MaxiiNet^{TM} VI3326 Operational Manual

20-port 10/100/1000Base-T + 4 TP/(100/1G) SFP Combo + 2 (100/1G) SFP L2 Plus Managed Switch

V2.64 August 2014

MaxiiNet^{TM} Vi3326 Gigabit Ethernet L2 Plus Managed Switch

Operational Manual

About This Guide

Copyright

Purpose

This manual gives specific information on how to operate and use the management functions of the switch.

Audience

This manual is intended for use by network administrators who are responsible for operating and maintaining network equipment. Consequently, it assumes a basic working knowledge of general switch functions, the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

Conventions

The following conventions are used through this guide to show information:

ⓘ **NOTE:** Emphasizes important information or calls your attention to related features or instructions.

⚡ **WARNING:** Alerts you to a potential hazard that could cause personal injury.

⚠ **CAUTION:** Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Warranty

See the customer support/warranty booklet included with the product. A copy of the specific warranty terms applicable to Vigitron products and replacement parts can be obtained from Vigitron sales and service office or authorized dealers.

Disclaimer

Vigitron, Inc. does not warrant that the hardware will work properly in all environments and applications, and marks no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose. Vigitron, Inc. disclaims liability for any inaccuracies or omissions that may have occurred. Information in this manual is subject to change without notice and does not represent a commitment on the part of Vigitron. Vigitron, Inc. assumes no responsibility for any inaccuracies that may be contained in this manual and makes no commitment to update or keep current the information in this manual. Vigitron, Inc. reserves the rights to make improvements to this manual and/or to the products described in this user's manual, at any time without notice.

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the CE/FCC remove 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.

FCC Caution

To assure continued compliance (e.g. use only shielded interface cables when connection to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CE Mark Warning

This is a Class A device. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Revision History

This section summarizes the changes in each revision of this guide.

Release	Date	Revision
2.60	8/01/2014	A1

Table of Content

Introduction

Overview

This user manual will guide you through installing and connecting your network system, and configuring and monitoring the Vi3326 through the web with the RJ-45 serial interface and Ethernet. You will be given detailed explanations of hardware and software functions, and as well as, web-based interface operations examples.

The Vi3326 series is th enext generation of web-managed switches from Vigitron, Inc. It is a portfolio of afforable managed switches that provide a reliable infrastructure for your business network. These switches deliver highly intelligent features to improve the availability of your business applications, protect sensitive information and optimate network bandwidth in order to deliver information and applications effectively. It provides the ideal combination of affordability and capabilities for entry level networking, including small business or enterprise application, and helps create a more efficient and better connected workforce.

The Vi3326 web-managed switches provide 26 ports in a single device. The specifications are as follows:

- L2+ features provide better manageability, security, QoS, and performance.
- High port count design with all Gigabit Ethernet ports.
- Support guest VLAN, voice VLAN, Port based, tag-based and Protocol based VLANs.
- Support 802.3az Energy Efficient Ethernet standard.
- Support 8K MAC table.
- Support IPv6/ IPv4 Dual stack.
- Support s-Flow.
- Easy port configuration to implement the IP phone, IP camera or wireless environment.

Overview of User Manual

- Chapter 1 “Operation of Web-based Management”
- Chapter 2 “Maintenance”

Chapter 1: Operation of Web-based Management

Initial Configuration

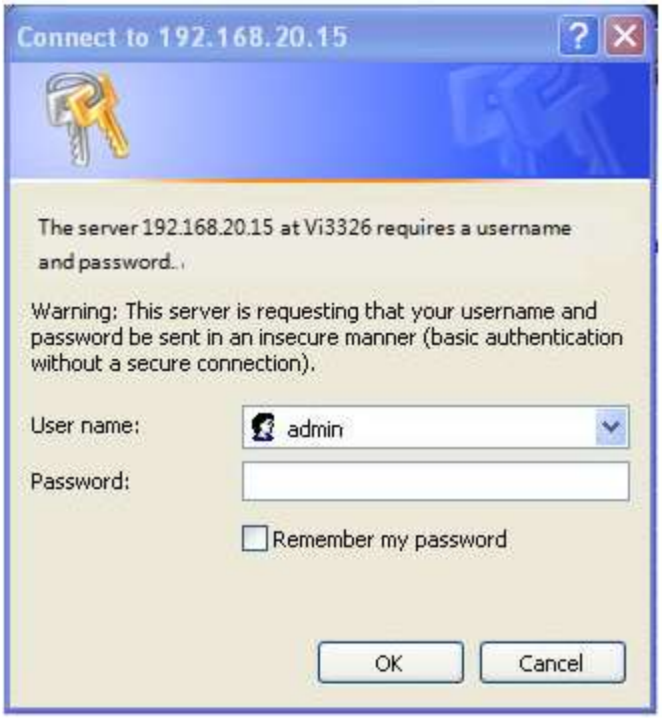
Chapter 1 walks you through the configurations and management of the Vi3326 through the web user interface. Through any of the ports on the switch, you can access and monitor all switch's statuses including MIBs statuses, port activities, Spanning Tree status, port aggregation status, multicast traffic, VLAN, priority status, illegal access record, and so on.

