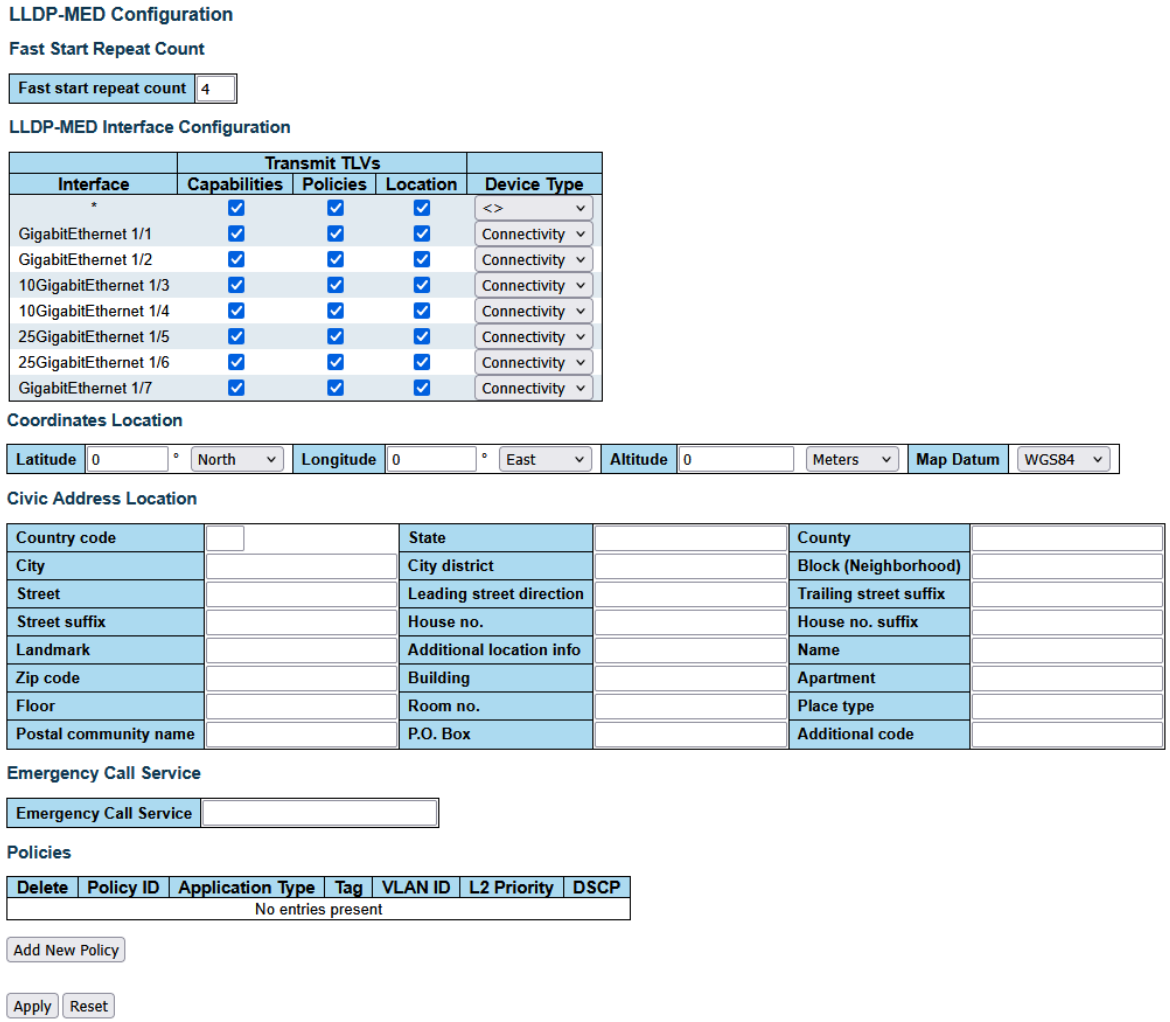


Figure 4-143: LLDP-MED Configuration displays

Table 4-132: LLDP MED Configuration Parameters

Fast start repeat count	
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. 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 neighbor has been detected in order share LLDP-MED information as fast as possible to new neighbors. Because there is a risk of an LLDP frame being lost during transmission between neighbors', it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbors' 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 Interface Configuration	
It is possible to select which LLDP-MED information that shall be transmitted to the neighbors. When the checkbox is checked the information is included in the frame transmitted to the neighbor.	
Interface	The port name to which the configuration applies.
Capabilities	When checked the switch's capabilities is included in LLDP-MED information transmitted.
Policies	When checked the configured policies for the interface is included in LLDP-MED information transmitted
Location	When checked the configured location information for the switch 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).
Coordinates Location	
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 -2097151.9 to 2097151.9 with a maximum of 1 digit. 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** is used for the coordinates given in these options: **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). The total number of characters for the combined civic address information must not exceed 250 characters. A couple of notes to the limitation of 250 characters. 1) A non-empty civic address location will use 2 extra characters in addition to the civic address location text. 2) The 2-letter country code is not part of the 250 characters limitation.	
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: Bank
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 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 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 Differentiated Services 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: • Voice • Guest Voice • Softphone Voice • Video Conferencing • Streaming Video • 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.	
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 interfaces

Application Type	Intended use of the application types: 1. **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. 2. **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. 3. **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. 4. **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. 5. **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. 6. **Video Conferencing** - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services. 7. **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. 8. **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 to **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.
Policies Interface 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.	
Interface	The interface number to which the configuration applies.
Policy Id	The set of policies that shall apply to a given port. The set of policies is selected by check marking the checkboxes that corresponds to the policies.

By clicking on “Add new policy” the following display is shown:

Web GUI: Monitor > Advanced > L2 & Switching > LLDP > LLDP-MED | New Policy

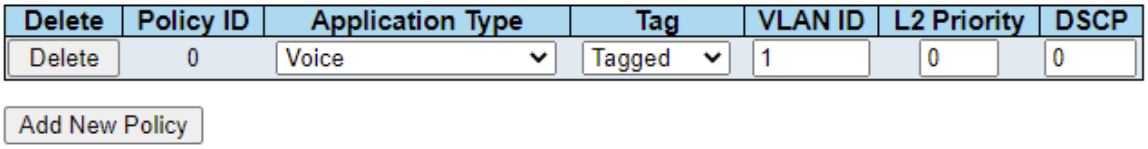


Figure 4-144: LLDP-MED Configuration displays

4.15.3 LLDP Monitoring

LLDP Monitoring is implemented by collecting:

- Neighbor
- LLDP-MED Neighbor
- EEE
- Port Statistics

4.15.3.1 Neighbors

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each interface on which an LLDP neighbor is detected. The columns hold the following information:

Web GUI: Monitor > Advanced > L2 & Switching > LLDP > Neighbors

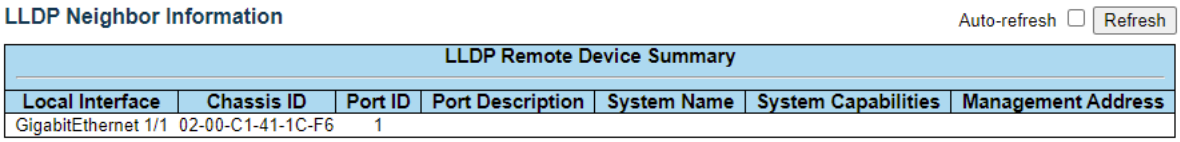


Figure 4-145: LLDP – Neighbor Information

Table 4-133: LLDP Neighbor Information Parameters

Local Interface	The interface 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 194 neighbor unit.
System Name	**System name** is the name advertised by the neighbor unit.
System Capabilities	Describes the 194 neighbor unit's capabilities. The possible capabilities are: • Other • Repeater • Bridge • WLAN Access Point • Router • Telephone • DOCSIS cable device • Station only • Reserved When a capability is "Enabled**"** – the capability is followed by (+). When a capability is "Disabled**"** – the capability is followed by (-).
Management Address	The neighbor unit's address used for higher layer entities to assist the discovery by the network management. This could for instance hold the neighbor's IP address.

4.15.3.2 LLDP-MED Neighbour

This section provides a status overview of all LLDP-MED neighbours. The displayed table contains a row for each port on which an LLDP neighbor is detected. This function applies to VoIP devices which support LLDP-MED. The columns hold the following information:

Web GUI: Monitor > Advanced > L2 & Switching > LLDP > LLDP-MED Neighbors

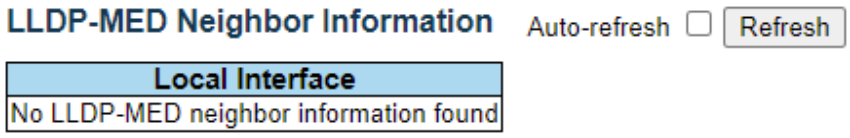


Figure 4-146: LLDP MED - Neighbour Information

Table 4-134: LLDP MED Neighbour Parameters

Interface	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: • LAN Switch/Router • IEEE 802.1 Bridge • IEEE 802.3 Repeater (included for historical reasons) • IEEE 802.11 Wireless Access Point • 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** LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework. 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. For-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: • LLDP-MED capabilities • Network Policy • Location Identification • Extended Power via MDI – PSE • Extended Power via MDI – PD • Inventory • 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 signalling 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 indicative of 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 the 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.

4.15.3.3 EEE

By using EEE power savings can be achieved at the expense of traffic latency. This latency occurs due to that the circuits EEE turn off to save power, need time to boot up before sending traffic over the link. This time is called "wakeup time". To achieve minimal latency, devices can use LLDP to exchange information about their respective tx and rx "wakeup time ", as a way to agree upon the minimum wakeup time they need.

EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az. This page provides an overview of EEE information exchanged by LLDP.

Web GUI: Monitor > Advanced > L2 & Switching > LLDP > LLDP-MED Neighbors > EEE

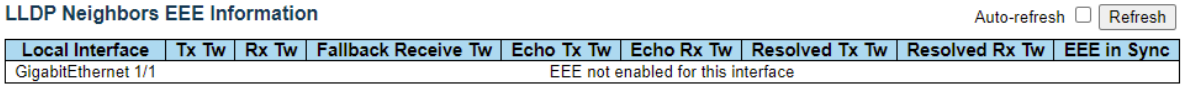


Figure 4-147: LLDP Neighbors EEE Information

Table 4-135: LLDP Neighbors EEE Parameters

The displayed table contains a row for each interface. If the interface does not support EEE, then it displays as "EEE not supported for this interface". If EEE is not enabled on particular interface, then it displays as "EEE not enabled for this interface". If the link partner doesn't supports EEE, then it displays as "Link partner is not EEE capable. The columns hold the following information:	
Local Interface	The interface at which LLDP frames are received or transmitted.
Tx Tw	The link partner's maximum time that transmits path can hold-off sending data after deassertion of LPI
Rx Tw	The link partner's time that receiver would like the transmitter to hold-off to allow time for the receiver to wake from sleep.
Fallback Receive Tw	The link partner's fallbacks receive Tw. A receiving link partner may inform the transmitter of an alternate desired Tw_sys_tx. Since a receiving link partner is likely to have discrete levels for savings, this provides the transmitter with additional information that it may use for a more efficient allocation. Systems that do not implement this option default the value to be the same as that of the Receive Tw_sys_tx.

Echo Tx Tw	The link partner's fallback receives Tw. The respective echo values shall be defined as the local link partners reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner it can determine whether the remote link partner has received, registered and processed its most recent values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information.
Echo Rx Tw	The link partner's Echo Rx Tw value.
Resolved Tx Tw	The resolved Rx Tw for this link. Note: NOT the link partner The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).
Resolved Rx Tw	The resolved Rx Tw for this link Note: NOT the link partner. The resolved value that is the actual "Rx wakeup time " used for this link (based on EEE information exchanged via LLDP).
EEE in Sync	Shows whether the switch and the link partner have agreed on wake times. **Red** – Switch and link partner have not agreed on wakeup times. **Green** – Switch and link partner have agreed on wakeup times**.**

4.15.3.4 Port Statistics

The EdgeGM 7000 unit 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** (LLDP Statistics) refer to counters for the currently selected switch port.

Web GUI: Monitor > Advanced > L2 & Switching > LLDP > Port Statistics

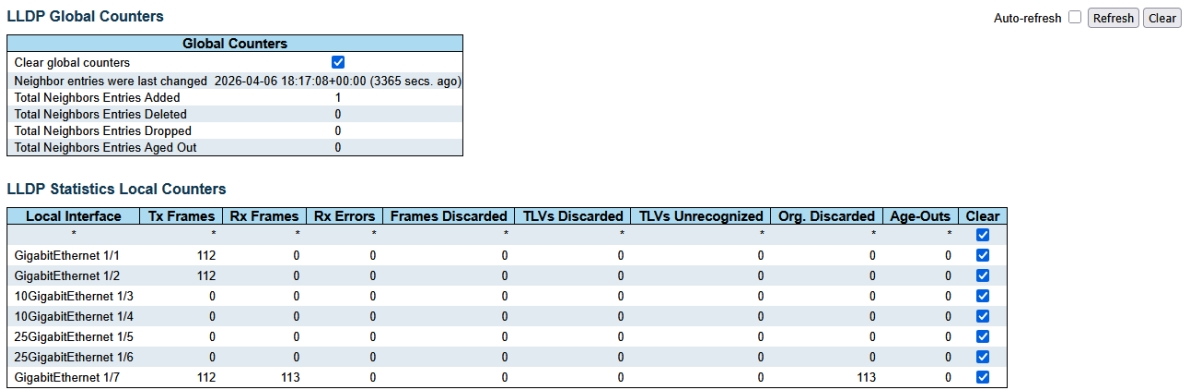


Figure 4-148: Port Statistics

Table 4-136: Port Statistic Parameters

Global Counters	
Clear Global counters	If checked the global counters are cleared when **Clear** is pressed.

Neighbor entries were last changed	Shows the time for the last entry when was last deleted or added. It also shows the time elapsed since last change was detected.
Total Neighbor Entries added	Shows the number of new entries added since switch reboot.
Total Neighbor Entries Deleted	Shows the number of new entries deleted since switch reboot.
Total Neighbor Entries Dropped	Shows the number of LLDP frames dropped due to that the entry table was full.
Total Neighbor Entries Aged Out	Shows the number of entries deleted due to Time-To-Live expiring.
Local Counters	
The displayed table contains a row for each interface.	
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 error.
Frames Discarded	If an LLDP frame is received on a port, and the switch's internal table is 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 **Chassis ID** or **Remote Port ID** is not already contained within the table. Entries are removed from the table when a given port link is down, an LLDP shutdown frame has been received, or when the entry ages out.
TLVs Discarded	Each LLDP frame can contain multiple pieces of information, known as TLVs (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 of value.
Org. Discarded	If LLDP frame is received with an organizationally TLV, but the TLV is not supported the TLV is discarded and counted.
Age-Outs	Each LLDP frame contains information about how long 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.
Clear	If checked the counters for the specific interface are cleared when is pressed.

4.16 Link OAM

The 802.3ah OAM standard provides the operation, administration and maintenance tools and mechanisms for monitoring link operation, fault detection and remote loopback control.

The 802.3ah is a complete standard for Ethernet in the first mile, which contains a link level (as opposed to service level) OAM mechanism. The protocol automatically discovers 802.3ah neighbors on a link. It can monitor and detect link degradation or failure in both bi-directional links and unidirectional links. Once a degradation or failure is detected, it provides diagnostic tools, e.g., it can set a link to “loopback” mode in order to check and isolate specific link problems.

The IEEE link layer OAM operates at the Ethernet layer and therefore (unlike SNMP or Ping) does not require an IP address.

The MIB variable retrieval operation allows collection of performance statistics.

The 802.3ah standard is a link oriented (port to port) protocol, i.e., it operates on a port level and communicates with the neighbor device directly connected to its port.

EdgeGM 7000 can communicate with any neighbor device supporting this protocol.

The major capabilities of 802.3ah are:

1. **Discovery**: detects the endpoints of a link and its OAM capabilities
2. **Remote Fault Detection**: allows one endpoint to convey severe events and failure conditions to its OAM link partner (Link fault, Dying Gasp, specific critical events)
3. **Link Performance Monitoring**: detection and notifications of different link faults. Event notification is delivered to the link partner when one of these events is detected on the link: Frame Error events, Frame Period Error events, Symbol Period Error events, Event Seconds Summary
4. **Remote Loopback**: can be used to put the remote port in loopback mode, useful for data-path test
5. **MIB variable retrieval**: collecting performance statistics. A MIB (Management Information Base) is a collection of variables which are deployed for measuring the link capability to support the defined SLA.
6. Verification of link port status
7. Simultaneous operation on multiple ports

A typical link OAM scenario is shown below:

Figure 4-149: Sample Network with OAM functionality.

4.16.1 Link OAM Port Configuration

This section allows the user to inspect the current Link OAM port configurations and change them as well.

Web GUI: Configuration > Advanced > L2 & Switching >Link OAM > Port Settings

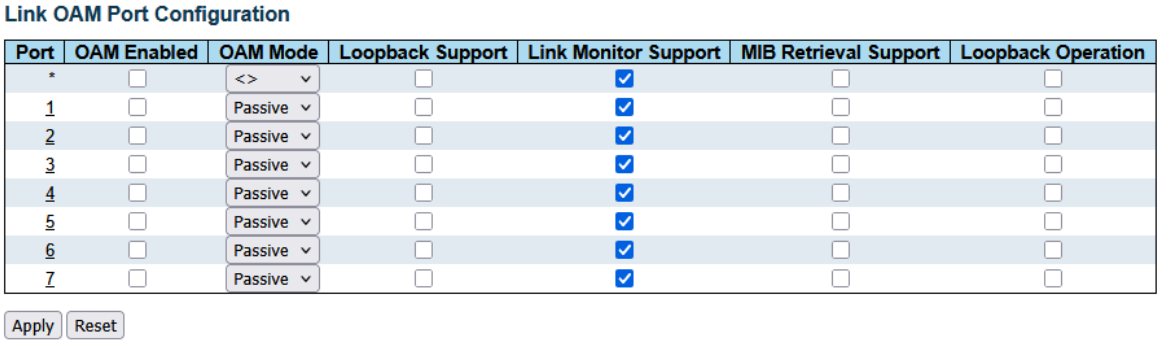


Figure 4-150: Link OAM Port Configuration

Table 4-137: Link OAM Port Configuration Parameters

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 initiates 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 operates 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 Active mode initiates the exchange of Information OAMPDUs as defined by 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.

4.16.2 Link Event Configuration for selected Port

This section allows the user to inspect the current Link OAM Link Event configurations and change them as well.

Web GUI: Configuration > Advanced > Link OAM > Events Settings

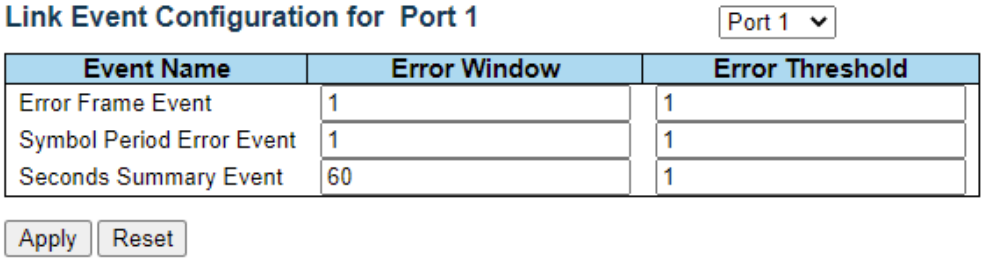


Figure 4-151: Link Event Configuration for selected port

Table 4-138: Link Event Configuration for selected port Parameters

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 0-0xffffffff and its default value is '0'.
Symbol Period Error Event	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.
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 0-0xffff and its default value is '1'.

4.16.3 Detailed Link OAM Statistics for selected port

This section 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 counters can occur at re-initialization of the management system.