The default values of the Vi3326 are listed in the table below:

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default	192.168.1.254
Username	admin
Password	

After the Vi3326 finished configuring the web user interface, you are free to browse it. For example, open up a broswer and type **http://192.168.1.1** in the address bar, a screen will appear and ask you to input the username and password in order to access the interface.

The default username is **"admin"** and password is **empty**. If this is the first time you are logging in, please input the default username and password, and click the login button. The login process should now be completed. The Vi3326 will not automatically give you a shortcut to the username. You have to input the complete username and password. This is the safer option to log in.



Connect to 192.168.20.15

The server 192.168.20.15 at Vi3326 requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name: admin

Password:

□ Remember my password

Figure 1: The Login Page

NOTE: If you need to configuration the function or parameter then you can refer the detail in the User Manual. Or you could access to the Switch and click the "help" under the web GUI and the switch will pop-up the simple help content to teach you how to set the parameters.

The Vi3326 supports a simple user management function to allow only one administrator to configure the system at a time. If there are two or more users who are using the administrator’s identity, the interface will only allow the user who logged in first to configure the system. All other users (even ones with the administrator’s identy) can only monitor the system. Only a maximum of three (3) users can log into the system simultaneously.

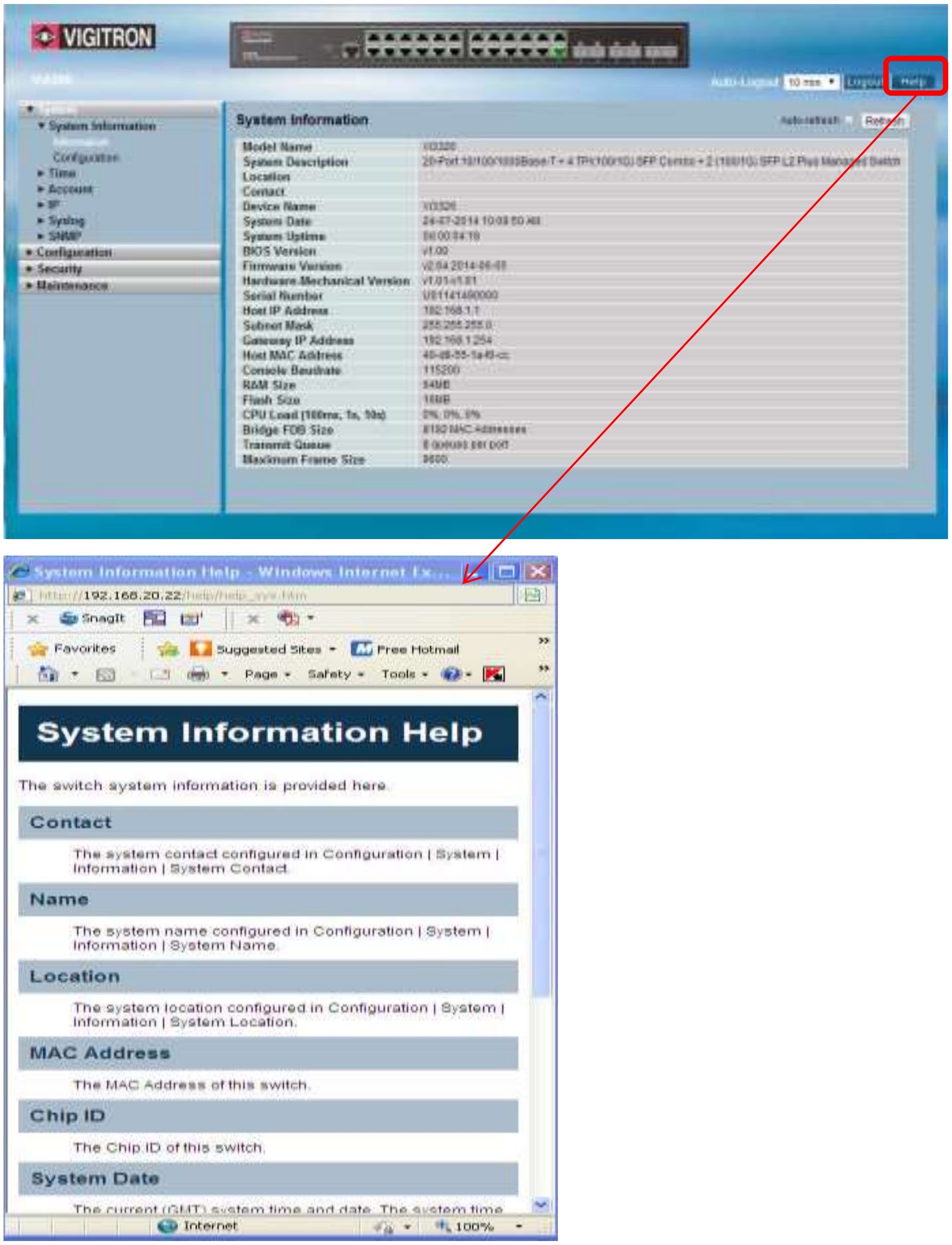
NOTE: When logging in to manage the switch, you will be asked to enter the username and password. The default username is “admin” and the password is empty. Click the login button to enter the interface.

You can use both IPv4 and IPv6 in order to login to manage the Vi3326 switch.

For optimal display, we recommend using Microsoft IE 6.0 above, Netscape v7.1 above, or FireFox v1.00 above, and have the resolution 1024x768. The switch supports neutral web browser interface.

NOTE: The Vi3326 switch function enables DHCP. If you do not have a DHCP service to provide IP addresses to the switch, the switch’s default IP address is **192.168.1.1.**

Vi3326 Web Help Function:



System Information

Model Name	Vi3326
System Description	20-Port 10/100/1000Base-T + 4 TP/(100/1G) SFP Combo + 2 (100/1G) SFP L2 Plus Managed Switch
Location	
Contact	
Device Name	Vi3326
System Date	24-07-2014 10:08:50 AM
System Uptime	0d 00:04:18
BIOS Version	v1.00
Firmware Version	v2.04 2014-06-05
Hardware-Mechanical Version	v1.01-v1.01
Serial Number	U01141490000
Host IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.254
Host MAC Address	40-d8-55-1a-f0-cc
Console Baudrate	115200
RAM Size	64MB
Flash Size	16MB
CPU Load (100ms, 1s, 10s)	0%, 0%, 0%
Bridge FDB Size	8192 MAC Addresses
Transmit Queue	8 queues per port
Maximum Frame Size	9600

System Information Help

The switch system information is provided here.

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

Connecting Network Devices

The switch is designed to be connected to 10, 100, or 1000Mbps network cards in PCs and servers, as well as, to other switches and hubs. It may also be connected to remote devices using optional SFP transceivers.

Twisted-Pair Devices

Each device requires an unshielded twisted-pair (UTP) cable with RJ-45 connectors at both ends. Use Category 5, 5e, or 6 cable for 1000BASE-T connections or Category 5 or better for 100BASE-TX connections.

Cabling Guidelines

The RJ-45 ports on the switch support automatic MDI/MDI-X pin-out configuration. This means you can use standard straight-through twisted-pair cables to connect to any other network devices such as PCs, servers, switches, routers, or hubs.

⚠ **CAUTION:** Do not plug a phone jack connector into an RJ-45 port. This will damage the switch. Use only twisted-pair cables with RJ-45 connectors that conform to FCC standards.

<u>Connecting to PCs, Servers, Hubs, and Switches</u>

Step 1: Attach one end of a twisted-pair cable segment to the device's RJ-45 connector.

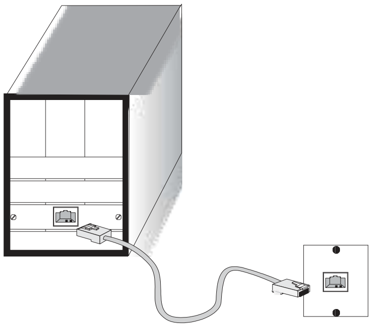


Figure 16: Making Twisted-Pair Connections

Step 2: If the device is a network card and the switch is in the wiring closet, attach the other end of the cable segment to a modular wall outlet that is connected to the wiring closet (see the section “Network Wiring Connections”). Otherwise, attach the other end to an available port on the switch. Make sure each twisted pair cable does not exceed 328ft (100m) in length.

NOTE: Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise, back pressure jamming signals may degrade the overall performance for the segment attached to the hub.

Step 3: As each connection is made, the link LED on the switch that corresponds to each port will light green (1000 Mbps) or amber (100 Mbps) to indicate that the connection is valid.