Web GUI: Configuration > Advanced > Link OAM > Events Settings

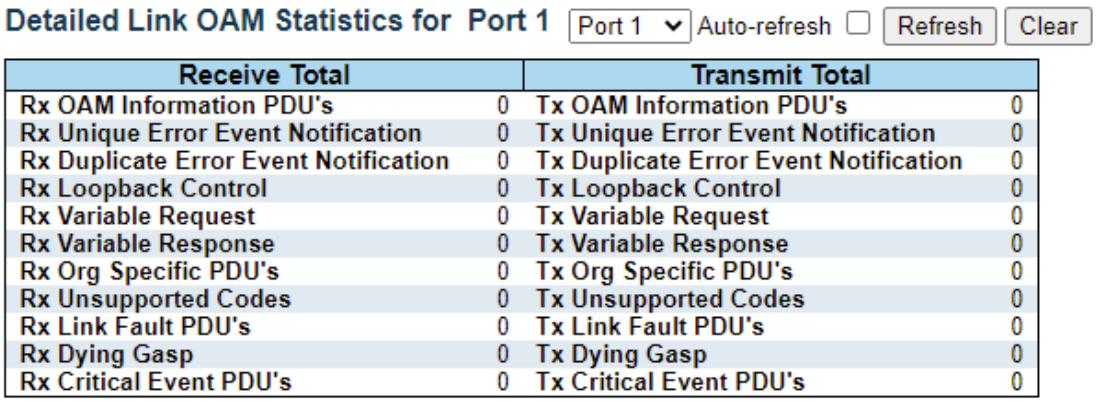


Figure 4-152: Detailed Link OAM Statistics for selected port

Table 4-139: Detailed Link OAM Statistics for selected port Parameters

Receive Total and Transmit Total	
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.

4.16.4 Detailed Link OAM Status for selected port

This page provides Link OAM configuration operational status. The displayed fields show the active configuration status for the selected port.

Web GUI: Monitor > Advanced > Link OAM > Port Status

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	00-05-80	Organizational Unique Identification	------
PDU Revision	0	PDU Revision	------

Figure 4-153: Detailed Link OAM Status for selected port

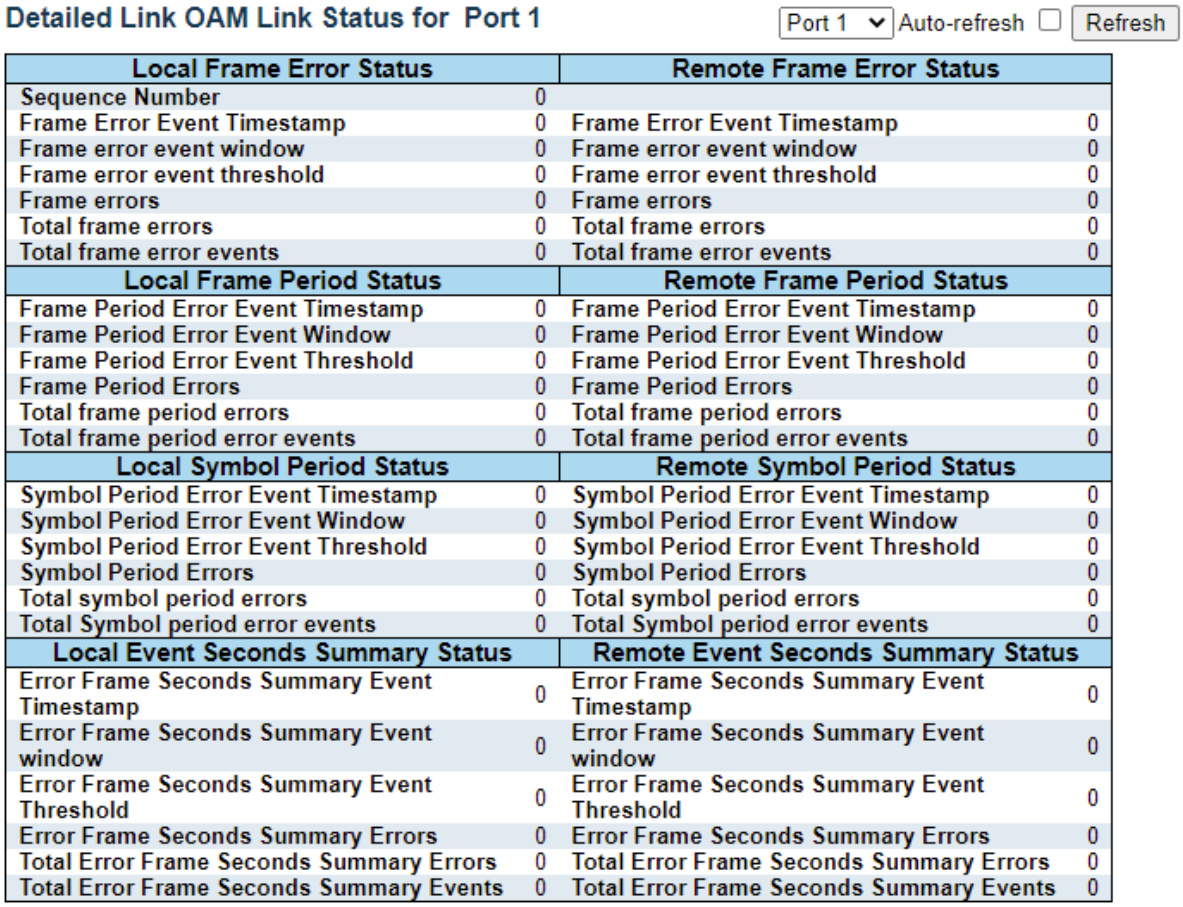
Table 4-140: Detailed Link OAM Status for selected port Parameters

Local and Peer	
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. In case 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.
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.

4.16.5 Detailed Link OAM Link Events Status for selected port

This section allows the user to inspect the current Link OAM Link Event configurations and change them as well. The left pane displays the Event status for the Local OAM unit while the right pane displays the status for the Peer for the respective port.

Web GUI: Monitor > Advanced > Link OAM > Event Status



Detailed Link OAM Link Status for Port 1

Port 1 | Auto-refresh | Refresh

Local Frame Error Status		Remote Frame Error Status	
Sequence Number	0		
Frame Error Event Timestamp	0	Frame Error Event Timestamp	0
Frame error event window	0	Frame error event window	0
Frame error event threshold	0	Frame error event threshold	0
Frame errors	0	Frame errors	0
Total frame errors	0	Total frame errors	0
Total frame error events	0	Total frame error events	0
Local Frame Period Status		**Remote Frame Period Status**	
Frame Period Error Event Timestamp	0	Frame Period Error Event Timestamp	0
Frame Period Error Event Window	0	Frame Period Error Event Window	0
Frame Period Error Event Threshold	0	Frame Period Error Event Threshold	0
Frame Period Errors	0	Frame Period Errors	0
Total frame period errors	0	Total frame period errors	0
Total frame period error events	0	Total frame period error events	0
Local Symbol Period Status		**Remote Symbol Period Status**	
Symbol Period Error Event Timestamp	0	Symbol Period Error Event Timestamp	0
Symbol Period Error Event Window	0	Symbol Period Error Event Window	0
Symbol Period Error Event Threshold	0	Symbol Period Error Event Threshold	0
Symbol Period Errors	0	Symbol Period Errors	0
Total symbol period errors	0	Total symbol period errors	0
Total Symbol period error events	0	Total Symbol period error events	0
Local Event Seconds Summary Status		**Remote Event Seconds Summary Status**	
Error Frame Seconds Summary Event Timestamp	0	Error Frame Seconds Summary Event Timestamp	0
Error Frame Seconds Summary Event window	0	Error Frame Seconds Summary Event window	0
Error Frame Seconds Summary Event Threshold	0	Error Frame Seconds Summary Event Threshold	0
Error Frame Seconds Summary Errors	0	Error Frame Seconds Summary Errors	0
Total Error Frame Seconds Summary Errors	0	Total Error Frame Seconds Summary Errors	0
Total Error Frame Seconds Summary Events	0	Total Error Frame Seconds Summary Events	0

Figure 4-154: Detailed Link OAM Link Status Events for selected port

Table 4-141: Link OAM Link Status Events for selected port Parameters

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.

4.17 RMON (Remote Network Monitoring)

4.17.1 RMON Statistics Configuration

Configure RMON Statistics table on this section. The entry index key is **ID**.

Web GUI: Configuration > Advanced > RMON > Statistics

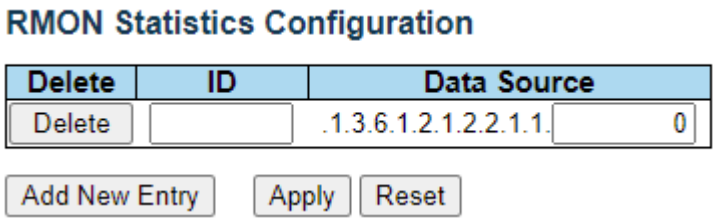


Figure 4-155: RMON Statistics Configuration

Table 4-142: RMON Statistics Configuration Parameters

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. If in stacking switch, the value must add 1000000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 20000005.

4.17.2 RMON History Configuration

Configure RMON History table on this section. The entry index key is **ID**.

Web GUI: Configuration > Advanced > RMON > History

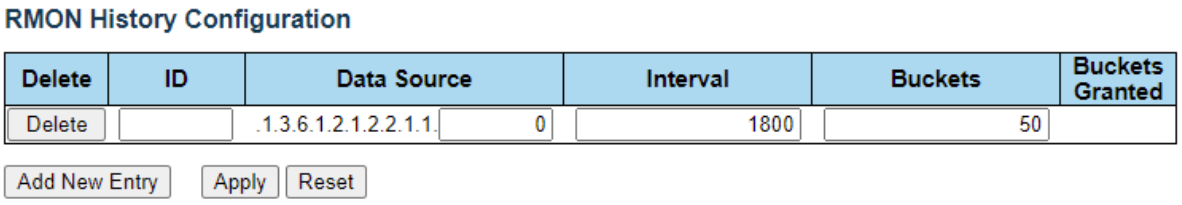


Figure 4-156: RMON History Configuration

Table 4-143: RMON History Configuration Parameters

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 must be monitored. If in stacking switch, the value must add 1000000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2000005
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 that shall be saved in the RMON.

4.17.3 RMON Alarm Configuration

This section provides configuration of RMON Alarm table. The entry index key is **`ID`**.

Web GUI: Configuration > Advanced > RMON > Alarm

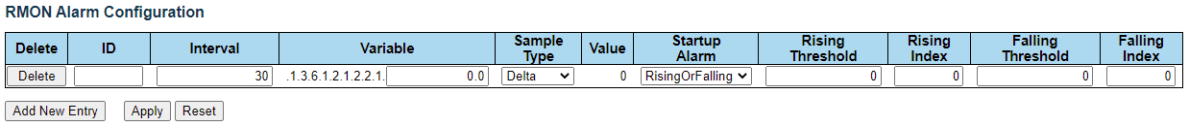


Figure 4-157: RMON Alarm Configuration

Table 4-144: RMON Alarm Configuration Parameters

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 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 broad-cast 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 contained errors preventing them from being deliverable to a higher-layer protocol. • **InUnknownProtos**: the number of the inbound packets that were 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 request to transmit. • **OutNUcastPkts**: The number of broad-cast and multi-cast packets that request to transmit. • **OutDiscards**: The number of outbound packets that are a discarded event the packets is 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. • **Failing** 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).

4.17.4 RMON Event Configuration

Configure RMON Event table on this section. The entry index key is **ID**.

Web GUI: Configuration > Advanced > RMON > Event

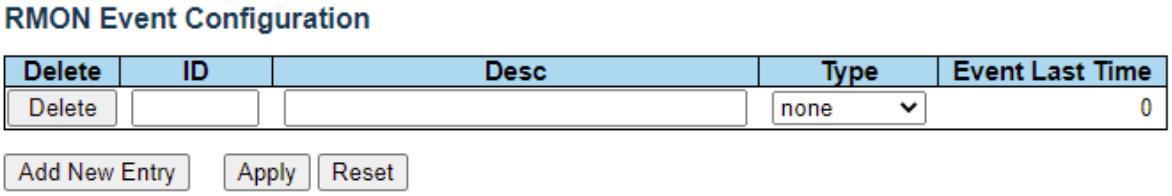


Figure 4-158: RMON Event Configuration

Table 4-145: RMON Event Configuration Parameters

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**: No SNMP log is created, no SNMP trap is sent. • **log**: Create SNMP log entry when the event is triggered. • **snmptrap**: Send SNMP trap when the event is triggered. • **logandtrap**: Create SNMP log entry and sent SNMP trap when the event is triggered.
Event Last Time	Indicates the value of sysUpTime at the time this event entry last generated an event.

4.18 Loop Protection

This page allows the user to inspect the current Loop Protection configurations.

Web GUI: Configuration > Advanced > L2 & Switching > Loop Protection

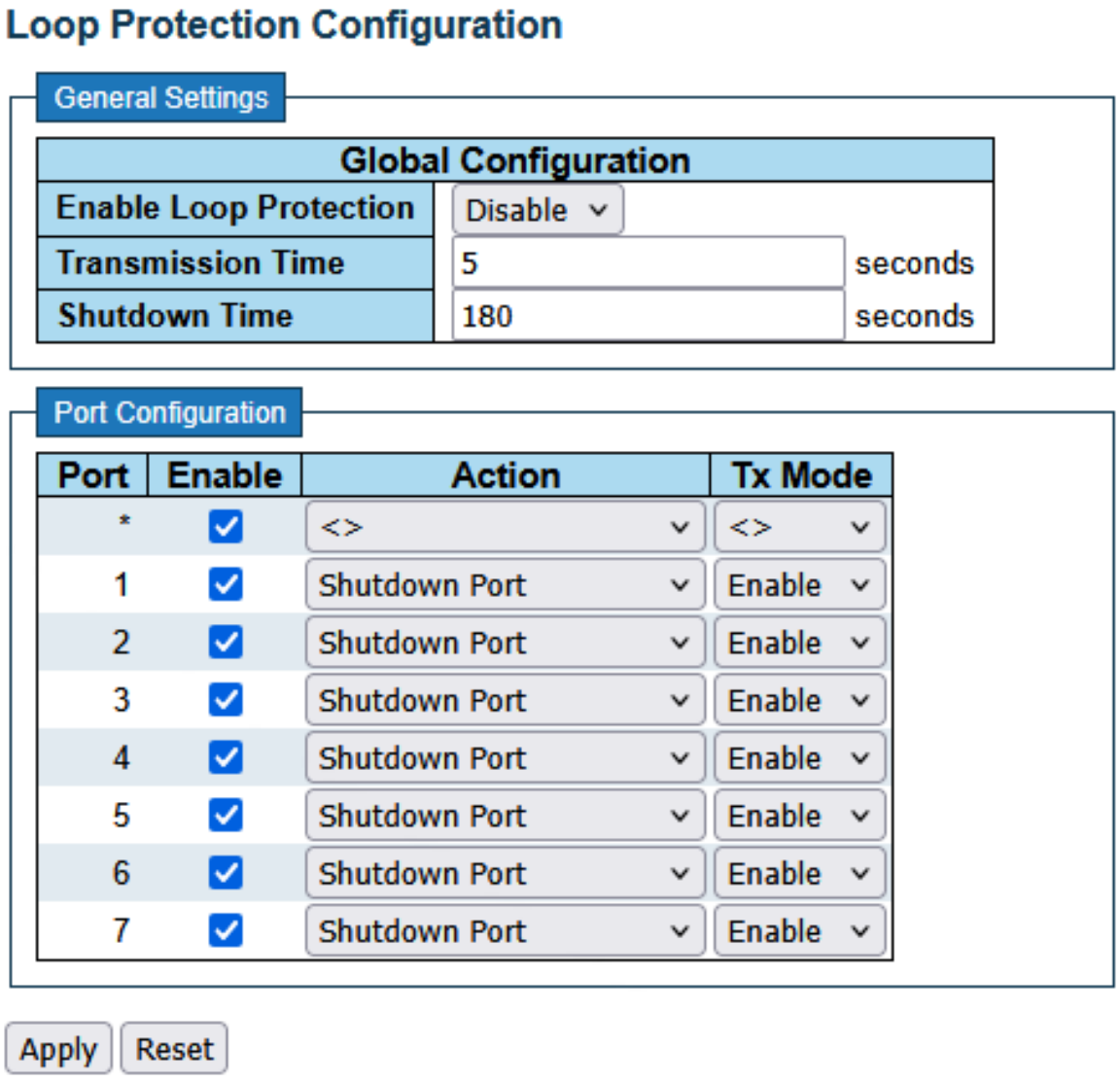


Figure 4-159: Loop Protection Configuration

Table 4-146: Loop Protection Configuration Parameters

General Settings Global Configuration	
Enable Loop Protection	Controls whether Loop Protection is enabled (as a whole).
Transmission Time	The interval between each Loop Protection PDU sent on each port. valid values are 1 to 10 seconds. Default value is 5 seconds
Shutdown Time	The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart). Default value is 180 seconds.
Port Configuration	
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.

4.18.1 Loop Protection Status

This page displays the loop protection port status the ports of the switch.

Web GUI: Monitor > Advanced > L2 & Switching > Loop Protection

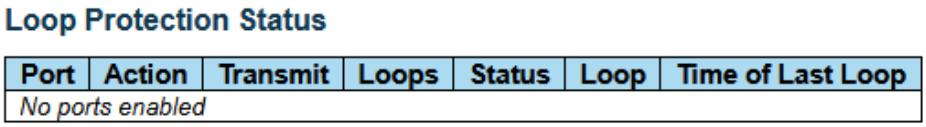


Figure 4-160: Loop Protection Status

Table 4-147: Loop Protection Status Parameters

Port	The switch 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.

4.19 GVRP Configuration

This section allows you to configure the global GVRP configuration settings that are commonly applied to all GVRP enabled ports. GVRP is an acronym for **G**ARP **V**LAN **R**egistration **P**rotocol. It is a protocol for dynamically registering VLANs on ports and is specified in IEEE 802.1Q-2005, clause 11. GVRP is an example of the use of GARP, hence the G in GVRP.

GARP is an acronym for **G**eneric **A**ttribute **R**egistration **P**rotocol. It is a generic protocol for registering attribute with other participants and is specified in IEEE 802.1D-2004, clause 12.

Web GUI: Configuration > Advanced > L2 & Switching > GVRP > Global config

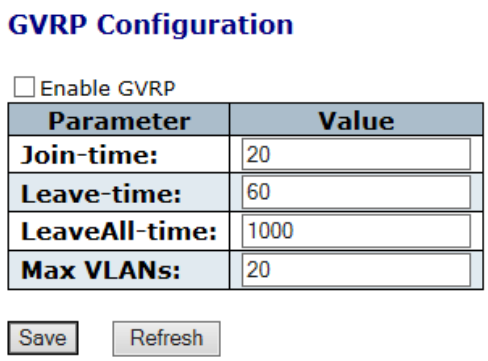


Figure 4-161: GVRP Configuration display

Table 4-148: GVRP Configuration parameters

GVRP Configuration	
Enable GVRP globally	The GVRP feature is globally enabled by setting the check mark in the checkbox named Enable GVRP and pressing the **Apply** button.
GVRP protocol timers	**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** is a value in the range of 60-300cs, i.e., in units of one hundredth of a second. The default is 60cs. Leave All-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.

4.20 sFlow Consideration

SFlow is an industry standard technology for monitoring switched networks through random sampling of packets on switch ports and time-based sampling of port counters. The sampled packets and counters (referred to as flow samples and counter samples, respectively) are sent as sFlow UDP datagrams to a central network traffic monitoring server. This central server is called an sFlow receiver or sFlow collector.

Additional information can be found at http://sflow.org.

4.20.1 sFlow Configuration displays

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.