Network Wiring Connections

Today, the punch-down block is an integral part of many newer equipment racks. It is actually a part of the patch panel. Instructions for making connections in the wiring closet with this type of equipment are as follows:

Step 1: Attach one end of a patch cable to an available port on the switch and the other end to the patch panel.

Step 2: If it’s not already in place, attach one end of a cable segment to the back of the patch panel where the punch-down block is located and the other end to a modular wall outlet.

Step 3: Label the cables to simplify future troubleshooting.

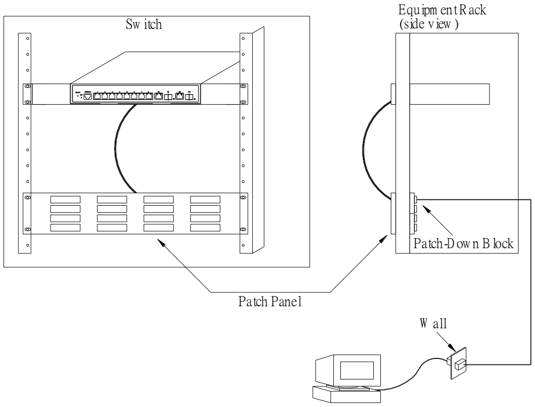


Figure 17: Network Wiring Connections

Chapter 2: System Configuration

2-1 System Information

Chapter 2 reviews all of the basic configuration tasks including system information and other management tasks such as time, account, IP, Syslog, and SNMP.

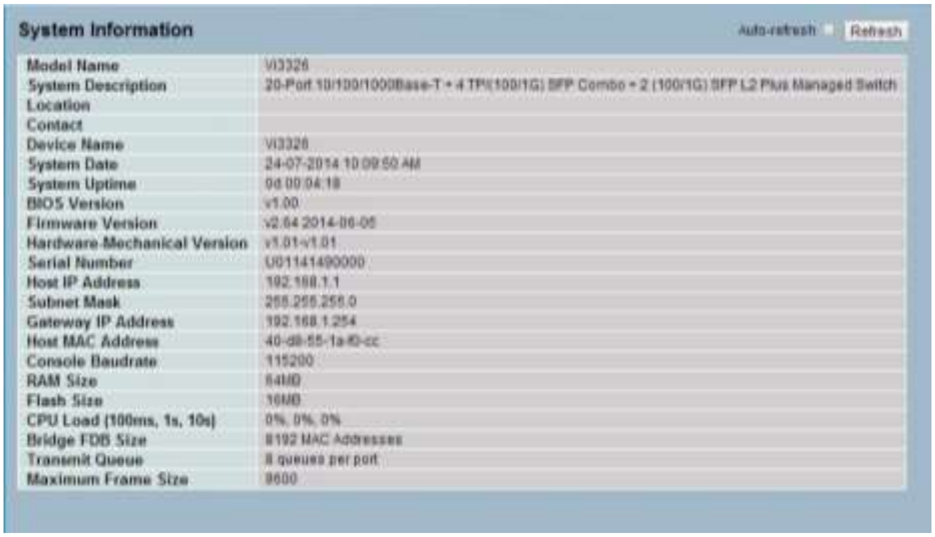
2-1.1 Information

After logging into the system interface, you will be taken to the default system information page. After you log in, the switch shows you the system information. This page gives you the basic information of the Vi3326 switch including model name, system description, contact, device name, system up time, BIOS version, firmware version, hardware-mechanical version, serial number, host IP address, host MAC address, device port, ram size, and flash size. This information will be helpful in case of any system malfunctions.

Web Interface

To configure the system information in the web interface:

1. Click SYSTEM, System, and Information.
2. Specify the contact information for the system administrator, and the name and location of the switch. Also, indicate the local time zone by configuring the appropriate offset.
3. Click refresh.



System Information

Model Name	Vi3326
System Description	20-Port 10/100/1000Base-T + 4 TP/(100/1G) SFP Combo + 2 (100/1G) SFP L2 Plus Managed Switch
Location	
Contact	
Device Name	Vi3326
System Date	24-07-2014 10:09:50 AM
System Uptime	0d 00:04:18
BIOS Version	v1.00
Firmware Version	v2.64 2014-06-05
Hardware-Mechanical Version	v1.01-v1.01
Serial Number	U01141490000
Host IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.254
Host MAC Address	40-d8-55-1a-f0-cc
Console Baudrate	115200
RAM Size	64MB
Flash Size	16MB
CPU Load (100ms, 1s, 10s)	0%, 0%, 0%
Bridge FDB Size	8192 MAC Addresses
Transmit Queue	8 queues per port
Maximum Frame Size	9600

Figure 2-1.1: System Information

Parameter Description

Model Name: The model name of this device.

System Description: System description describes what the device is - "20-Port 10/100/1000Base-T + 4 TP/(100/1G) SFP Combo + 2 (100/1G) SFP L2 Plus Managed Switch".

Location: This is where the switch is placed. User-defined.

Contact: To keep management and maintenance simple, write the contact information for the person who could help you with the switch. This step can be configured through the device's user interface or SNMP.

Device Name: This is the name of the switch. User-defined.

System Date: This displays the current system time and date. The field format is YYYY-MM-DD HH:MM:SS.

System Up Time: This is the time accumulated since this switch was powered up. The field format is day, hour, minute, second.

BIOS version: This is the BIOS version of this switch.

Firmware version: This is the firmware version of this switch.

Hardware-Mechanical version: This is the hardware and mechanical version of the switch. The figure before the hyphen is the version of electronic hardware and the one after the hyphen is the version of mechanical.

Serial number: This is the serial number assigned by Vigitron, Inc.

Host IP Address: This is the IP address of the switch.

Subnet Mask: This displays the IP subnet mask assigned to the device.

Gateway IP Address: This displays the default gateway IP address assigned to the device.

Host MAC Address: This is the Ethernet MAC address of the management agent in this switch.

Console Baudrate: This displays the baudrate of RS232(COM) port.

RAM Size: This is the size of the RAM in this switch.

Flash Size: This is the size of the flash memory in this switch.

Bridge FDB Size: This displays the bridge forwarding database size of the device.

Transmit Queue: This displays the information about the transmit priority queue of switch.

Maximum Frame Size: This displays the information about switch supported maximum frame size.

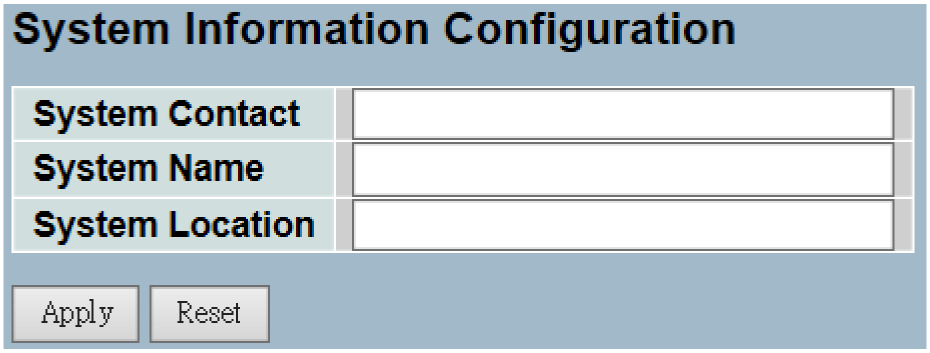
2-1.2 Configuration

By configuring the contact information, name, and location of the switch, you can now identify the system.

Web Interface

To configure the system information in the web interface:

1. Click System, System Information, and Configuration.
2. Enter in the system contact, the system name, and the system location information.
3. Click save.



System Information Configuration

System Contact	
System Name	
System Location	

Figure 2-1.2: System Information Configuration

Parameter Description

System Contact: This is the textual identification of the contact person for this managed node, along 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: This is 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), and 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: This is 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.

2-2 Time

This section guides the user on how to configure the switch time. Time configure includes time configuration and NTP configuration.