Web GUI: Configuration > Advanced > L2 & Switching > sFlow

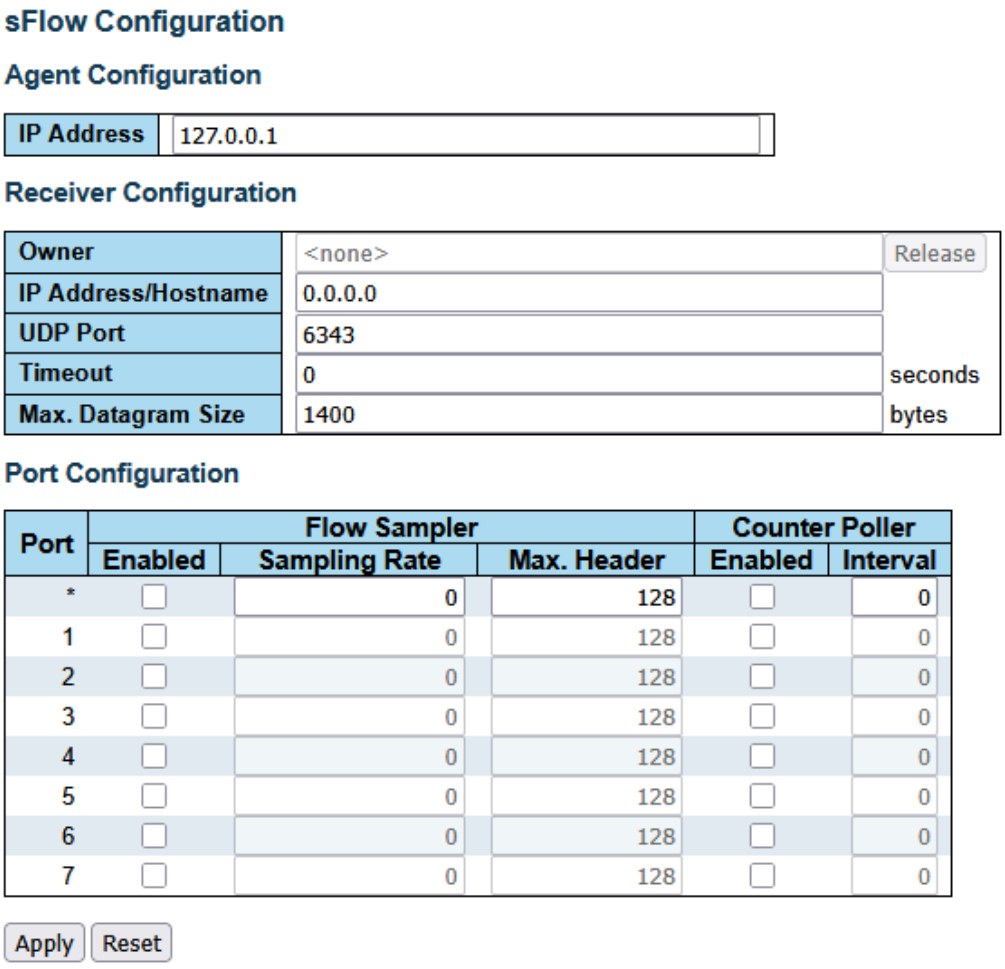


Figure 4-162: sFlow Configuration displays

Table 4-149: sFlow Configuration display parameters

Agent Configuration	
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.
Receiver Configuration	
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 **Release** 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.
Port Configuration	
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 consider 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.

4.20.2 sFlow Statistics

This sub-section shows receiver and per-port sFlow statistics.

Web GUI: Monitor > Advanced > L2 & Switching > sFlow

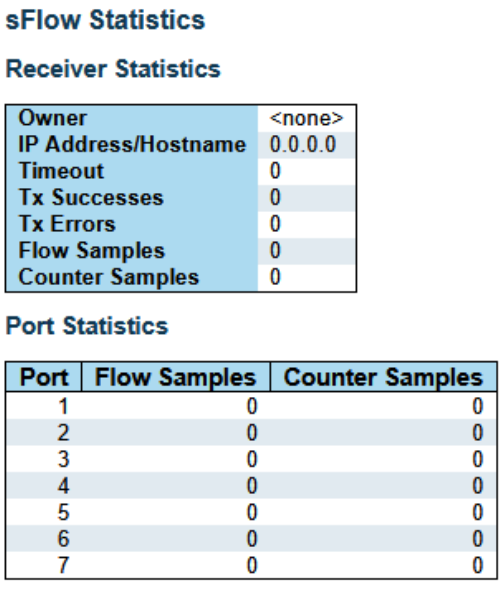


Figure 4-163: sFlow Statistics displays

Table 4-150: sFlow Statistics

Receiver Statistics	
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 Sample	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 Configuration	
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.

4.21 UDLD Configuration

UDLD is an acronym for **U**ni **D**irectional **L**ink **D**etection. UDLD protocol monitors the physical configuration of the links between devices and ports that support UDLD. It detects the existence of unidirectional links. Its functionality is to provide mechanisms useful for detecting one-way connections before they create a loop or other protocol malfunction.

RFC 5171 specifies a way at data link layer to detect Uni directional link.

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

4.21.1 UDLD Port Configuration

Web GUI: Configuration > Advanced > L2 & Switching > UDLD

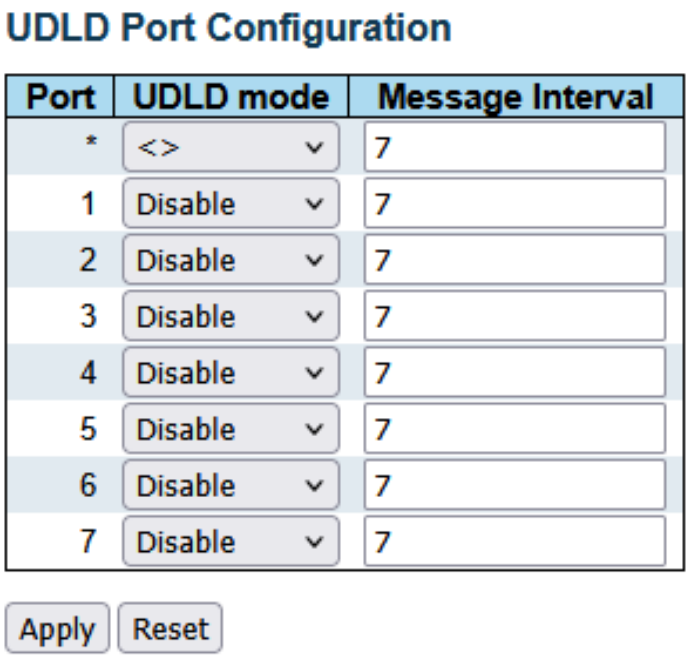


Figure 4-164: UDLD Port Configuration display

Table 4-151: UDLD Port Configuration parameters

UDLD Port Configuration	
Port	Port number of the switch.
UDLD Mode	Configure 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 UDLD on 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).

4.21.2 Detailed UDLD Status for Port 1

This section displays the UDLD status of the selected port

Web GUI: Monitor > Advanced > L2 & Switching > UDLD

Detailed UDLD Status for Port 1

UDLD status	
UDLD Admin state	Disable
Device ID(local)	00-05-80-08-87-AA
Device Name(local)	EGM-7000-716725070044
Bidirectional State	Indeterminant

Neighbor Status

Port	Device Id	Link Status	Device Name
No Neighbor ports enabled or no existing partners			

Figure 4-165: UDLD Status for Port 1

Table 4-152: UDLD Status for Port 1 parameters

UDLD Port Status	
UDLD Admin State	The current port state of the logical port, is 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.
Neighbor Status	
Port	The current port of neighbor device.
Device ID (local)	The ID of neighbor device.
Link Status	The current link status of neighbor port.
Device Name (local)	Name of the neighbor device.

4.22 TSN

The following sections describe the configuration and monitoring of TSN

4.22.1 PTP Check

This section describes the TSN configuration parameters.

Configuration > Advanced > L2 & Switching > TSN > PTP Check

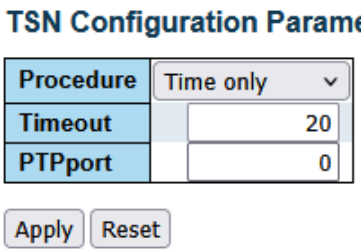


Figure 4-166: PTP Check parameters

4-153: PTP Check parameters

Procedure	Specify the procedure to use. The options are: • Time only • Time and PTP
Timeout	Specify the timeout.
PTP Port	Specify the PTP port.

4.22.2 Frame Preemption Configuration

This section describes the TSN configuration parameters.

Configuration > Advanced > L2 & Switching > TSN > PTP Check

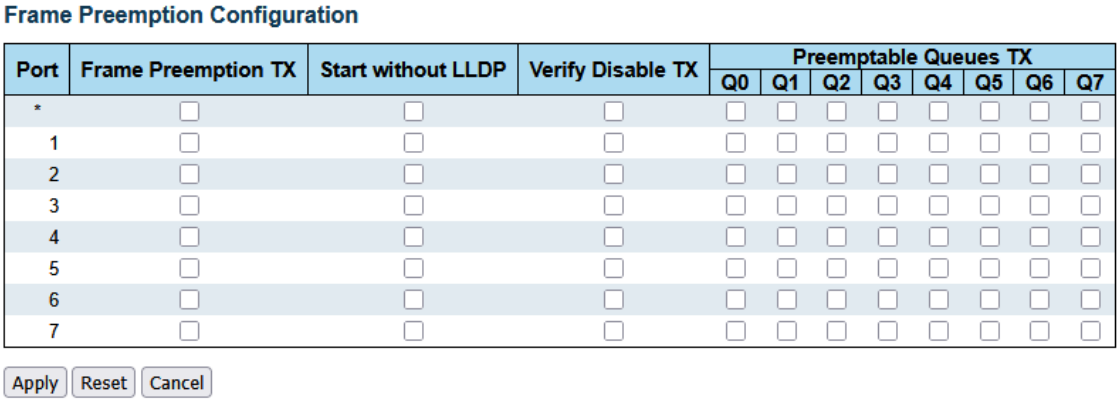


Figure 4-167: PTP Check parameters

4-154: PTP Check parameters

Port	The port to configure
Frame Preemption TX	Enable or disable Frame Preemption on the port
Start without LLDP	Indicate whether frame preemption starts without LLDP
Verify Disable TX	Enable or disable Verify Disable TX
Preemptable Queues TX	Indicate the TX queues to apply Frame Preemption

4.22.3 TAS

The following sections describe the configuration and monitoring of TAS.

4.22.3.1 TAS Ports configuration

This section describes the TAS Ports configuration parameters.

Configuration > Advanced > L2 & Switching > TAS > Ports

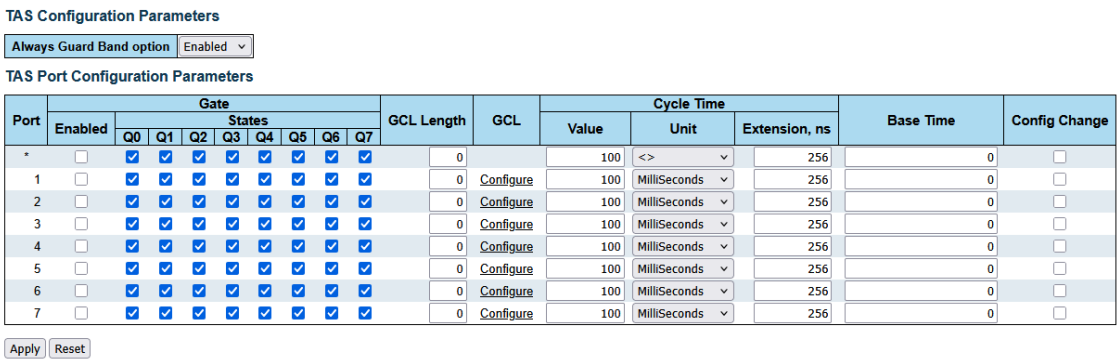


Figure 4-168: TAS Port parameters

4-155: TAS Port parameters

TAS Configuration Parameters	
Always Guard Band option	Enable or disable the Always Guard Band option on the port.
TAS Port Configuration Parameters	
Port	The port to be configured.
Gate	Enable the Gate functionality on the selected queue states
GCL Length	Specify the GCL length
GCL	Click **Configure** to open the GCL Configuration page
Cycle Time	Specify the Value, Unit, and Extension of the cycle time
Base Time	Specify the Base Time
Config Change	Enable the configuration change

4.22.3.2 Max SDU

This section describes the MAX SDU configuration parameters.

Configuration > Advanced > L2 & Switching > TSN > TAS > Max SDU

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
5	1536	1536	1536	1536	1536	1536	1536	1536
6	1536	1536	1536	1536	1536	1536	1536	1536
7	1536	1536	1536	1536	1536	1536	1536	1536

Apply Reset

Figure 4-169: TAS SDU Configuration parameters

4-156: TAS SDU parameters

Port	The port to configure
Max SDU Size	Specify the maximum SDU size for each queue

4.22.4 PSFP

This section describes the PSFP parameters.

4.22.4.1 Flow Meter

Configuration > Advanced > L2 & Switching > TSN > PSFP > Flow Meter

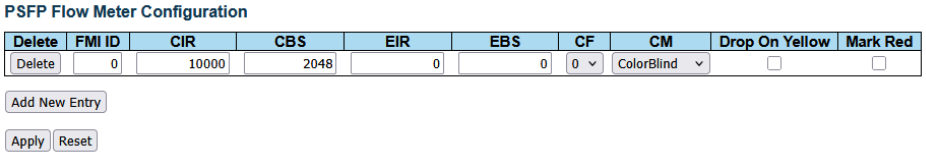


Figure 4-170: PSFP Flow Meter Configuration parameters

4-157: PSFP Flow Meter Configuration parameters

Delete	Click to delete the PSFP Flow Meter
FMI ID	Specify the FMI ID
CIR	Specify the CIR
CBS	Specify the CBS
EIR	Specify the EIR
EBS	Specify the EBS
CF	Select the CF (0 or 1)
CM	Specify the CM to be used. The options are: • ColorBlind • ColorAware
Drop On Yellow	Specify whether to drop on yellow
Mark Red	Specify whether or not to mark red entries

4.22.4.2 Stream Filter

Configuration > Advanced > L2 & Switching > TSN > PSFP > Stream Filter

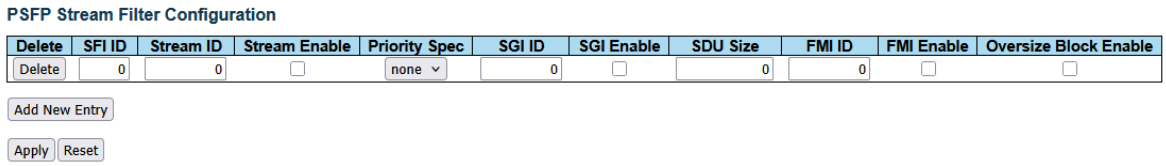


Figure 4-171: PSFP Stream Meter Configuration parameters

4-158: PSFP Stream Meter Configuration parameters

Delete	Click to delete the stream filter
SFI ID	Specify the SFI ID
Stream ID	Specify the Stream ID
Stream Enable	Enable the stream
Priority Spec	Specify the priority. The range is 1 to 7.

SGI ID	Specify the SGI ID
SGI Enable	Enable or disable SGI
SDU Size	Specify the SDU Size
FMI ID	Specify the FMI ID
FMI Enable	Enable or disable FMI on the stream
Oversize Block Enable	Enable or disable oversized blocks

4.22.4.3 Stream Filter

Configuration > Advanced > L2 & Switching > TSN > PSFP > Stream Gate

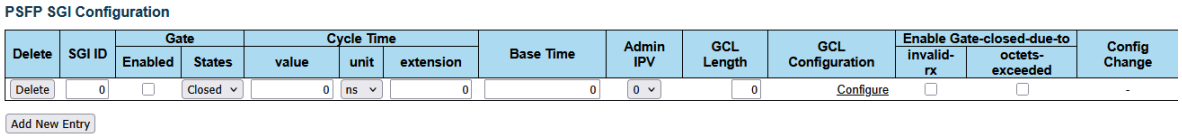


Figure 4-172: PSFP SGI Configuration parameters

4-159: PSFP SGI Configuration parameters

Delete	Click to delete the stream filter
SFI ID	Specify the SFI ID
Gate	Enable or disable the gate and specify whether it is open or closed
Cycle Time	Specify the value, unit, and extension of the cycle time
Base Time	Specify the base time of the gate
Admin IPV	Specify the admin IPV. The range is 0 to 7.
GCL Length	Specify the GCL length
GCL Configuration	Click **Configure** to open the GCL Configuration. Note – Apply the PSFP SGI configuration before configuring the GCL
Enable Gate-closed-due-to	Specify the Gate-Closed conditions. The options are Invalid-Rx and Octets-Exceeded
Config Change	Enable the configuration change

This page intentionally left blank.

5 Management

The following topics are discussed in this chapter:

- General Introduction
- System Information
- DHCP (Dynamic Host Configuration Protocol)
- Simple Network Management Protocol (SNMP)
- Supported SNMP MIBs
- Command Line Interface (CLI)
- Events Configuration
- Web Interface
- RMON Overview

This page intentionally left blank.

5.1 General Introduction

The EdgeGM 7000 can be remotely or locally managed via a variety of mechanisms and platforms:

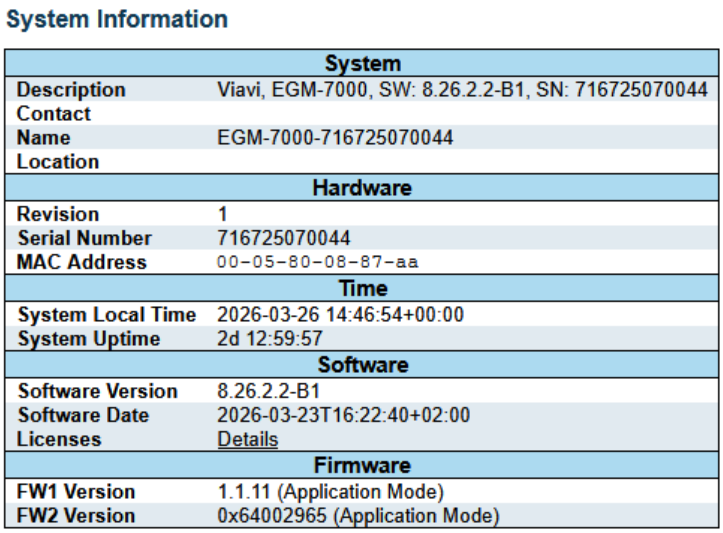
- IP Based (in-band): SNMP (v1/v2/v3), Telnet (CLI), SSH, Web – HTTP/HTTPS.
- Console (RJ-45): RS-232 (115200Bd) CLI

See Chapter 3: Getting Started for more information about connecting to the EdgeGM 7000.

5.2 System Information

This section provides general information about the system.

Web GUI: Monitor > System > Information


System Information

System	
Description	Viavi, EGM-7000, SW: 8.26.2.2-B1, SN: 716725070044
Contact	
Name	EGM-7000-716725070044
Location	
Hardware	
Revision	1
Serial Number	716725070044
MAC Address	00-05-80-08-87-aa
Time	
System Local Time	2026-03-26 14:46:54+00:00
System Uptime	2d 12:59:57
Software	
Software Version	8.26.2.2-B1
Software Date	2026-03-23T16:22:40+02:00
Licenses	Details
Firmware	
FW1 Version	1.1.11 (Application Mode)
FW2 Version	0x64002965 (Application Mode)

Figure 5-1: System Information

Table 5-1: System Information Parameters

Contact	The system contact configured in Configuration | System | Information | System Contact.
Name	The system name configured in Configuration | System | Information | System Name.
Location	The system location configured in Configuration | System | Information | System Location
MAC Address	The MAC Address of this switch.
Chip ID	The Chip ID of this switch.
System Date	The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any.
System Uptime	The period of time the device has been operational.

Software Version	The software version of this switch.
Software Date	The date when the switch software was produced.
Code Revision	The version control identifier of the switch software.

5.2.1 System Status

The switch system status is provided here.