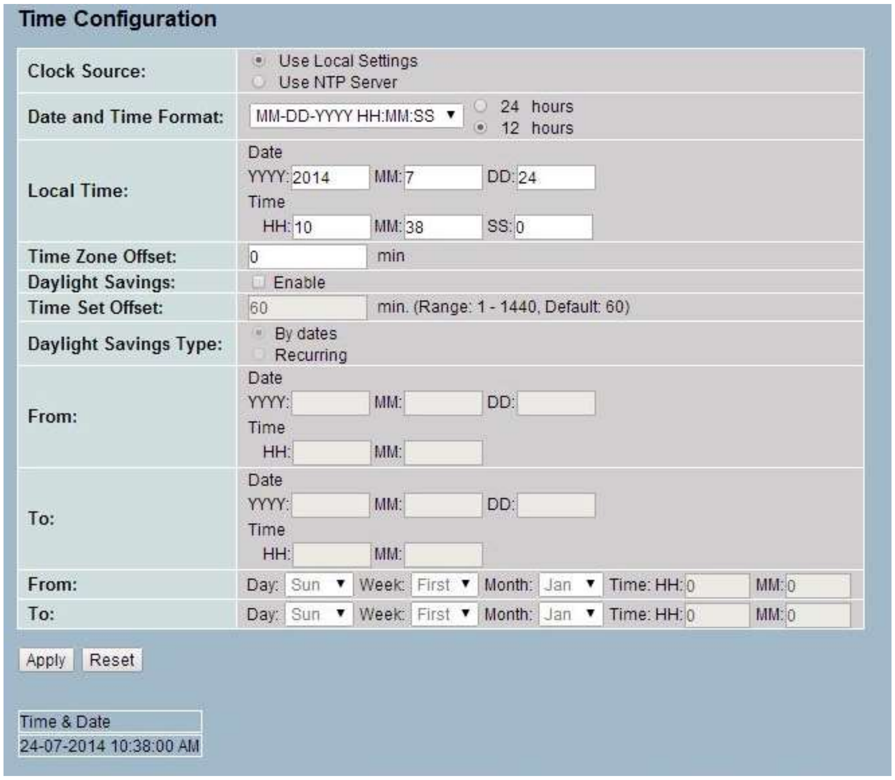
2-2.1 Manual

The switch provides manual and automatic ways to set the system time via NTP. Manual setting is simple. Just input the year, month, day, hour, minute and second within the valid value range indiciated for each item.

Web Interface

To configure the time in the web interface:

1. Click Time and Manual.
2. Specify the time parameter in manual parameters.
3. Click save.



Time Configuration

Clock Source:	● Use Local Settings ○ Use NTP Server
Date and Time Format:	MM-DD-YYYY HH:MM:SS ▼ ○ 24 hours ● 12 hours
Local Time:	Date YYYY: 2014 MM: 7 DD: 24 Time HH: 10 MM: 38 SS: 0
Time Zone Offset:	0 min
Daylight Savings:	□ Enable
Time Set Offset:	60 min. (Range: 1 - 1440, Default: 60)
Daylight Savings Type:	● By dates ○ Recurring
From:	Date YYYY: MM: DD: Time HH: MM:
To:	Date YYYY: MM: DD: Time HH: MM:
From:	Day: Sun ▼ Week: First ▼ Month: Jan ▼ Time: HH: 0 MM: 0
To:	Day: Sun ▼ Week: First ▼ Month: Jan ▼ Time: HH: 0 MM: 0

Time & Date
24-07-2014 10:38:00 AM

Figure 2-2.1: The Time Configuration

Parameter Description

Clock Source: There are two sources for configuring time.

1. Use Local Settings: In this mode Clock Source is from Local Time. Set the time manually.
2. Use NTP Server: In this mode Clock Source is from NTP Server. The switch can link to Network Time Protocol server to obtain the correct time automatically when NTP server has been set.

Date and Time Format: The drop bar is for choose appropriate time format. Three selections are provided.

YYYY-MM-DD HH:MM:SS

MM-DD-YYYY HH:MM:SS

DD-MM-YYYY HH:MM:SS

24 hours: The time is always represented in the 24-hour system

12 hours: The time is always represented in the 12-hour system

Local Time: Show the current time of the system. The local time can only be filled out in 24 hours format.

Time Zone Offset: Provide the timezone offset relative to UTC/GMT. The offset is given in minutes east of GMT. The valid range is from -720 to 720 minutes

Daylight Saving: Indicates the Daylight Savings mode operation. Possible modes are:

- Enabled: Enable Daylight Savings mode operation.
- Disabled: Disable Daylight Savings mode operation.

Time Set Offset: Used for non-USA and European countries to set the amount of time for Daylight Saving Time(DST) (in minutes). The valid range is from 1 to 1440 minutes. The default time is 60 minutes.

Daylight Savings Type: There are two types for configuring

1. By dates: Daylight Savings Type by Dates.
2. Recurring: Daylight Savings Type by Recurring. DST occurs on the same date every year.

From: To configure when Daylight saving start date and time, the format is “YYYY-MM-DD HH:MM”. The column “HH:MM” can only be filled out in 24 hour format.

To: To configure when Daylight saving end date and time, the format is “YYYY-MM-DD HH:MM”. The column “HH:MM” can only be filled out in 24 hour format.

NOTE: The under “from” and “to” was displayed what you set on the “From” and “To” field information.

NOTE: The local time column and Day light saving column will not actively change by the date time format selection.

2-2.2 NTP

NTP is an acronym for Network Time Protocol. It is used to sync the network time based Greenwich Mean Time (GMT). When you're using the NTP mode, you can either select the built-in NTP time server or you can manually specify the NTP server and time zone. The switch will sync the time after you click the apply button. Though it synchronizes the time automatically, the NTP does not update the time periodically without the user's processing.

Time zone is an offset time off GMT. You must select the time zone first and then perform time sync via the NTP. The switch will combine this time zone offset and updated NTP time to determine the local time. Otherwise, you will not be able to get the correct time. The switch supports configurable time zone from –12 to +13 step 1 hour. The default time zone is +8 Hrs.

Web Interface

To configure the time in the web interface:

1. Click SYSTEM and NTP.
2. Specify the time parameter in manual parameters.
3. Click save.

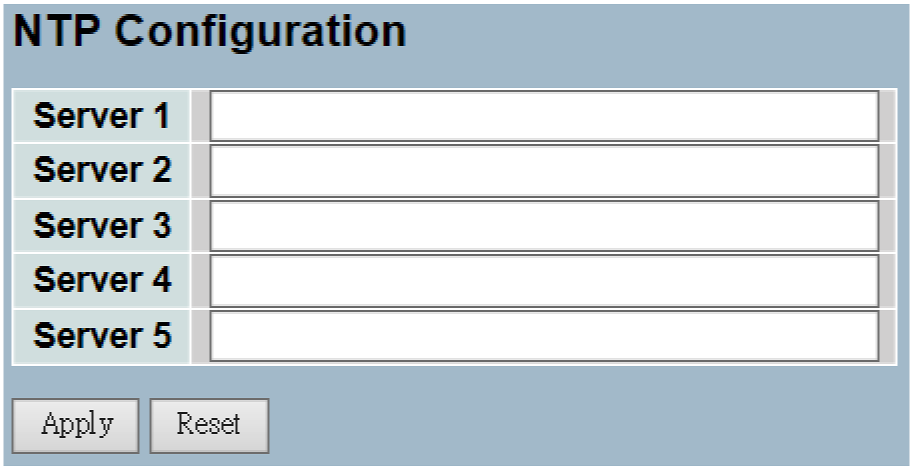


Figure 2-2.2: The NTP Configuration

Parameter Description

Server 1 to 5: This provides the NTP IPv4 or IPv6 address of the switch. The IPv6 address is in 128-bit records and is represented as eight fields of up to four (4) hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

Buttons: These buttons are displayed on the NTP page:

- Apply – Click to apply changes.
- Reset - Click to restore default settings.

2-3 Account

For the account function, only the administrator can create, modify, or delete the username and password. They can modify other guest identities' password without needing to confirm the password. However, it is necessary to confirm when modifying the administrator-equivalent identity. Guest-equivalent identity can only modify their password only. Please note that you must confirm administrator/guest identity in the authorization field in advance before configuring the username and password. Only one administrator is allowed to exist and cannot be deleted. In addition, up to 4 guest accounts can be created.

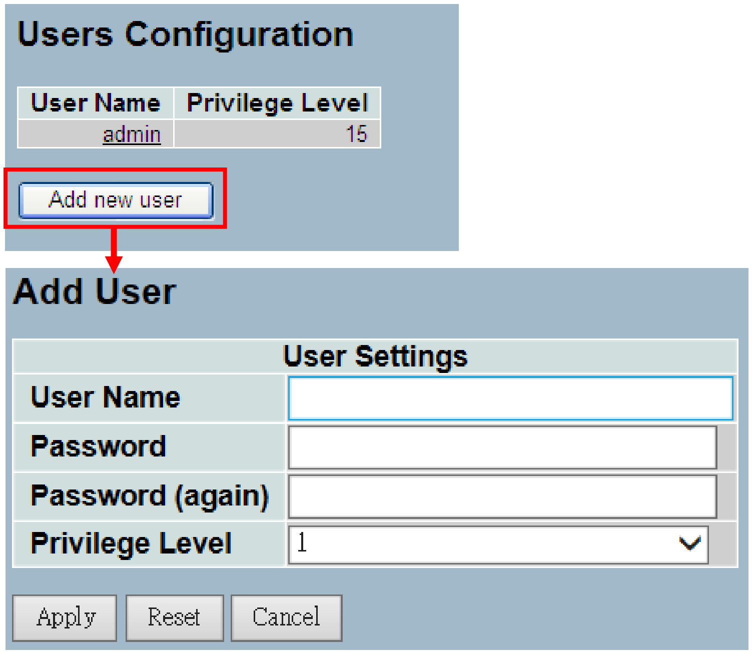
2-3.1 Users

This page provides an overview of the current users. Currently, the only way to login as another user on the web server is to close and reopen the browser.