Web GUI: Monitor > System > Status

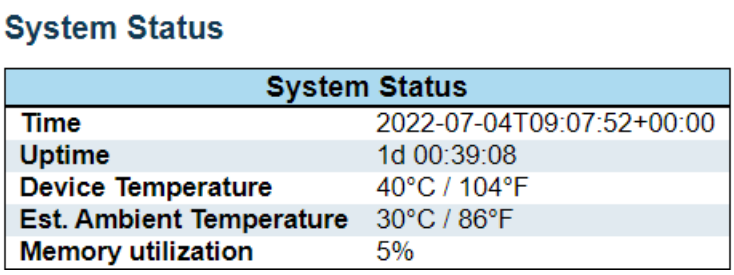


Figure 5-2: System Status

Table 5-2: System Status Parameters

System Status	
Time	The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any.
Uptime	The period the device has been operational.
Device Temperature	The device actual temperature.
Estimated Ambient Temperature	The estimated ambient temperature.
Memory utilization	Derived from the percent of available memory in use at a given moment.

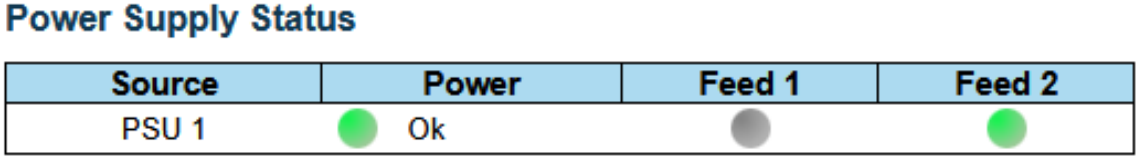


Figure 5-3: Power Supply Status

Table 5-3: Power Supply Status Parameters

Power Supply Status	
Source	Indicate which power supply is installed/not installed.
Power	Indicate if PS is up or disable.
Feed 1	Indicates the status of feed one
Feed 2	Indicates the status of feed two

5.2.2 CPU Load

This page displays the CPU load, using an SVG graph.

The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well.

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 plug-in installed to support SVG.

Web GUI: Monitor > System > CPU Load

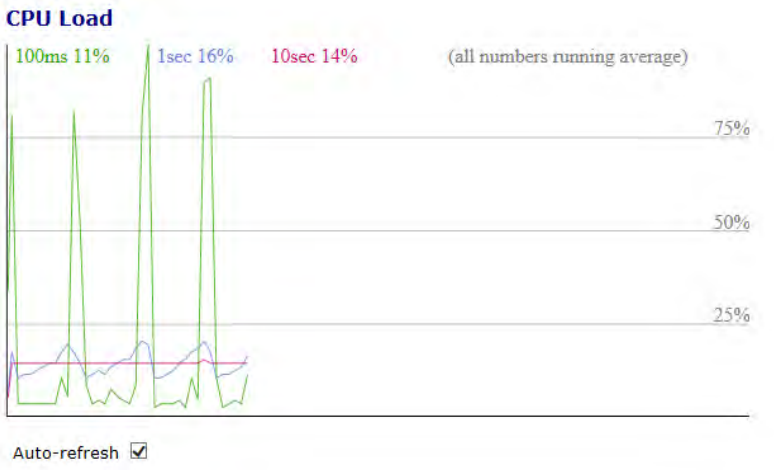
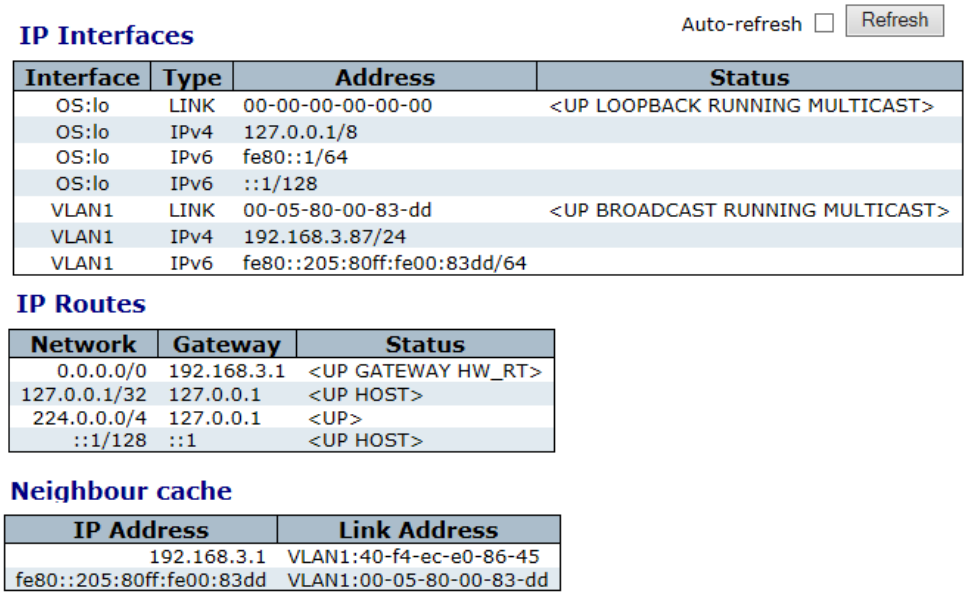


Figure 5-4: CPU Load

5.2.3 IP Status

This section 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.

Web GUI: Monitor > System > IP Status



IP Interfaces

Auto-refresh ☐ Refresh

Interface	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	fe80::1/64	
OS:lo	IPv6	::1/128	
VLAN1	LINK	00-05-80-00-83-dd	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.3.87/24	
VLAN1	IPv6	fe80::205:80ff:fe00:83dd/64	

IP Routes

Network	Gateway	Status
0.0.0.0/0	192.168.3.1	<UP GATEWAY HW_RT>
127.0.0.1/32	127.0.0.1	<UP HOST>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

Neighbour cache

IP Address	Link Address
192.168.3.1	VLAN1:40-f4-ec-e0-86-45
fe80::205:80ff:fe00:83dd	VLAN1:00-05-80-00-83-dd

Figure 5-5: IP Status displays

Table 5-4: IP Status displays Parameters

IP Interfaces	
Interface	The name of the interface.
Type	The address type of the entry. This may be **LINK**, **IPv4** or **IPv6**.
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 IPv4/IPv6 address of the entry.
Link Address	Link (MAC) address for which a binding to the IP address given exist.

5.2.4 System Log Information

The switch system log information is provided here.

Web GUI: Monitor > System > Log

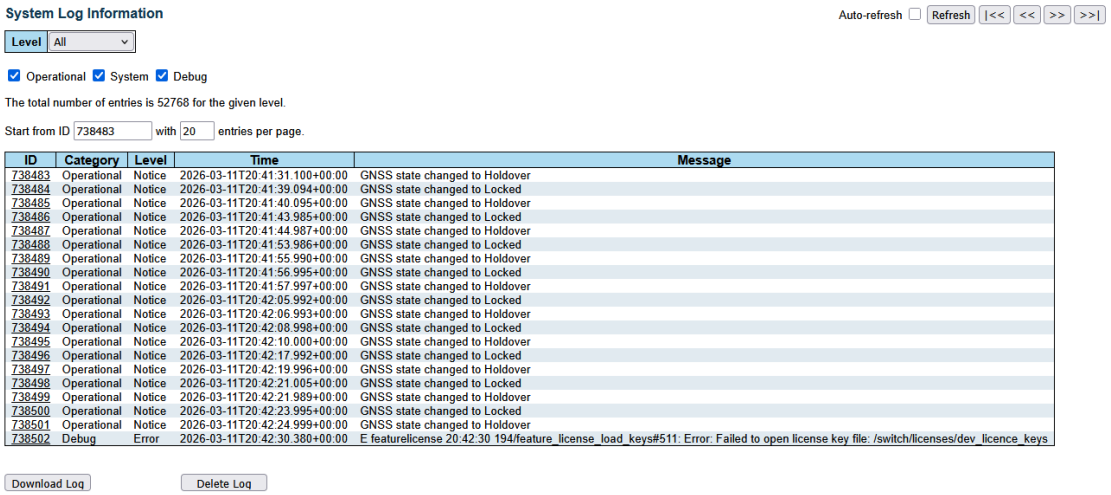


Figure 5-6: System log information

Table 5-5: System Log Information Parameters

System Log Information Entry Columns	
ID	The identification of the system log entry.
Category	The category of the system log entry. The options are: • Operational • System • Debug
Level	The level of the system log entry. Info: The system log entry belongs to the information level. Warning: The system log entry belongs to the warning level. Error: The system log entry belongs to the error level.
Time	The occurred time of the system log entry.
Message	The detail message of the system log entry.
Navigating the System Log Information Table Each page shows up to 999 table entries, selected through the "entries per page" input field. When first visited, the web page will show the beginning entries of this table. The **Level** input field is used to filter the display system log entries. The **Clear Level** input field is used to specify which system log entries will be cleared. To clear specific system log entries, select the clear level first then click the **Clear** button. The **Start from ID** input field allow the user to change the starting point in this table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next entry match. In addition, these input fields will upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.	

The **>>** 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. Use the **<<** to start over.

5.2.5 Detailed System Log Information

The switch system detailed log information is provided here.

Web GUI: Monitor > System > Detailed Log

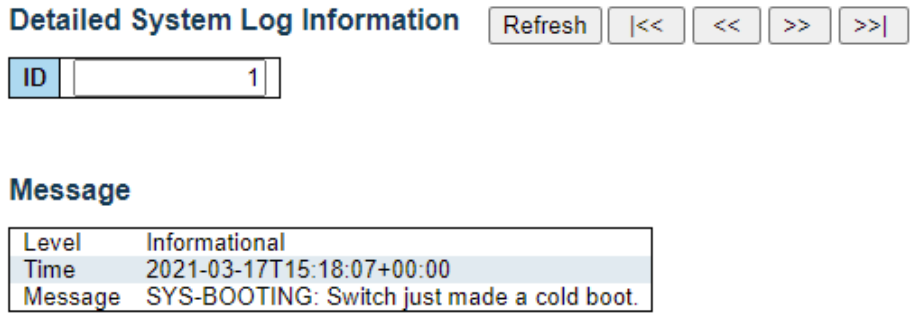


Figure 5-7: Detailed system log information

Table 5-6: Detailed System Log Information Parameters

Detailed System Log Information	
ID	The ID (>= 1) of the system log entry
Level	The severity level of the system log entry
Time	The time and date of the system log entry
Message	The detailed message of the system log entry

5.2.6 Events

The switch system detailed log information is provided here.

Web GUI: Monitor > System > Events

Events Handler Status

Category: All

#	Event	Severity	Enable	Interface				Status	Counter	Clear
				SNMP	Syslog	CLI	Call-Home			
1	Cold start	Info	✓	✓	✓	✓	✓	●	1	Clear
2	Warm start	Info	✓	✓	✓	✓	✓	●	0	Clear
3	Link down	Warning	✓	✓	✓	✓	✓	●	0	Clear
4	Link Up	Info	✓	✓	✓	✓	✓	●	3	Clear
5	SNMP Authentication failure	Notice	✓	✓	✓	✓	✓	●	0	Clear
6	PSU state change	Notice	✓	✓	✓	✓	✓	●	0	Clear
7	Temperature state change	Notice	✓	✓	✓	✓	✓	●	0	Clear
8	CPU state change	Notice	✓	✓	✓	✓	✓	●	0	Clear
9	SFP module plugged in	Info	✓	✓	✓	✓	✓	●	0	Clear
10	SFP module unplugged	Info	✓	✓	✓	✓	✓	●	0	Clear
11	SyncCenter state changed	Notice	✓	✓	✓	✓	✓	●	2	Clear
12	SyncCenter selected input clock changed	Notice	✓	✓	✓	✓	✓	●	1	Clear
13	SyncCenter input clock status changed	Notice	✓	✓	✓	✓	✓	●	706	Clear
14	SyncCenter output quality changed	Notice	✓	✓	✓	✓	✓	●	0	Clear
15	SyncCenter BITS output state changed	Notice	✓	✓	✓	✓	✓	●	0	Clear
16	SyncCenter system clock state change	Notice	✓	✓	✓	✓	✓	●	0	Clear
17	GPS status changed	Notice	✓	✓	✓	✓	✓	●	10364	Clear
18	GPS antenna status changed	Notice	✓	✓	✓	✓	✓	●	3	Clear
19	GNSS satellite state changed	Warning	✓	✓	✓	✓	✓	●	35	Clear
20	STL status changed	Notice	✓	✓	✓	✓	✓	●	285	Clear
21	GEOL status changed	Notice	✓	✓	✓	✓	✓	●	0	Clear
22	PTP state changed	Notice	✓	✗	✓	✓	✓	●	0	Clear
23	PTP BMCA Master select changed	Notice	✓	✗	✓	✗	✗	●	0	Clear
24	PTP BMCA Announce time out	Notice	✓	✗	✓	✗	✗	●	6	Clear
25	PTP BMCA Clock quality changed	Notice	✓	✗	✓	✗	✗	●	4	Clear
26	PTP BMCA Tine properties changed	Notice	✓	✗	✓	✗	✗	●	4	Clear

Figure 5-8: Events Handler Status

Table 5-7: Detailed System Log Information Parameters

#	Event Index
Event	Unique Name of the Event.
Severity	Indicates the severity of the event (Notice, Info, Warning).
Enable	Disable/Enable Event (Change will take effect on all checked interfaces: SNMP, syslog, cli).
Interface	Distribute event on a given interface: SNMP, Syslog, CLI, Flash.
Status	Indication whether an event occurred or not.
Counter	The number of occurrences of the event since last Clear operation.
Clear	Clear event occurred indication.

5.2.7 Temperature

Temperature statistics are provided here.

Web GUI: Monitor > System > Temperature

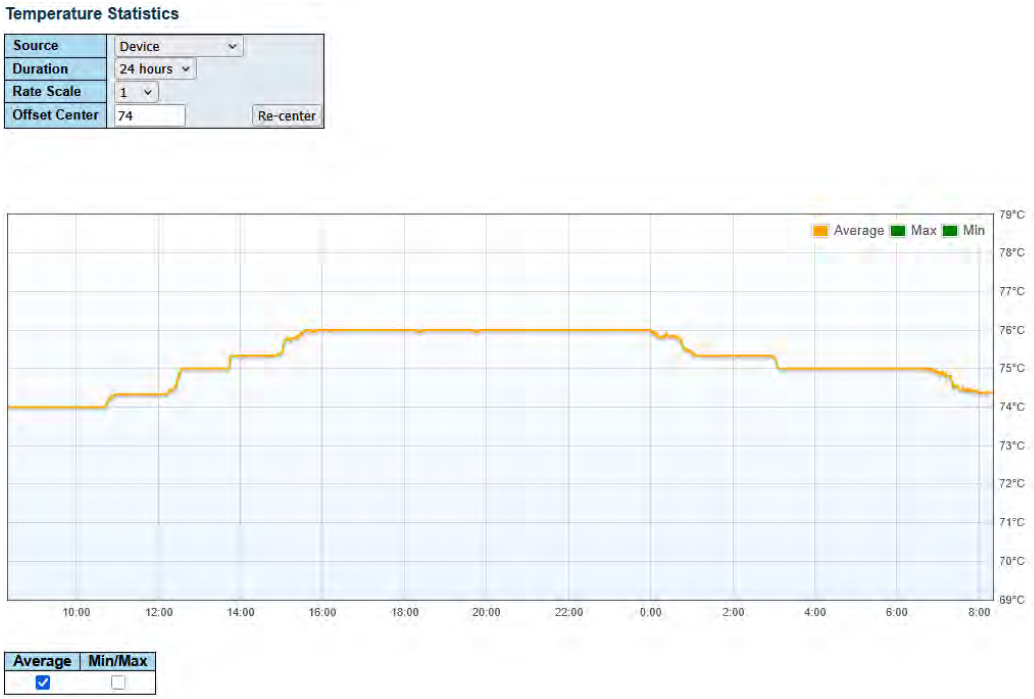


Figure 5-9: Detailed system log information

Table 5-8: Detailed System Log Information Parameters

Source	The source of the temperature statistics. The options are: • Device • Ambient • Junction • Sensors Average • Sensor 1-3
Duration	The duration of the statistical collection
Rate Scale	The rate scale
Offset Center	The offset required to center the readings in the graph
Recenter	Click Recenter to recenter the graph based on the offset
Average	Display the average
Min/Max	Display the minimum and maximum temperatures

5.3 DHCP (Dynamic Host Configuration Protocol)

DHCP is an acronym for **D**ynamic **H**ost **C**onfiguration **P**rotocol. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

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.

5.3.1 DHCP Server Mode Configuration

DHCP Server is used to allocate network addresses and deliver configuration parameters to dynamically configured hosts called DHCP client.

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

DHCP Server is used to allocate network addresses and deliver configuration parameters to dynamically configured hosts called DHCP client.

Web GUI: Configuration> Advanced> IP & Routing> DHCP> Server > Mode

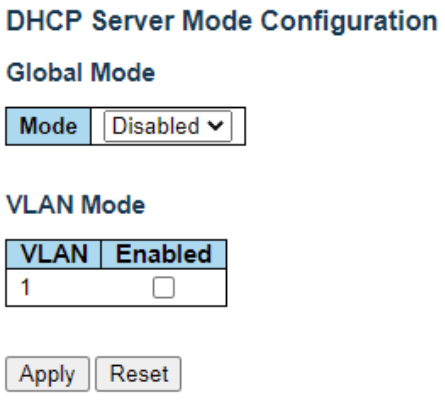


Figure 5-10: DHCP Server Mode Configuration

Table 5-9: DHCP Server Mode Configuration Parameters

Global Mode Configure operation mode to enable/disable DHCP server per system.	
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.	
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 VLAN Range** to add a new VLAN range 2. Input the VLAN range that you want to disable 3. Choose Mode to be **Disabled**. 4. Press **Save** 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.

5.3.2 DHCP Server Excluded IP Configuration

This section configures excluded IP addresses. DHCP server will not allocate these excluded IP addresses to DHCP client.

Web GUI: Configuration> Advanced> IP & Routing> DHCP> Server > Excluded IP

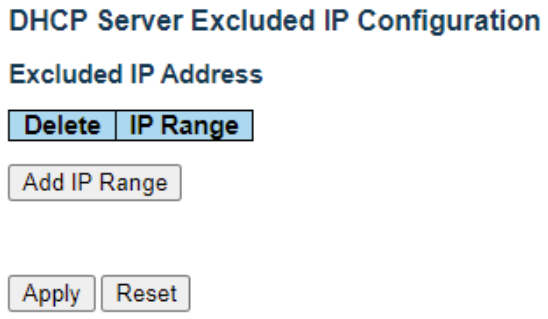


Figure 5-11: DHCP Server Excluded IP Configuration

Table 5-10: DHCP Server Excluded IP Configuration Parameters

Excluded IP Address	
Configure excluded IP addresses.	
Delete	Delete Excluded Ip Address operation
IP Range	Define the IP Range to be excluded. 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	**Add IP Range**: Click to add anew exclude IP range.

5.3.3 DHCP Server Pool Configuration

This page manages DHCP pools. According to the DHCP pool, DHCP server will allocate IP address and deliver configuration parameters to DHCP client.

Web GUI: Configuration> Advanced> IP & Routing> DHCP> Server > Pool

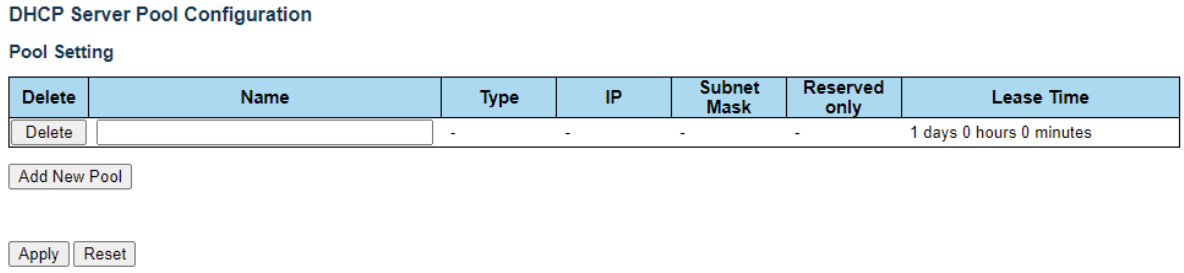


Figure 5-12: DHCP Server Pool Configuration

Table 5-11: DHCP Server Pool Configuration Parameters

Pool Setting	
	Add or delete pools. Adding a pool and giving a name is to create a new pool with "default" configuration. If you want to configure all settings including type, IP subnet mask and lease time, you can click the pool name to go into the configuration page.
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 types of 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. If "-" is displayed, it means not defined.

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.
Reserved Only	If on, Ip addresses obtainable from the pool are limited to those entered into the reserved entries table.
Lease Time	Display lease time of the pool.

5.3.4 DHCP Snooping Configuration

Configure DHCP Snooping on this section.

Web GUI: Configuration> Advanced> IP & Routing> DHCP> Snooping

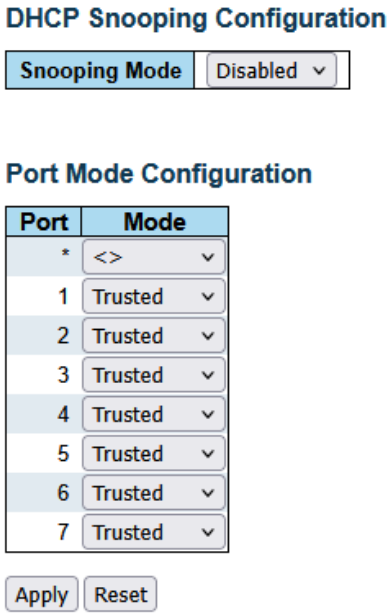


Figure 5-13: Snooping Configuration

Table 5-12: Snooping Configuration Parameters

DHCP Snooping Configuration	
Snooping mode	Indicates the DHCP Snooping mode of operation. Possible modes are: **Enabled**: Enable DHCP snooping mode operation. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports. **Disabled**: Disable DHCP snooping mode operation.
Port Mode Configuration	Indicates the DHCP snooping mode. Possible modes are: **Trusted**: Configures the port as trusted source of the DHCP messages. **Untrusted**: Configures the port as untrusted source of the DHCP messages.

5.3.5 Dynamic DHCP Snooping

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 section

Web GUI: Monitor > DHCP > Snooping Table

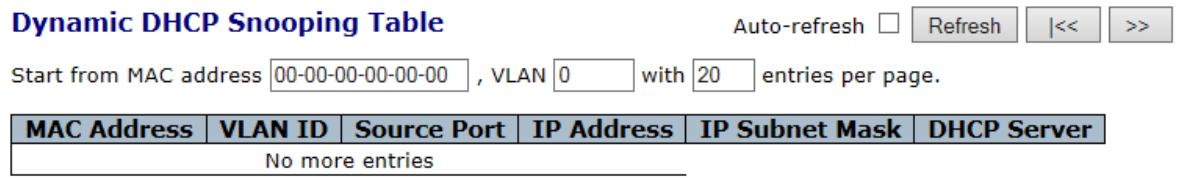


Figure 5-14: Dynamic DHCP Snooping Table

Table 5-13: Dynamic DHCP Snooping Table Parameters

Dynamic DHCP snoopingTable	
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
Navigating the DHCP snooping Table	

Each page shows up to 99 entries from the, Dynamic DHCP snooping 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 DHCP snooping Table. The “MAC address” and “VLAN” input fields allows the user to select the starting point in the Dynamic DHCP snooping Table.

Clicking the **Refresh** button will update the displayed table starting from that or the closest next MVR Channels (Groups) Information 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 table 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.

5.3.6 DHCP Relay Configuration

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.

Web GUI: Configuration> Advanced> IP & Routing> DHCP> Relay

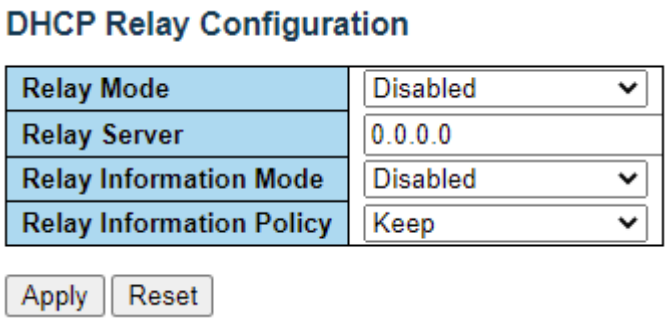


Figure 5-15: DHCP Relay Configuration

Table 5-14: DHCP Relay Configuration Parameters

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 is always equal 0, in stackable device it means switch ID) and the last two characters are the port number. For example, "00030108" means the message receives 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 agent receives a DHCP message that already contains relay agent information it will enforce the policy. And it only works under DHCP if relay information operation mode is enabled. 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.
	Drop: Drop the package when a DHCP message that already contains relay information is received.

5.3.7 DHCP Relay Statistics

EdgeGM 7000 provide statistics for DHCP relay, which is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain. Note: for a detailed description of the DHCP Relay feature, go to DHCP Relay Configuration.

Web GUI: Monitor > DHCP > Relay Statistics

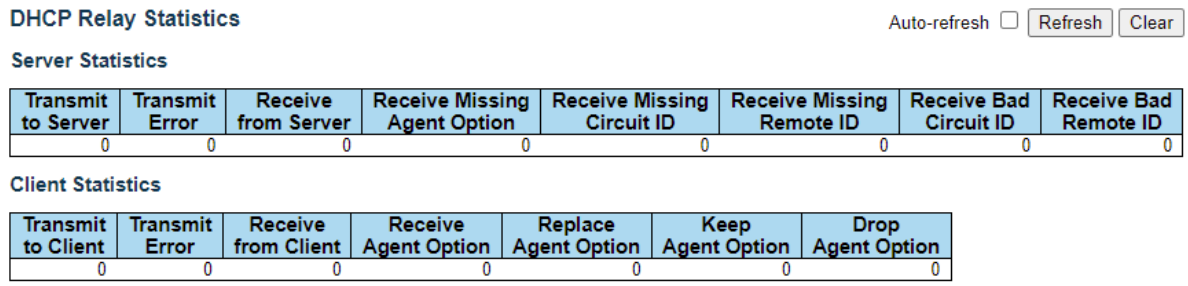


Figure 5-16: DHCP Relay Statistics

Table 5-15: DHCP Relay Statistics Parameters

Server Statistics	
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 client
Receive from Server	The packets number 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.
Receive Missing Remote ID	The number of packets received with the remote ID option missing.
Receive Bad Circuit ID	The number of packets received with the Circuit ID option did not match known circuit ID.
Receive Bad Remote ID	The packets number of which the Remote ID option did not match known Remote ID.
Client Statistics	
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 received packets 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.

5.3.8 DHCP Server Statistics

This section displays the database counters and the number of DHCP messages sent and received by DHCP server.

Web GUI: Monitor > DHCP > Server > Statistics

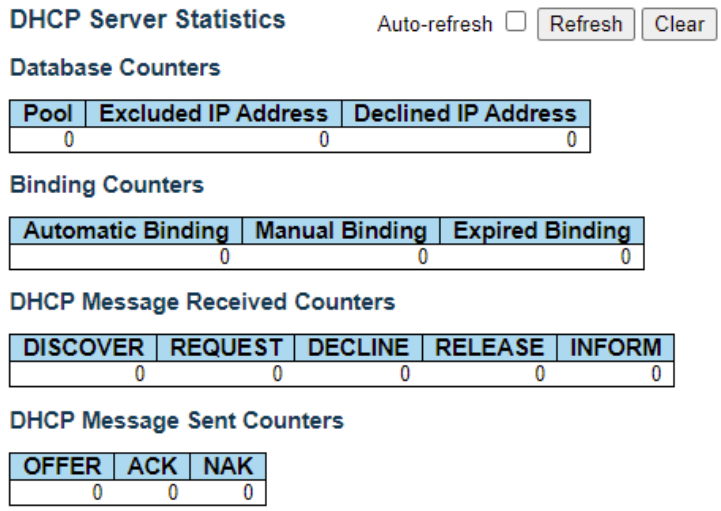


Figure 5-17: DHCP Server Statistics

Table 5-16: DHCP Server Statistics Parameters

Database Counters	
Display counters of various databases.	
Pool	Number of pools
Excluded IP Address	Number of excluded IP address ranges
Declined IP Address	Number of declined IP addresses.
Binding Counters	
Display counters of various databases.	
Automatic Number 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	
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	
OFFER	Number of DHCP OFFER messages sent.
ACK	Number of DHCP ACK messages sent.
NAK	Number of DHCP NAK messages sent.

5.3.9 DHCP Server Binding IP

This section displays bindings generated for DHCP clients.

Web GUI: Monitor > DHCP > Server > Binding

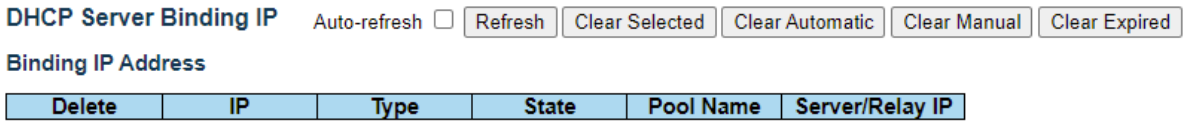


Figure 5-18: DHCP Server Binding IP

Table 5-17: DHCP Server Binding IP Parameters

Binding IP Address	
IP	IP address allocated to DHCP client.
Type	Type of binding. Possible types are Automatic, Manual, Expired.
State	State of binding. Possible states are Committed, Allocated, Expired.
Pool Name	The pool that generates the binding.
Server/Relay IP	Either IP address of dhcp server or, in case of relayed binding, IP address of relay agent through which binding was negotiated.
Buttons	• **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.

5.3.10 DHCP Server Declined IP

This section displays declined IP addresses.

Web GUI: Monitor > DHCP > Server > Declined IP

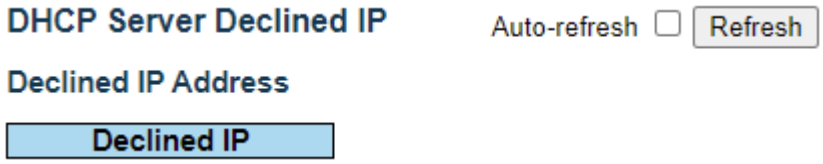


Figure 5-19: DHCP Server Declined IP

Table 5-18: DHCP Server Declined IP Parameters

Declined IP Address	
Display IP addresses declined by DHCP clients.	
Declined IP	List of IP addresses declined.

5.3.11 DHCP Detailed Statistics Port 1

This page provides statistics for DHCP snooping.

Notice that the normal forward per-port TX statistics is not increased if the incoming DHCP packet is done by L3 forwarding mechanism. And clear the statistics on specific port may not take effect on global statistics since it gathers the different layer overview.

Web GUI: Monitor > DHCP > Detailed Statistics

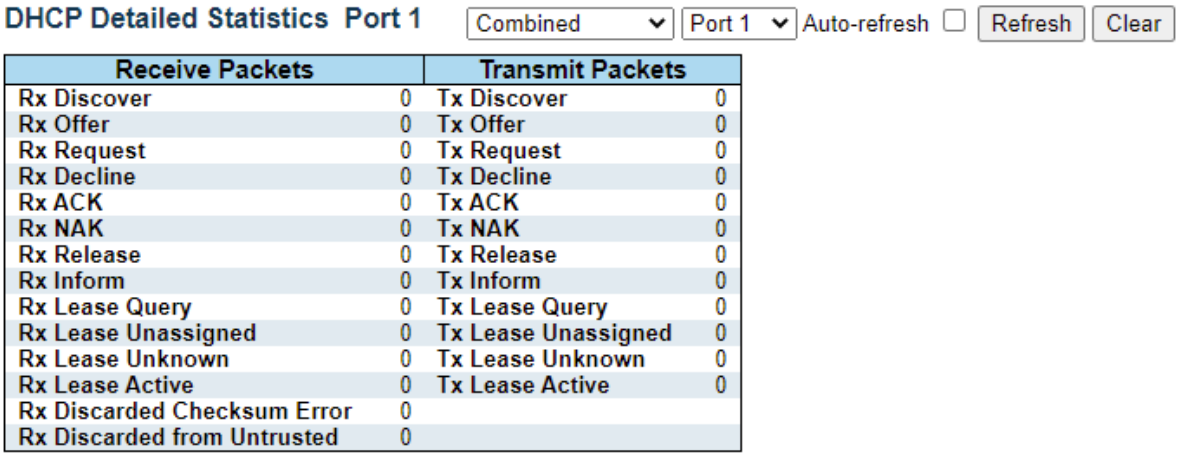


Figure 5-20: DHCP Detailed Statistics Port 1

Table 5-19: DHCP Detailed Statistics Port 1

DHCP Detailed Statistics Port 1	
Rx and Tx Discover	The number of of discover (option 53 with value 1) packets received and transmitted.
Rx and Tx Offer	The number of offer (option 53 with value 2) packets received and transmitted.
Rx and Tx Request	The number of request (option 53 with value 3) packets received and transmitted.
Rx and Tx Decline	The number of of decline (option 53 with value 4) packets received and transmitted.
Rx and Tx ACK	The number of ACK (option 53 with value 5) packets received and transmitted.
Rx and Tx NAK	The number of NAK (option 53 with value 6) packets received and transmitted.

DHCP Detailed Statistics Port 1	
Rx and Tx Release	The number of release (option 53 with value 7) packets received and transmitted.
Rx and Tx Inform	The number of inform (option 53 with value 8) packets received and transmitted.
Rx and Tx Lease Query	The number of lease query (option 53 with value 10) packets received and transmitted.
Rx and Tx Lease Unassigned	The number of lease unassigned (option 53 with value 11) packets received and transmitted.
Rx and Tx Lease Unknown	The number of lease unknown (option 53 with value 12) packets received and transmitted.
Rx and Tx Lease Active	The number of lease active (option 53 with value 13) packets received and transmitted.
Rx Discarded checksum error	The number of discard packet that IP/UDP checksum is error.
Rx Discarded from Untrusted	The number of discarded packet that are coming from untrusted port.

5.4 Simple Network Management Protocol (SNMP)

EdgeGM 7000 supports **SNMP** management, inspection and configuration.

The following screens are used to set SNMP System Configuration and SNMP Trap settings.

- SNMP System Configuration
- SNMPv3 Trap Configuration
- SNMPv3 Community Configuration
- SNMPv3 Users Configuration
- SNMPv3 Group Configuration
- SNMPv3 View Configuration
- SNMPv3 Access Configuration

5.4.1 SNMP System Configuration

Web GUI: Configuration > SNMP > System

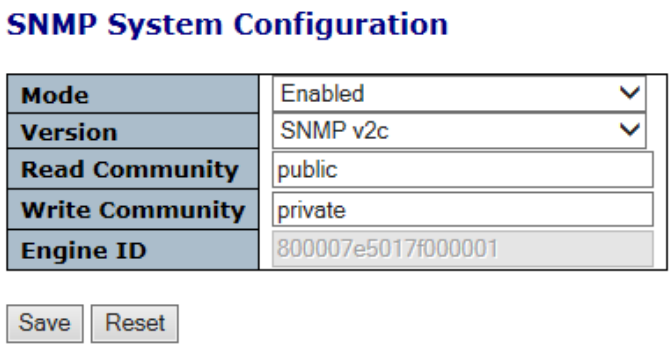


Figure 5-21: SNMP System Configuration display

Table 5-20: SNMP System Configuration Parameters

SNMP System Configuration	
Mode	Indicate 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 (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.

5.4.2 Trap Configuration

Configure the SNMP trap on this section.

Web GUI: Configuration > SNMP > System

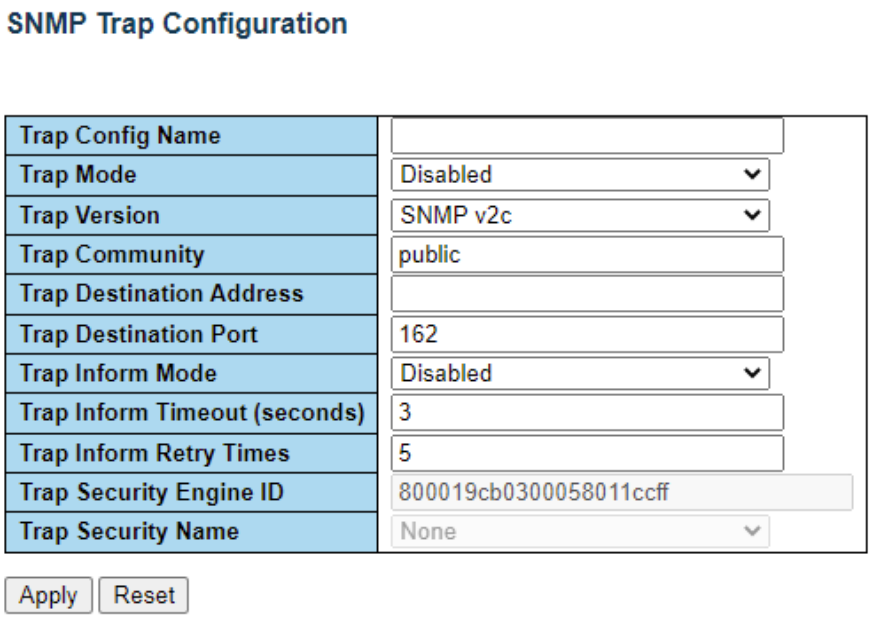


Figure 5-22: SNMP Trap Configuration display

Table 5-21: SNMP Trap Configuration Parameters

SNMP Trap Detailed Configuration	
Config Name	Indicates which trap Configuration's name for configuring. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Mode	Indicate the SNMP trap mode operation. Possible modes are: • **Enabled**: Enable SNMP trap mode operation. • **Disabled**: Disable SNMP trap mode operation.
Version	Indicate the SNMP trap version. Possible versions are: • **SNMP v1**: Set SNMP trap supported version 1. • **SNMP v2c**: Set SNMP supported version 2c. • **SNMP v3**: Set SNMP trap supported version 3.
Community	Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 63, and the allowed content is ASCII characters from 33 to 126.

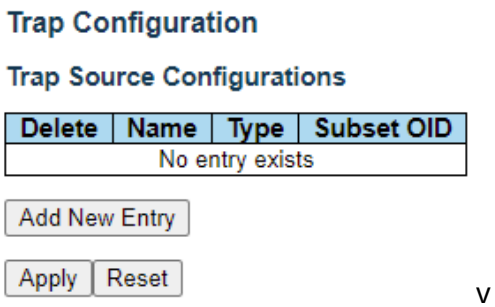
Destination Address	Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). And it also allows a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash. Indicates the SNMP trap destination IPv6 address. 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. It can also represent a legally valid IPv4 address. For example, ':: 192.1.2.34'.
Destination port	Indicates the SNMP trap destination port SNMP Agent will send SNMP message via this port; the port range is 1~65535.
Inform Mode	Indicates the SNMP trap inform mode operation. Possible modes are: • **Enabled**: Enable SNMP trap inform mode operation. • **Disabled**: Disable SNMP trap inform mode operation.
Inform Timeout (seconds)	Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.
Inform Retry Times	Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.
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. 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.
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.
Trap Event	
Configure SNMP trap on this page.	
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: Indicates that the SNMP entity is permitted to generate authentication failure traps. Possible modes are: • **Link Up**: Enable/disable Link up trap. • **Link Down**: Enable/disable Link down trap. • **LLDP**: Enable/disable LLDP trap.

Authentication	Indicates that the authentication group's traps. Possible traps are: SNMP 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.

5.4.3 Trap Source Configurations

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.

Web GUI: Configuration > SNMP > Trap > Source



v

Figure 5-23: SNMP Trap Source Configuration display

Table 5-22: SNMP Trap Source Configuration Parameters

Delete	Check to delete the entry. It will be deleted during the next save.
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 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

5.4.4 SNMPv3 Community Configuration

Configure SNMPv3 community table. The entry index key is “**Community”.**

Web GUI: Configuration > SNMP > Communities

Figure 5-24: SNMPv3 Community Configuration

Table 5-23: SNMPv3 Community Configuration Parameters

Delete	Check to delete the entry. It will be deleted during the next save.
Community Name	Indicates the security name to map the community to the SNMP Groups configuration. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
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 prefix.
Source Prefix	Indicates the SNMP access source address prefix.

5.4.5 SNMPv3 User Configuration

Configure **SNMP**v3 user table. The entry index keys are **Engine ID** and **Username.**

Web GUI: Configuration > SNMP > Users

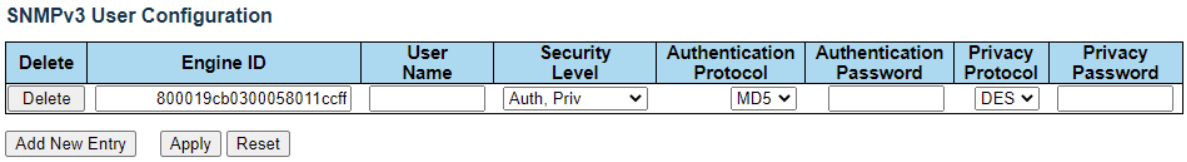


Figure 5-25: SNMPv3 User Configuration

Table 5-24: SNMPv3 User Configuration Parameters

SNMPv3 User Configuration	
Delete	Check to delete the entry. It will be deleted during the next save.

SNMPv3 User Configuration	
Engine ID	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number between 10 and 64 hexadecimal digits, 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.
Username	A string identifying the username 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 Level	Indicates the security model that this entry should belong to. Possible security models are: • **NoAuth**, **NoPriv**: No authentication and no privacy. • **Auth**, **NoPriv**: Authentication and no privacy. • **Auth**, **Priv**: Authentication and privacy. The value of security level cannot be modified if the entry already exists. This means that 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 is using MD5 authentication protocol. • **SHA**: An optional flag to indicate that this user is using SHA authentication protocol. The value of security level cannot be modified if the entry already exists. That means must first ensure that the value is set correctly.
Authentication Password	A string identifying the authentication password 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 ASCII characters from 33 to 126.

SNMPv3 User Configuration	
Privacy Protocol	Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are: • **None**: None privacy protocol. • **DES**: An optional flag to indicate that this user is using DES encryption standard • **AES**: An optional flag to indicate that this user uses AES authentication protocol.
Privacy Password	A string identifying the privacy password 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.

5.4.6 SNMPv3 Group Configuration

Configure **SNMPv3** groups table. The entry index keys are **Security Model** and **Security Name.**

Web GUI: Configuration > SNMP > Groups

SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
☐	v1	public	default_ro_group
☐	v1	private	default_rw_group
☐	v2c	public	default_ro_group
☐	v2c	private	default_rw_group

Add New Entry | Apply | Reset

Figure 5-26: SNMPv3 Group Configuration

Table 5-25: SNMPv3 Group Configuration Parameters

SNMPv3 Group Configuration	
Delete	Check the box 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.

5.4.7 SNMPv3 View Configuration

Configure **SNMPv3** views table. The entry index keys are **View Name** and **OID Subtree**.

Web GUI: Configuration > SNMP > Views

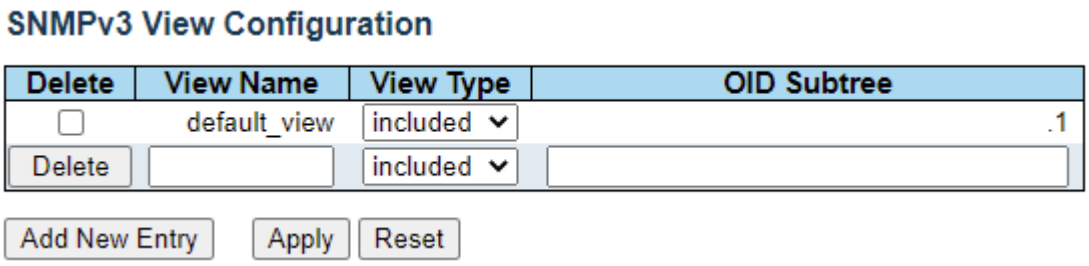


Figure 5-27: SNMPv3 View Configuration

Table 5-26: SNMPv3 View Configuration Parameters

SNMPv3 View Configuration	
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 is: • **Included**: An optional flag to indicate that this subtree view should be included. • **Excluded:** An optional flag to indicate that this subtree view should be excluded. ***Note:*** *In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and its OID subtree should overstep the 'excluded' view entry.*
OID Subtree	The OID defining the root of the sub tree to be added to the named view. The allowed OID length is 1 to 128. The allowed string content is a digital number or an asterisk (*).

5.4.8 SNMPv3 Access Configuration

Configure **SNMP**v3 accesses table. The entry index keys are **Group Name**, **Security Model** and **Security Level**.

Web GUI: Configuration > SNMP > Access

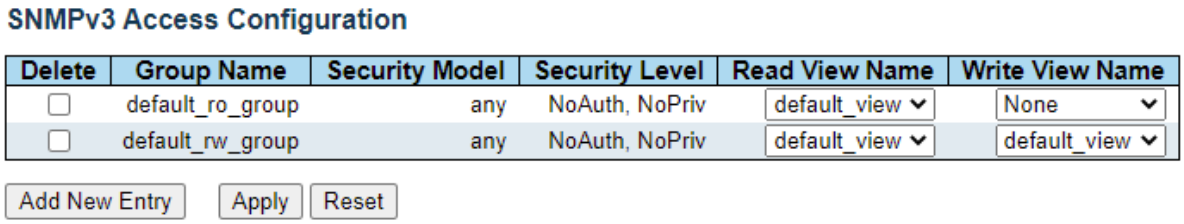


Figure 5-28: SNMPv3 Access Configuration

Table 5-27: SNMPv3 Access Configuration Parameters

SNMPv3 Access Configuration	
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:** Any security model accepted (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:** No authentication and no privacy. • **Auth, NoPriv:** Authentication and no 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.

5.5 Supported SNMP MIBs

The EdgeGM 7000 support a variety of MIBs. Future software versions will extend this list adding support for new features.

Note: In order to retrieve the required MIB, you must access VIAVI Web site/Support section.

To download the complete EdgeGM 7000 MIB pack refer to the Resources section in the VIAVI web site.

5.6 Command Line Interface (CLI)

CLI commands are used to manage the EdgeGM 7000 for displaying and modifying configuration of the various elements within the system.

Use one of the following methods to open a CLI session with the EdgeGM 7000:

- Connect the switch console port to a management station. For information about connecting to the console port, refer to Console Connection and Configuration.
- Open a Telnet session from a remote management station. The switch must have network IP connectivity with this remote management station.

Changes made by one Telnet user are reflected in all other Telnet sessions.

To Access EdgeGM 7000 via Telnet

Use any Telnet client application. The following example relates to Windows OS.

Start the “Run” option and in the command line enter:

“telnet XX.XX.XX.XX" (IP address of the EdgeGM 7000)

The Telnet screen prompts for a username and password.

Username: moose

Password: 1234

5.6.1 SSH Configuration

Secure Shell or SSH is a network protocol that allows exchange of data between two networked devices using a secure channel. SSH has been designed to replace Telnet and other insecure remote applications. The encryption deployed by SSH provides integrity of data.

Configure SSH in this section. See SSH Configuration.

5.6.2 HTTP Secure (HTTPS)

The EdgeGM 7000 supports secured web interface sessions using the HTTPS (HTTP over SSL) protocol.

HTTP 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.

See HTTPS Configuration.

5.7 Events Configuration

In this section, the user may change (enable/disable) the current events configuration.

5.7.1 Events Configuration table

Web GUI: Configuration > System > Events

Events Configuration

#	Event	Severity	Enable	Interface					Status	Counter	Clear
				SNMP	Syslog	CLI	SMTP	Flash			
*			☑	☑	☑	☑		☑			
1	Cold start	Info	☑	☑	☑	☑	☑	🟢	0	Clear	
2	Warm start	Info	☑	☑	☑	☑	☑	🟢	0	Clear	
3	Link down	Warning	☑	☑	☑	☑	☐	🟢	0	Clear	
4	Link Up	Info	☑	☑	☑	☑	☐	🔴	1	Clear	
5	SNMP Authentication failure	Notice	☑	☑	☑	☑	☐	🟢	0	Clear	
6	PSU state change	Notice	☑	☑	☑	☑	☑	🟢	0	Clear	
7	Temperature state change	Notice	☑	☑	☑	☑	☑	🟢	0	Clear	
8	CPU state change	Notice	☑	☑	☑	☑	☑	🟢	0	Clear	
9	SFP module plugged in	Info	☑	☑	☑	☑	☐	🟢	0	Clear	
10	SFP module unplugged	Info	☑	☑	☑	☑	☐	🟢	0	Clear	
11	SyncCenter state changed	Notice	☑	☑	☑	☑	☐	🟢	0	Clear	
12	SyncCenter selected input clock changed	Notice	☑	☑	☑	☑	☐	🟢	0	Clear	
13	SyncCenter input clock status changed	Notice	☑	☑	☑	☑	☐	🟢	0	Clear	
14	SyncCenter output quality changed	Notice	☑	☑	☑	☑	☐	🟢	0	Clear	
15	SyncCenter BITS output state changed	Notice	☑	☑	☑	☑	☐	🔴	1	Clear	
16	SyncCenter system clock state change	Notice	☑	☑	☑	☑	☐	🟢	0	Clear	
17	GPS status changed	Notice	☑	☑	☑	☑	☐	🔴	1	Clear	
18	GPS antenna status changed	Notice	☑	☑	☑	☑	☐	🔴	1	Clear	
19	PTP state changed	Notice	☑	☐	☑	☑	☐	🟢	0	Clear	
20	Device configuration changed	Info	☑	☑	☑	☑	☑	🟢	0	Clear	
21	Port security MAC limit	Warning	☑	☑	☑	☑	☐	🟢	0	Clear	
22	MEP status changed	Warning	☑	☑	☑	☑	☐	🟢	0	Clear	
23	Throughput Rx status overload	Warning	☑	☑	☑	☑	☐	🟢	0	Clear	
24	Throughput Tx status overload	Warning	☑	☑	☑	☑	☐	🟢	0	Clear	
25	Dying Gasp	Warning	☑	☑	☐	☐	☐	🟢	0	Clear	

Apply | Clear All | Reset

Figure 5-29: Events Configuration

Table 5-28 Events Configuration Parameters

Events Configuration	
#	Event Index.
Event	Unique Name of the Event.
Severity	The severity level of the listed events. The following severity types are supported: • **Informational**: Information level of the system log. • **Warning**: Warning level of the system log. • **Notice**: Made to help the memory.
Enable	Disable/Enable Event (Change will take effect on all checked interfaces: SNMP, syslog, cli).
Interface	Distribute event on a given interface: SNMP, SYSLOG, CLI, FLASH.
Status	Indication whether an event occurred or not.
Counter	The number of occurrences of the event since last Clear operation.
Clear	Clear event occurred indication.

5.8 Web Interface

To Access the EdgeGM 7000 through the Web Browse use the IP address of the device as described in the Getting Started chapter.

5.8.1 User Configuration & Edit User

This subsection 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.

Web GUI: Configuration > Security > Switch > Users

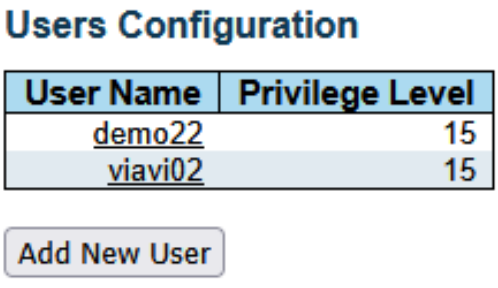


Figure 5-30: Users Configuration

Table 5-29: Users Configuration Parameters

Username	The name identifying the user. This is also a link to Add/Edit User display**.**
Privilege level	The privilege level of the user. The allowed range is **1** 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 must 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 etc.) need 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.

Edit a Username by clicking on the User Name field. The following is displayed.

Web GUI: Configuration > Security > Switch > Users | Click one of the users under the User Name column

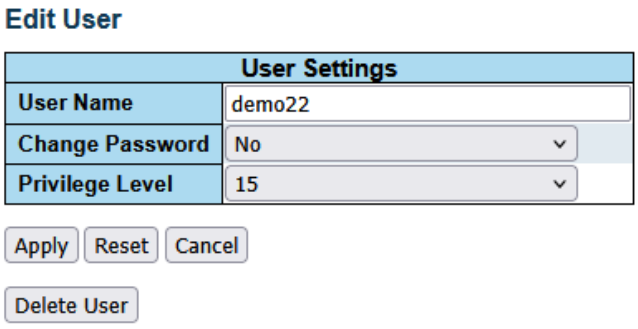


Figure 5-31: Edit User Configuration

Table 5-30: Edit Users Configuration Parameters

Username	A string identifying the username that this entry should belong to. The allowed string length is **1** to **31**. The valid username is a combination of letters, numbers and underscores.
Password	The password of the user. The allowed string length is **0** to **31**.
Privilege level	The privilege level of the user. The allowed range is **1** 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 must 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 etc.) need 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.

By clicking “Add New User” you get the: Add User” display to add a new user.

Web GUI: Configuration > Security > Switch > Users | Add New User

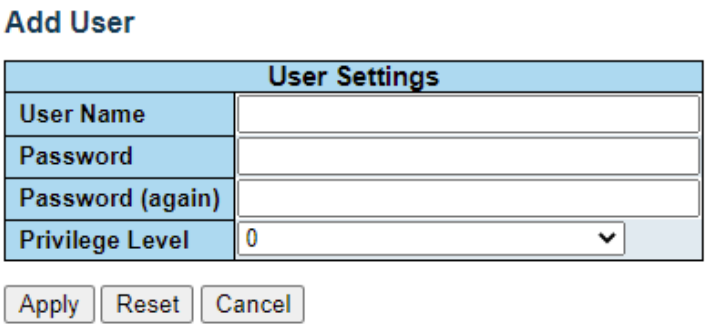


Figure 5-32: Add User Configuration

The Parameters are the same as reported in the above table.

5.8.2 Authentication Method Configuration

The EdgeGM 7000 support multiple methods for user login authentication. The configured authentication method is applied to all user interfaces (console, Telnet/SSH and Web). The available methods in current version are shown in the following display:

Web GUI: Configuration > Security > Switch > Auth Method

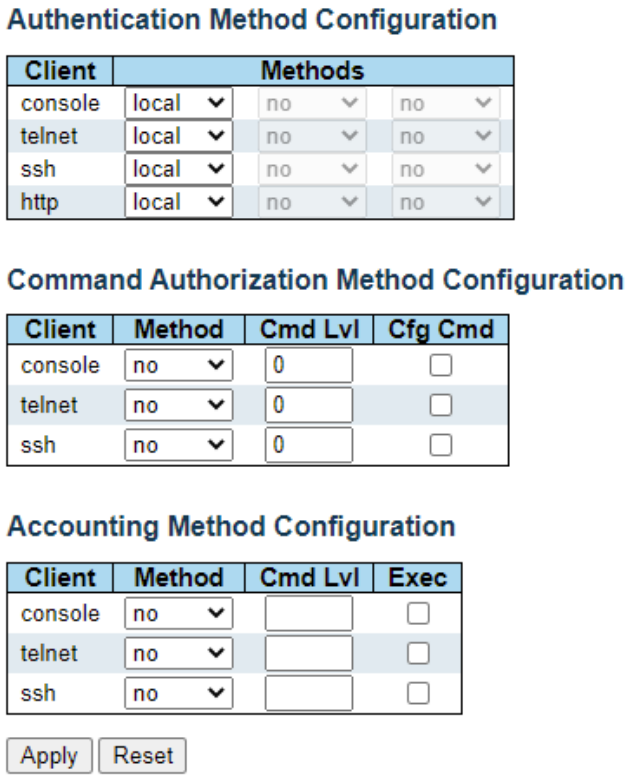


Figure 5-33: Authentication Method Configuration

To access the related setup, go to: Authentication Method Configuration.

5.8.3 Authentication Servers Configuration

This section allows the user to configure the different RADIUS Authentication Servers

To access this section, go to Authentication Server Configuration (AAA).

5.8.4 Access Management Configuration

In this section, you may configure the access management configuration

The maximum number of entries is **16**. If the application types match any one of the access management entries, it will allow access to the switch.

To configure the Access Management Configuration, go to: Access Management Configuration.

5.9 RMON Overview

The RMON Overview includes the following displays:

- RMON Statistics Status Overview
- RMON History Overview
- RMON Alarm Overview
- RMON Event Overview

5.9.1 RMON Statistics Status Overview

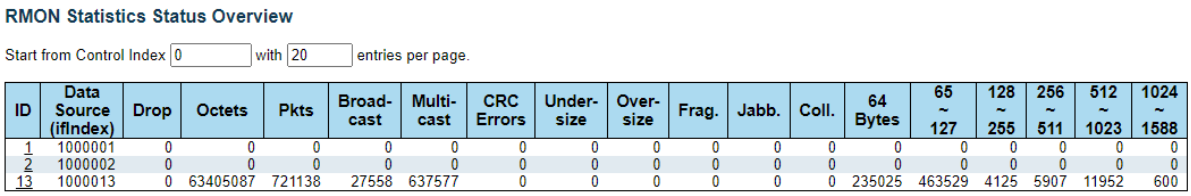
This page provides an overview of RMON Statistics entries.

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. The "Start from Event Index and Log Index" allows the user to select the starting point in the Event table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest Event table match.

The **>>**will use the last entry of the currently displayed entry 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.

Web GUI: Monitor > Advanced > RMON > Statistics



RMON Statistics Status Overview

Start from Control Index 0 with 20 entries per page.

ID	Data Source (ifIndex)	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
1	1000001	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	1000002	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	1000013	0	63405087	721138	27558	637577	0	0	0	0	0	0	235025	463529	4125	5907	11952	600

Figure 4-5-34: Rmon Statistics Status Overview

Table 5-31: Rmon Statistics Status Overview Parameters

RMON Statistics Status Overview	
ID	Indicates the index of History control entry.
Data Source (ifIndexif)	The port ID which must be monitored.
Drop	The value of sysUpTime at the start of the interval over which this sample was measured.
Octets	The total number of events in which packets were dropped by the probe due to lack of resources.
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 the multicastaddress.
CEC Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error)
Under size	The total number of packets received that were less than 64 octets.
Over size	The total number of packets received that were longer than 1518 octets.
Frag.	The number of frames of a size lesser than 64 octets received with invalid CRC.
Jabb.	The number of frames which size is larger than 64 octets received with invalid CRC.
Coll.	The total number of octets of data (including those in bad packets) received on the network.
64	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.
1024~1588	The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length

5.9.2 RMON History Overview

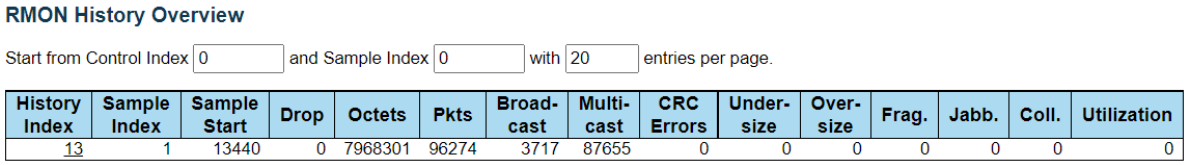
This section provides an overview of RMON History entries. Each page shows up to 99 entries from the Event table, default being 20, selected through the "entries per page" input field.

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.

The "Start from Event Index and Log Index" allows the user to select the starting point in the Event table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest Event table match.

The **>>** will use the last entry of the currently displayed entry 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.

Web GUI: Monitor > Advanced > RMON > History


RMON History Overview

Start from Control Index 0 and Sample Index 0 with 20 entries per page.

History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
13	1	13440	0	7968301	96274	3717	87655	0	0	0	0	0	0	0

Figure 5-35: Rmon History Overview

Table 5-32: Rmon History Overview Parameters

RMON History Overview	
History Index	Indicates the index of History control entry.
Sample Index	Indicates the index of. the data entry associated with the control entry.
Sample Start	The value of sysUpTime at the start of the interval over which this sample was measured.
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.
CECErrors	The total number of packets received that had a length (excluding framing bits but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
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 which size is less than 64 octets received with invalid CRC.
Jabb.	The number of frames which size is larger than 64 octets received with invalid CRC.
Coll.	The best estimate of the total number of collisions on this Ethernet segment.
Utilization	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

5.9.3 RMON Alarm Overview

This section provides an overview of RMON Alarm entries.

Web GUI: Monitor > Advanced > RMON > Alarm

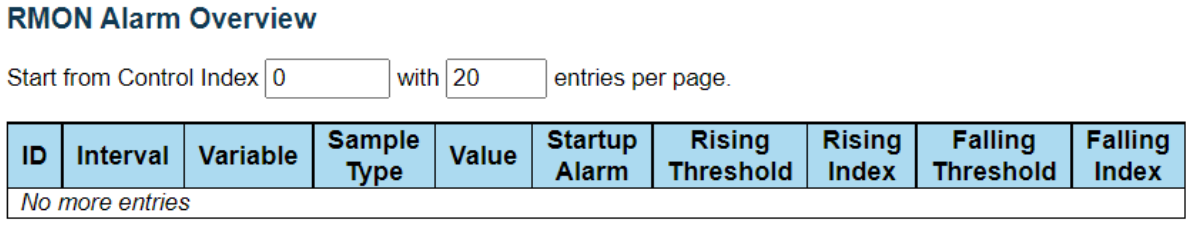


Figure 5-36: Rmon Alarm Overview

Table 5-33: Rmon Alarm Overview Parameters

RMON Alarm Overview	
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
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 "Start from Event Index and Log Index" allows the user to select the starting point in the Event table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest Event table match. The **>>** will use the last entry of the currently displayed entry 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.	

5.9.4 RMON Event Overview

This section 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.

The "Start from Event Index and Log Index" allows the user to select the starting point in the Event table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest Event table match.

The **>>** will use the last entry of the currently displayed entry 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.

Web GUI: Monitor > Advanced > RMON > Event

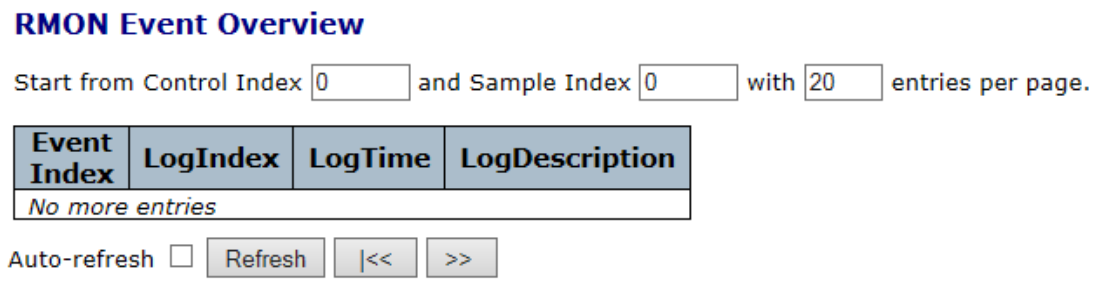


Figure 5-37: Rmon Event Overview

Table 5-34: Rmon Alarm Overview Parameters

RMON Event Overview	
Event Index	Indicates the index of the event entry.
Log Index	Indicates the index of the log entry.
Log Time	Indicates Event log time
Log Description	Indicates the Event description

6 Diagnostics

The following topics are discussed in this chapter:

- Diagnostics Overview
- Ping IPv4
- Ping IPv6
- Link OAM MIB Retrieval
- VeriPHY Cable Diagnostics

This page intentionally left blank.

6.1 Diagnostics Overview

Diagnostics include the following procedures:

- Ping
- Ping6
- Link OAM MIB Retrieval
- Copper Link Test
- RFC2544
- EdgeGM 7000 Report Configuration

6.2 Ping IPv4

This section allows the user to issue ICMP PING packets to troubleshoot IP connectivity issues.

After you press, Start ICMP packets are transmitted, and the sequence number and round-trip time are displayed upon reception of a reply. The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested data space (the ICMP header). The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

PING server 10.10.132.20, 56 bytes of data.

64 bytes from 10.10.132.20: icmp_seq=0, time=0ms
64 bytes from 10.10.132.20: icmp_seq=1, time=0ms
64 bytes from 10.10.132.20: icmp_seq=2, time=0ms
64 bytes from 10.10.132.20: icmp_seq=3, time=0ms
64 bytes from 10.10.132.20: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad

The IP Address and Ping Size Parameters of the issued ICMP packets (for ICMP Ping) can be configured.

Web GUI: Diagnostics > Ping (IPv4)

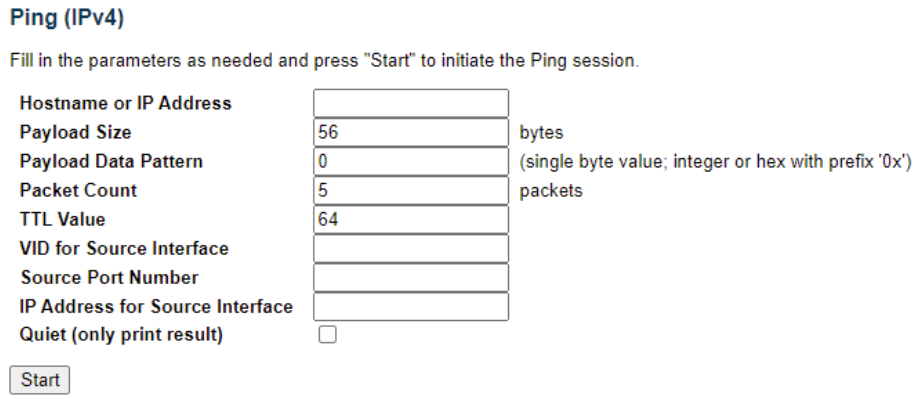


Figure 6-1: ICMP PING Configuration

Table 6-1 Ping (IPv4)

Hostname or IP Address	The address of the destination host, either as a symbolic hostname or an IP Address.
Payload Size	Determines the size of the ICMP data payload in bytes (excluding the size of Ethernet, IP and ICMP headers). The default value is 56 bytes. The valid range is 2-1452 bytes.
Payload Data Pattern	Determines the pattern used in the ICMP data payload. The default value is 0. The valid range is 0-255.
Packet Count	Determines the number of PING requests sent. The default value is 5. The valid range is 1-60.
TTL Value	Determines the Time-To-Live /TTL) field value in the IPv4 header. The default value is 64. 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.*
Source Port Number	This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the Source Port Number 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.

Quiet (only print result)	Checking this option will not print the result of each ping request but will only show the final result. After you press , ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply. The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested payload data size (the difference is the ICMP header). The page refreshes automatically until responses to all packets are received, or until a timeout occurs. The output from the command will look like the following: PING 172.16.1.1 (172.16.1.1) from 172.16.1.10: 56 data bytes 64 bytes from 172.16.1.1: seq=0 ttl=64 time=2.034 ms 64 bytes from 172.16.1.1: seq=1 ttl=64 time=1.729 ms 64 bytes from 172.16.1.1: seq=2 ttl=64 time=1.954 ms 64 bytes from 172.16.1.1: seq=3 ttl=64 time=1.699 ms 64 bytes from 172.16.1.1: seq=4 ttl=64 time=1.916 ms --- 172.16.1.1 ping statistics --- 5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 1.699/1.866/2.034 ms

6.3 Ping IPv6

EdgeGM 7000 allow you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.
After you press Start, 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

Web GUI: Diagnostics > Ping (IPv6)

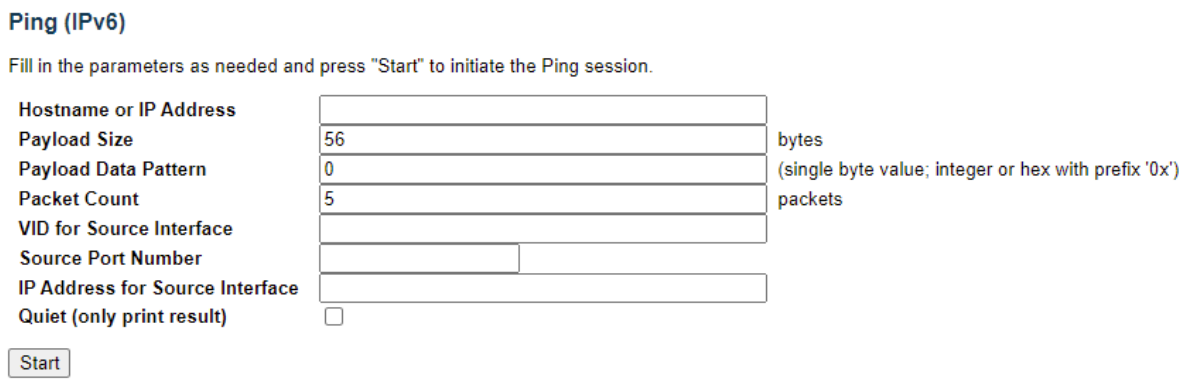


Figure 6-2: ICMPv6 PING Configuration

PING6 server ff02::2, 56 bytes of data.

64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=0, time=10ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=0, time=10ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=1, time=0ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=1, time=0ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=2, time=0ms

64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=2, time=0ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=3, time=0ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=3, time=0ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=4, time=0ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=4, time=0ms

Sent 5 packets, received 10 OK, 0 bad

You can configure the following properties of the issued ICMP packets

Table 6-2: ICMP PING Parameters

IP Address	The destination IP Address.
Ping Length	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.
Ping Count	The count of the ICMP packet. Values range from 1 time to 60 times.
Ping Interval	The interval of the ICMP packet. Values range from 0 second to 30 seconds.
Egress Interface (Only for IPv6)	The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet goes. The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid. When the egress interface is not given, PING6 finds the best match interface for destination. Do not specify egress interface for loopback address. Do specify egress interface for link-local or multicast address.
Buttons	**Start**: Click to start transmitting ICMP packets. **New Ping**: Click to re-start diagnostics with PING.

6.4 Link OAM MIB Retrieval

This procedure allows the user to retrieve the local or remote OAM MIB variable data on a particular port.

1. Select the appropriate radio button and enter the port number of the switch to retrieve the content of interest.
2. Click on Start to retrieve the content.
3. Click on New Retrieval to retrieve another content of interest.

Web GUI: Diagnostics > Link OAM > MIB Retrieval

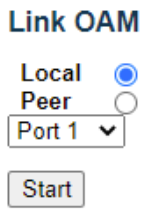


Figure 6-3: Link OAM MIB Retrieval display.

6.5 VeriPHY Cable Diagnostics

This section is used for running the VeriPHY Cable Diagnostics for 10/100 and 1G copper ports.

Web GUI: Diagnostics > VeriPHY

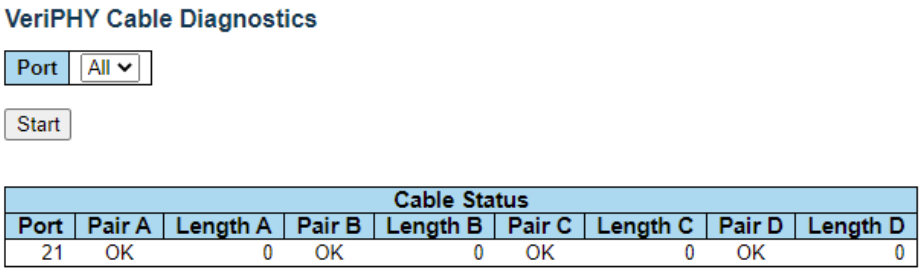


Figure 6-4: Copper Link Test Cable Status Diagnostics

Press **Start** to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table.

Note that VeriPHY is only accurate for cables of length 7 — 140 meters.

10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete

Table 6-3: Copper Link Test Cable Diagnostics Parameters

Port	The port where the Cable Diagnostics is requested.
Cable Status	"**Port"**: Port number. **"Pair"**: The status of the cable pair. OK - Correctly terminated pair Open - Open pair Short - Shorted pair Short A - Cross-pair short to pair A Short B - Cross-pair short to pair B

	Short C - Cross-pair short to pair C Short D - Cross-pair short to pair D Cross A - Abnormal cross-pair coupling with pair A Cross B - Abnormal cross-pair coupling with pair B Cross C - Abnormal cross-pair coupling with pair C Cross D - Abnormal cross-pair coupling with pair D “Length”: The length (in meters) of the cable pair. The resolution is 3 meters

7 Maintenance

The following topics are discussed in this chapter:

- Maintenance Overview
- Restart Device
- Factory Defaults
- Software Management
- Configuration Management
- Power Supply Overview

This page intentionally left blank.

7.1 Maintenance Overview

The Maintenance includes the following procedures:

- Restart Device
- Factory Default
- System Update
- Configuration (Save/Upload)

7.2 Restart Device

You can restart the switch here. After restart, the switch will boot normally. **Web GUI: Maintenance > Restart Device**

Figure 7-1: Restart Device Screen

Table 7-1: Restart Device Parameters

Yes:	Click to restart device.
No:	Click to return to the Port State page without restarting.

7.3 Factory Defaults

You can reset the configuration of the switch. Only the IP configuration is retained.

The new configuration is available immediately, which means that no restart is necessary.

Web GUI: Maintenance > Factory Defaults

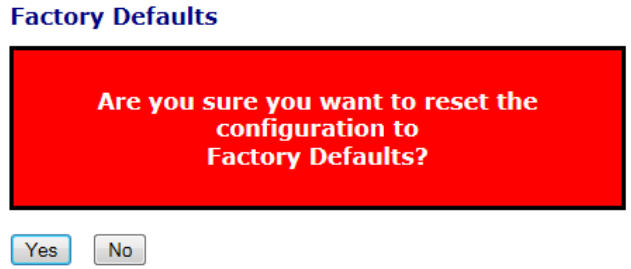


Figure 7-2: Restore to Factory Defaults Screen

Table 7-2: Restore to Factory Defaults Parameters

Yes:	Click to reset the configuration to Factory Defaults.
No:	Click to return to the Port State screen without resetting the configuration.

Note: Restoring factory default can also be performed by making a physical loopback between port 1 and port 2 within the first minute from switch reboot. In the first minute after boot, 'loopback' packets will be transmitted at port 1. If a 'loopback' packet is received at port 2 the switch will do a restore to default

7.4 Software Management

This section facilitates an update of the firmware controlling the switch.

Web GUI: Maintenance > Software > Upload

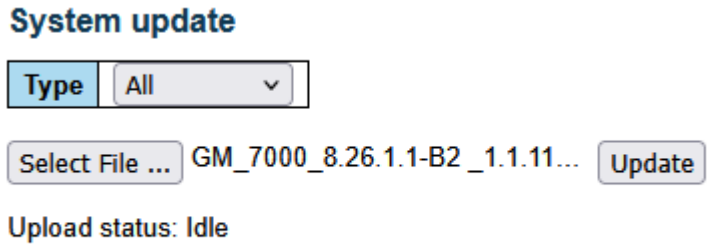


Figure 7-3: Software Upload

Table 7-3: Software Upload Parameters

Type:	Select the type of image file to upload: - SW only: Software image only (file_name.gz) - FPGA only: FPGA image only (file_name.rbf) - All: a combined file
Select File:	Browse to the location of the image file and click **Select**.
Update	Click to start the upgrade
After the image is uploaded, a page announces that the firmware update is initiated. After a few moments, the software/firmware is updated and the switch restarts.	

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

7.4.1 Software Image Select

This section 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.

Web GUI: Maintenance > Software > Image Select

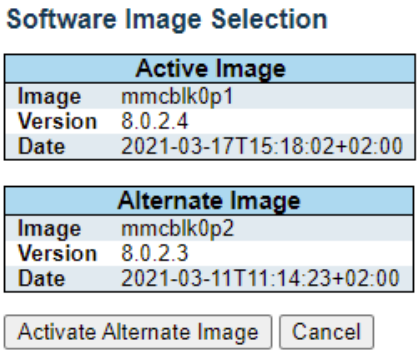


Figure 7-4: Software Image Selection

Table 7-4: Software Image Selection Parameters

Image	The file name of the firmware image, from when the image was last updated.
Version	The version of the firmware image.
Date	The date where the firmware was produced.
Buttons	**Activate Alternate Image**: Click to use the alternate image. This button may be disabled depending on system state. **Cancel:** Cancel activating the backup image. Navigates away from this page.

7.5 Configuration Management

The switch stores its configuration in several text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch. The available files are:

- ***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. If this file doesn't exist at boot time, the switch will start up in default configuration
- ***Default-config*****:** A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings
- **Up to 31 other files**, typically used for configuration backups or alternative configurations.

7.5.1 Save startup configuration

This copies *running-config* to *startup-config*, thereby ensuring that the currently active configuration will be used at the next reboot.

Web GUI: Maintenance > Configuration > Save Startup Config

Figure 7-5: Save Startup Configuration File

7.5.2 Download Configuration

It is possible to download any of the files on the switch to the web browser. Select the file and click **Download Configuration**. Download of *running-config* may take a little while to complete, as the file must be prepared for download.

Web GUI: Maintenance > Configuration > Download

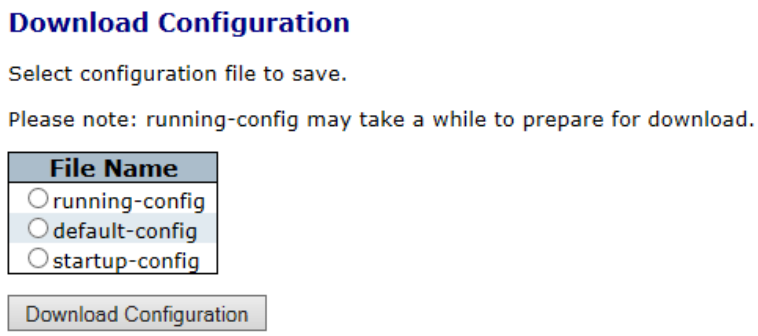


Figure 7-6: Download Configuration

7.5.3 Upload Configuration

Web GUI: Maintenance > Configuration > Upload

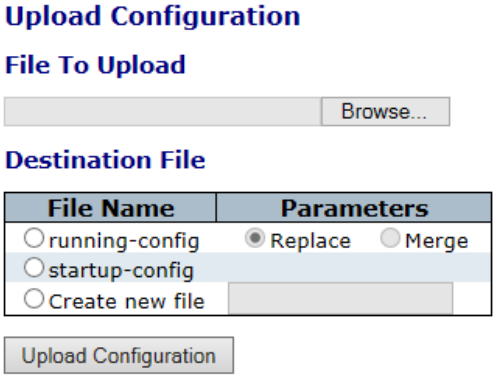


Figure 7-7: Upload Configuration

It is possible to upload a file from the web browser to all the files on the switch, except *default-config* which is read-only. Select the file to upload, select the destination file on the

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

7.5.4 Activate

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 **Activate Configuration**. This will initiate the process of completely replacing the existing configuration with that of the selected file.

Web GUI: Maintenance > Configuration > Activate

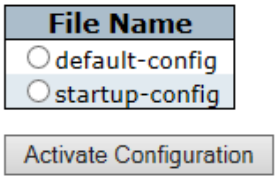


Figure 7-8: Activate Configuration

7.5.5 Delete

It is possible to delete any of the writable files stored in flash, including *startup-config*. If this is done and the switch is rebooted without a prior Save operation, this effectively resets the switch to default configuration.

Web GUI: Maintenance > Configuration > Delete

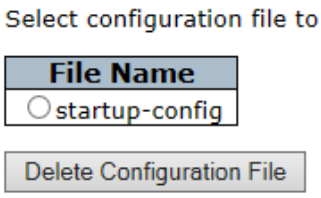


Figure 7-9: Delete Configuration

7.6 Power Supply Overview

Warning 	The designated VIAVI Power Supply (AC or DC) is the ONLY power supply suitable to be used with the R Class models. Any other type of power supply module (VIAVI products or other), even if mechanically matching, may cause irreversible damage to the system. IN SUCH CASES THIS WILL VOID ANY WARRANTY!
FR Attention	L'alimentation VIAVI désignée (AC ou DC) est la SEULE alimentation appropriée pour être utilisée avec les modèles de classe R. Tout autre type de module d'alimentation (produits VIAVI ou autre), même s'il est mécaniquement adapté, peut causer des dommages irréversibles au système. DANS DE TELS CAS, CELA ANNULERA TOUTE GARANTIE !
Warning 	NEVER OPEN THE DEVICE WHEN IT IS CONNECTED TO POWER LINES!
FR Attention	N'OUVREZ JAMAIS L'APPAREIL LORSQU'IL EST CONNECTÉ À DES LIGNES ÉLECTRIQUES !
Caution 	When connecting a device to an AC (DC) power outlet, always: 1. Connect the power cord to the device first (ensure that it is securely fastened). 2. After the power cord is connected to the device, plug it into the wall outlet. Make sure to use grounded (3 way) outlets (for AC models).
FR Attention	Lors de la connexion d'un appareil à une prise de courant CA (CC), toujours : 1. Connectez d'abord le cordon d'alimentation à l'appareil (assurez-vous qu'il est bien fixé). 2. Une fois le cordon d'alimentation connecté à l'appareil, branchez-le dans la prise murale. Assurez-vous d'utiliser des prises de terre (3 voies) (pour les modèles CA).

Note: For most countries VIAVI ships an appropriate power supply cord which is safety approved in accordance with the country's National Electric Code.

For certain countries Products are shipped without power cords. In such cases, locally purchased safety approved power cords (in accordance with that country's National Electric Code) may be used.

7.6.1 AC Power Supply

Connect AC line voltage using the power supply cords provided (alternatively you may use other 18AWG three wire cord). The device will accept any line voltage from 100 to 240 VAC, 50-60 Hz. There is no ON/OFF switch on the device. When the power is connected to the device, the device is ON. This will be indicated by the Power (PWR) LED lit green on the front panel. The PS is rated for ambient temperature of: -10°C ÷ +50°C.

125VDC Connection: In this case, the supplied AC cable allows the connection to an external DC source of 125VDC.

7.6.2 DC Power Supplies

Connect DC line voltage using the power supply cords provided (alternatively you may use other 18AWG three wire cord). The device will accept any line voltage from 20 to–60VDC. There is no ON/OFF switch on the device. When the power is connected to the device, the device is ON. This will be indicated by the Power (PWR) LED lit green on the front panel.

Note: The earthen conductor of power cord must be grounded.

–20 to – 60VDC Power Connection

The rear panel is equipped with a suitable screw connection (ST connector).

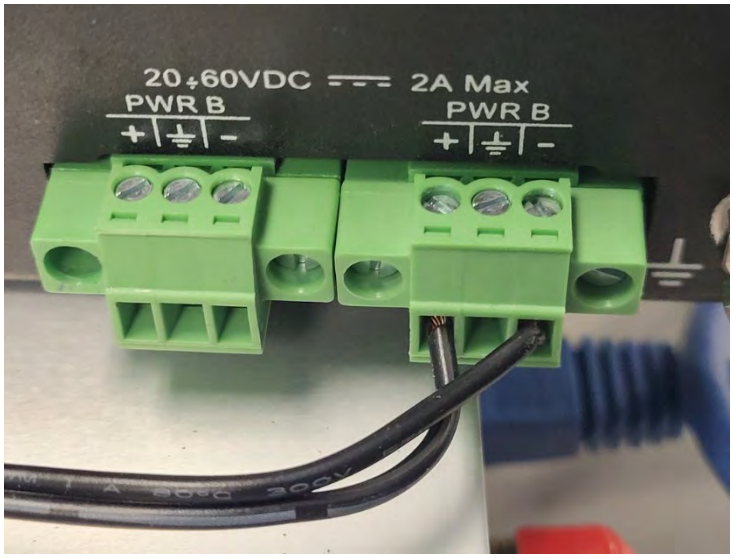


Figure 7-10: EdgeGM 7000 series DC PS rear panel ST connector

DC powered models**:** Required current rating = 2A

CAUTION DOUBLE POLE FUSING

Verify that the DC-Mains provide a 2 Amp double pole circuit breaker. Required power conductor size = at least 0.75mm² for flexible cable or 1mm² for non-flexible.

(FR) ATTENTION FUSIBLES DOUBLE PÔLE

Vérifiez que le secteur CC fournit un disjoncteur bipolaire de 2 Amp. La taille requise du conducteur d'alimentation doit être d'au moins 0,75 mm² pour un câble flexible ou de 1 mm² pour un câble non flexible.

Power Consumption (AC and DC Power Supplies):

- Maximum <25W
- Typical <20W

7.7 Laser Safety

Laser Warning 	CAUTION! Radiation emitted from fiber optic ports may be hazardous to human vision. Therefore, the following rules must be strictly observed: • All single-mode (SM) models are CLASS I LASER PRODUCT that may endanger your eyes and must be handled with special care. When not in use, keep the fiber optic connector closed using its protective cover. • Never stare directly into the fiber optic connector of a powered device or into the end of a fiber connected to it.
Laser Safety	The emissions produced by the end products described in this guide are under Class 1 emission level according to IEC 60825-1 2007 These products shall not be installed in an optical network handling above Class 1 level

Avertissement Laser 	PRUDENCE ! Le rayonnement émis par les ports de fibre optique peut être dangereux pour la vision humaine. Par conséquent, les règles suivantes doivent être strictement respectées : • Tous les modèles monomodes (SM) sont des PRODUITS LASER DE CLASSE 1 qui peuvent mettre en danger vos yeux et doivent être manipulés avec un soin particulier. Lorsqu'il n'est pas utilisé, maintenez le connecteur fibre optique fermé à l'aide de son capot de protection. • Ne regardez jamais directement dans le connecteur de fibre optique d'un appareil alimenté ou dans l'extrémité d'une fibre qui y est connectée.
Sécurité Laser 	Les émissions produites par les produits finaux décrits dans ce guide sont sous le niveau d'émission de classe 1 selon la norme CEI 60825-1 2007 Ces produits ne doivent pas être installés dans un réseau optique traitant au-dessus du niveau de classe 1

This page intentionally left blank.

8 Glossary of Terms

Acronym	Description
ACL	Access Control List
AIS	Alarm Indication Signal
ALD	Autonomous Link Discovery
ARP	Address Resolution Protocol
BPDU	Bridge Protocol Data Unit
CBWFQ	Frame Lost Weighted Fair Queuing
CC	Continuity Check
CCM	Continuity Check Message
CDP	Cisco Discovery Protocol
CE	Customer Edge (Equipment)
CFM	Connectivity Fault Management (IEEE 802.1ag)
CIR	Committed Insured Rate
CLI	Command Line Interface
CLNP	Connectionless Network Protocol
CMIP	Common Management Info Protocol
CoS	Class of Service
CPE	Customer Premises Equipment
CSF	Client Signal Fail
CSMA/CD	Carrier Sense Multiple Access with Collision Detection

Acronym	Description
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DM	Delay measurement
DMAC	Destination MAC address
DMM	Delay Measurement Message
DMR	Delay Measurement Reply
DNS	Domain Name System
DSCP	Differentiated Services Code Point
EAP	Extensible Authentication Protocol
ECFM	Ethernet Connectivity Fault Management
EEC	Synchronous Ethernet Equipment clock
EFM	Ethernet in the First Mile
EMS	Element Management System
ELPS	Ethernet Linear Protection Switching
ERPS	Ethernet Ring Protection Switching
EVC	Ethernet Virtual Connection
EVPL	Ethernet Virtual Private Line
FD	Frame Delay
FDV	Frame delay variation
FDX	Full Duplex
FEF	Far End Fault

Acronym	Description
FP	Fault Propagation
FTP	File Transfer Protocol
FTTB	Broadband Access Over Fiber
FTTB MDU	Broadband Access Over Fiber Multi Dwelling Unit
Gbps	Gigabits per second
HDLC	High-Level Data Link Control
HDX	Half Duplex
FDX	Full Duplex
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
ICMP	Internet Control Message Protocol
IEEE	Institute of Electronic and Electronic Engineers developing the standards for communications and networks. IEEE Number IEEE 802 standards Number and Description 802.1d – Spanning Tree Protocol 802.1w – Rapid Spanning Tree 802.1s – Multiple Instance Spanning Tree 802.1q – VLAN Frame Tagging 802.2 – Logical Link Control 802.3 – Ethernet (CSMA/CD) 802.3u – Fast Ethernet 802.3z – Gigabit Ethernet 802.1ab – LLDP= Link Layer Discovery Protocol

Acronym	Description
	802.3ad – LACP=Link Aggregation Control Protocol 802.3ah – Link OAM
IETF	Internet Engineering Task Force
ITU-T	International Telecommunication Union Telecommunication
IEEE 802.1X	IEEE Standard for port based Network Access Control
MLD	Interior Gateway Media Protocol Internet Group Management Protocol
MLD Querier	A router sends MLD query messages over a particular link. This router is called the Querier.
IP	Internet Protocol
IPX	Internetwork Packet Exchange
ISO	International Standardization Organization
LAG	Link Aggregation Group
LAN	Local Area Network
LACP	Link Aggregation Control Protocol
Last Gasp – Dying Gasp	Remote Device Power Failure
LB	Loop-Back
LBM	Loop-back Message
LBR	Loop-back reply
LCK	Locked Signal
LDP	Label Distribution Protocol

Acronym	Description
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LM	Loss measurement
LOC	Loss of continuity
LMM	Loss Measurement Message
LMR	Loss Measurement Reply
LTM	Link Trace Message
LTR	Link Trace Reply
LOS	Loss of Signal
LST	Link Segmentation Test
LTM	Link Trace Message
LTR	Link Trace Reply
MA	Media Access & Maintenance Association
MAC	Media Access Control
MAC Address	Media Access Control Address (hardware address, MAC-layer address, physical address)
MA	Maintenance Association
MA™	Micro Agent (an on-chip management system facilitating the management and maintenance of remote access devices)
MAID	Maintenance Association Identifier
MAU	Media Attachment Unit
MD	Maintenance Domain

Acronym	Description
MDU	Multi Dwelling Unit
MEF	Metro Ethernet Forum
MEG	Maintenance Entity Group
MEL	MEG Level
MEP	Maintenance Entity Point
MIB	Management information base
MIP	Maintenance Immediate Point
MNCP	Maximum Number of Cells Packed
MPLS	Multi-Protocol Label Switching
MPLS-TP	MPLS Transport Profile
MTTR	Mean time to repair
MTU	Maximum Transmission Unit
MTU-s	Multi Tenant Unit- switch
NCP	Netware Core Protocol
NetBIOS	Network Basic Input/Output System
NFS	Network File System
NGN	Next Generation Network
NGN Access	Next Generation Network Access
NIC	Network Interface Card
NMS	Network Management System
NTP	Network Time Protocol

Acronym	Description
NTU	Network Termination Unit
NU	Node Unit
OA	Operation and Administration,
OAM	Operation, Administration, Management
ODI	Open Data-link Interface
OpEx	Operating Expenditures
Optional TLVs	A LLDP frame contains multiple TLVs
OSI	Open System Interconnection
OSPF	Open Shortest Path First
OUI	Organization Unique Identifier
PE	Provider Edge
PM	Performance monitoring
PRC	Primary Reference Clock
PIR	Peak Information Rate
Policer	A Policer can limit the bandwidth of received frames. It is located in front of the ingress queue
POST	Power-on Self Test
PPP	Point-to-Point Protocol
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
PW	Pseudowire

Acronym	Description
QCE	Quality of Service Control List Entries
QCL	Quality of Service Control List
Q-in-Q	Selective Q-in-Q per IEEE802.1ad Provider Bridging
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RARP	Reverse Address Resolution Protocol
RDI	Remote Defect Indication
RIP	Routing Information Protocol
RMON	Remote Monitoring
RSTP	Rapid Spanning Tree Protocol (IEEE 802.1w)
Rx	Receive
SFP	Small Form-factor Pluggable
SLA	Service Level Management
SLE	Subscriber Link Emulation
SMAC	Source MAC address
SNMP	Simple Network Management Protocol
SPX	Sequenced Packet Exchange
SSH	An acronym for Secure Shell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices.
SSM	Synchronization Status Messages
STA	Spanning Tree Algorithm

Acronym	Description
STP	Spanning Tree Protocol
SU	Subscriber Unit
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)
TACACS+	Terminal Access Controller Access Control System Plus
TCM	Three Color Marker
TCO	Total cost of ownership
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
Telnet	Standard terminal emulation protocol in the TCP/IP protocol stack
TFTP	It is an acronym for Trivial File Transfer Protocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading,
TLV	It is an acronym for Type Length Value. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV
ToS	It is an acronym for Type of Service. It is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header.
TrTCM	Two rate Three Color Marker
TTL	Time To Live
TST	Test PDU
Tx	Transmit
UI	User Interface

Acronym	Description
UNI	User Network Interface
UPnP	It 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
UTC	Coordinated Universal Time/International Atomic Time
VLAN	Virtual Local Area Network
VLAN ID	VLAN Identifier
WAN	Wide Area Network
WDM	Wavelength-division multiplexing

8.1 Alphabetical Glossary of Terms

ACE

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.

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 Ports 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" - page. 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: Under this page you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per seconds. Under "Ports" and "Access Control List" web-pages you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

AES

AES is an acronym for Advanced Encryption Standard. The encryption key protocol is applied in 802.1i 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 Auto Media Select. AMS is used for dual media ports (ports supporting both copper (cu) and fiber (SFP) cables. AMS automatically determines if a 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 Automatic Protection Switching. This protocol is used to secure that switching is done bidirectional in the two 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 Address Resolution Protocol. 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.

CC

CC is an acronym for Continuity Check. 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 Continuity Check Message. It is a OAM frame transmitted from a MEP to it's peer MEP and used to implement CC functionality.

CDP

CDP is an acronym for Cisco Discovery Protocol.

DEI

DEI is an acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.

DES

DES is an acronym for Data Encryption Standard. 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 Dynamic Host Configuration Protocol. 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 (in standalone switch it always equal 0, in stackable switch it means switch 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 Domain Name System. 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 Denial of Service. 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.

Drop Precedence Level

Every incoming frame is classified to a Drop Precedence Level (DP level), which is used throughout the device for providing congestion control guarantees to the frame according to what was configured for that specific DP level. A DP level of 0 (zero) corresponds to 'Committed' (Green) frames and a DP level of 1 or higher corresponds to 'Discard Eligible' (Yellow) frames.

DSCP

DSCP is an acronym for Differentiated Services Code Point. It is a field in the header of IP packets for packet classification purposes.

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.

FTP

FTP is an acronym for File Transfer Protocol. 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

Multicast 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. This processing applies to MLD and MLD.

HTTP

HTTP is an acronym for Hypertext Transfer Protocol. 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 Hypertext Transfer Protocol over Secure 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.

ICMP

ICMP is an acronym for Internet Control Message Protocol. 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.

MLD

MLD is an acronym for Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. MLD 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. MLD can be used for online video and gaming and allows more efficient use of resources when supporting these uses.

MLD Querier

A router sends MLD Query messages onto a particular link. This router is called the Querier.

IMAP

IMAP is an acronym for Internet Message Access Protocol. 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 Internet Protocol. It is a protocol used for communicating data across an internet network.

IP is a "best effort" system, which means that no packet of information sent over 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 MultiCast.

IPMC supports IPv4 and IPv6 multicasting. IPMCv4 denotes multicast for IPv4. IPMCv6 denotes multicast for IPv6.

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.

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.

LLC

The IEEE 802.2 **L**ogical **L**ink **C**ontrol (LLC) protocol provides a link mechanism for upper layer protocols. It is the upper sub-layer of the Data Link Layer and provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX) to coexist within a multipoint network. LLC header consists of 1-byte DSAP (Destination Service Access Point), 1 byte SSAP (Source Service Access Point), 1 or 2 bytes Control field followed by LLC information.

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 entity or 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 Loss Of Connectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as a switch criteria byEPS

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 Maintenance Entity Endpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).

MD5

MD5 is an acronym for Message-Digest 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 MLD 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).

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 Network Basic Input/Output System. 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 Network File System. 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 Network TimeProtocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.

OAM

OAM is an acronym for Operation Administration and Maintenance.

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

A LLDP frame contains multiple TLVs

For some TLVs it is configurable if the switch shall include the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLVs 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 a MAC address.

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 Powered Device. 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.

PoE

PoE is an acronym for Power Over Ethernet.

Power Over Ethernet is used to transmit electrical power, to remote devices over standard Ethernet cable. It could for example be used for powering IP telephones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

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 Post Office Protocol 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, PVLANs provide layer 2 isolation between ports within the same broadcast domain. Isolated ports configured as part of PVLAN cannot communicate with each other. Member ports of a PVLAN can communicate with each other.

PTP

PTP is an acronym for Precision TimeProtocol, a network protocol for synchronizing the clocks of computer systems.

QCE

QCE is an acronym for QoS Control Entry. 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 QoS Control List. 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 Quality of Service. 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.

RARP

RARP is an acronym for Reverse Address Resolution Protocol. 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 Remote Authentication DialIn User Service. 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 Remote Defect Indication. It is a OAM functionallity 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 Rapid Spanning Tree Protocol, 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.

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 Secure Hash Algorithm. 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 Simple Mail Transfer Protocol. 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 **S**ub**N**etwork **A**ccess **P**rotocol (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 Simple Network Management Protocol. 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 Simple Network TimeProtocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

SPROUT

Stack Protocol using ROUting Technology. 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 Set Identifier 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 Secure SHell. 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 Tree Protocol 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.

Switch ID

Switch IDs (1-16) are used to uniquely identify the switches within a stack. The Switch ID of each switch is shown on the display on the front of the switch and is used widely in the web pages as well as in the CLI commands.

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).

sFlow

sFlow is an acronym for sample Flow. This protocol is used to monitor the sampled traffic on the switch. The sFlow Agent configures the sampling rate at which the samples have to collected. The sFlow collector is configured to send the sample data to the external traffic monitoring application.

TACACS+

TACACS+ is an acronym for Terminal Acess Controller AccessControl System Plus. 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 Transmission Control Protocol. 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 TELetype NETwork. 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 Trivial File Transfer Protocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provide directory service and security features.

ToS

ToS is an acronym for Type of Service. It is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant 6 bits of the ToS 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 Type Length Value. 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 Temporal Key Integrity Protocol. 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.

UDP

UDP is an acronym for User Datagram Protocol. 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 does not 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 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

User Priority

User Priority is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as PCP.

VLAN

Virtual LAN. 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.

WEP

WEP is an acronym for Wired Equivalent Privacy. 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).

WiFi

WiFi is an acronym for Wireless Fidelity. 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 Wi-Fi Protected Access. 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 Wi-Fi Protected Access - Pre Shared Key. 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 Wi-Fi Protected Access - 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 Wi-Fi Protected Setup. 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 Weighted Random Early Detection. 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 Wait To Restore. This is the time a failure on a resource must be 'not active' before restoration back to this (previously failing) resource is done.

22194201 R000

Apr-26

English

Viavi Solutions

North America: 1.844.GO VIAVI / 1.844.468.4284

Latin America +52 55 5543 6644

EMEA +49 7121 862273

APAC +1 512 201 6534

All Other Regions: viavisolutions.com/contacts

email TAC@viavisolutions.com

Address 1445 South Spectrum Blvd., Suite 102, Chandler, AZ, 85286, USA