Web Interface

To configure the account in the web interface:

1. Click SYSTEM, Account, and Users.
2. Click add new user.
3. Specify the user name parameter.
4. Click save.



Users Configuration

User Name	Privilege Level
admin	15

Add User

User Settings	
User Name	
Password	
Password (again)	
Privilege Level	1

Figure 2- 3.1: The Users Account Configuration

Parameter Description

User Name: User name is a string identifying the user that this entry should belong to. The allowed string length is 1 to 32. The valid user name is a combination of letters, numbers, and underscores.

Password: To type the password. The allowed string length is 0 to 255 and the allowed content is the ASCII characters from 32 to 126.

Password (again): To type the password again. You must type the same password again in the field.

Privilege Level: The privilege level identifies what type of account this user has. The allowed range is 1 to 15. Privilege level 15 gives full access to all groups and full control of the switch. Other values need to refer to each group privilege level. The user's privilege should be same or greater than the group privilege level in order to gain access to that group. By default, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. In order to maintain the system (software upload, factory defaults, and more), the user needs to have privilege level 15. Usually, privilege level 15 is used for the administrator account, privilege level 10 is for standard user accounts, and privilege level 5 is for guests accounts.

NOTE: You may add up to 19 usernames in “Users Configuration”. You can configure a total of 20 usernames, including the administrator account.

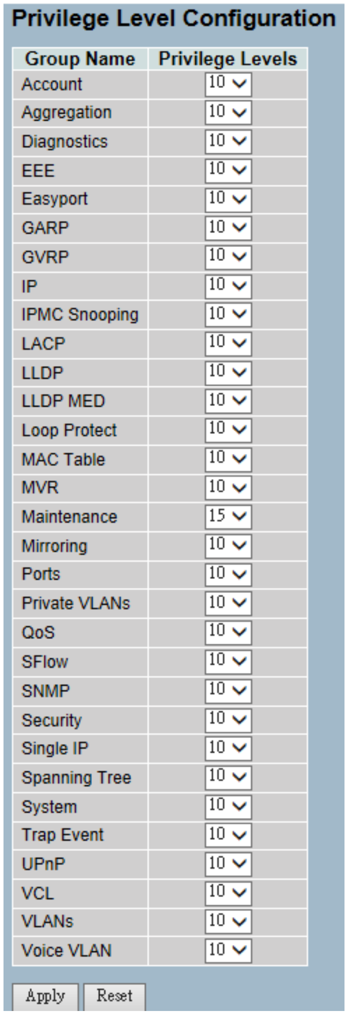
2-3.2 Privilege Level

This section provides an overview of different privilege levels. Users can defined privilege levels (from 1 to 15) for the following settings: Account, Aggregation, Diagnostics, EEE, GARP, GVRP, IP, IPMC Snooping, LACP, LLDP, LLDP, MED, MAC Table, MRP, MVR, MVRP Maintenance, Mirroring, Ports, Private VLANs, QoS, SNMP, Security, Spanning Tree, System Trap Event, VCL, VLANs, and Voice VLAN.

Web Interface

To configure the privilege level in the web interface:

1. Click SYSTEM, Account, and Privilege Level.
2. Specify the privilege parameter from 1 to 15.
3. Click save.



Privilege Level Configuration

Group Name	Privilege Levels
Account	10
Aggregation	10
Diagnostics	10
EEE	10
Easyport	10
GARP	10
GVRP	10
IP	10
IPMC Snooping	10
LACP	10
LLDP	10
LLDP MED	10
Loop Protect	10
MAC Table	10
MVR	10
Maintenance	15
Mirroring	10
Ports	10
Private VLANs	10
QoS	10
SFlow	10
SNMP	10
Security	10
Single IP	10
Spanning Tree	10
System	10
Trap Event	10
UPnP	10
VCL	10
VLANs	10
Voice VLAN	10

Figure2- 3.2: The Privilege Level Configuration

Parameter Description

Group Name: Group name is the name identifying the privilege group. Usually, 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 details:

- **System:** Contact, Name, Location, Timezone, Log.
- **Security:** Authentication, System Access Management, Port (contains Dot1x port, MAC-based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection and IP Source Guard.
- **IP:** Everything except 'ping'.
- **Port:** Everything except 'VeriPHY'.
- **Diagnostics:** 'ping' and 'VeriPHY'.
- **Maintenance:** System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load, Firmware Load, Web-Users, Privilege Levels, and everything in Maintenance.

Privilege Levels: 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 in order to gain access to that group.

2-4 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 to allow 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, the IPv4 is still the protocol of choice for most of the Internet.

2-4.1 IPv4

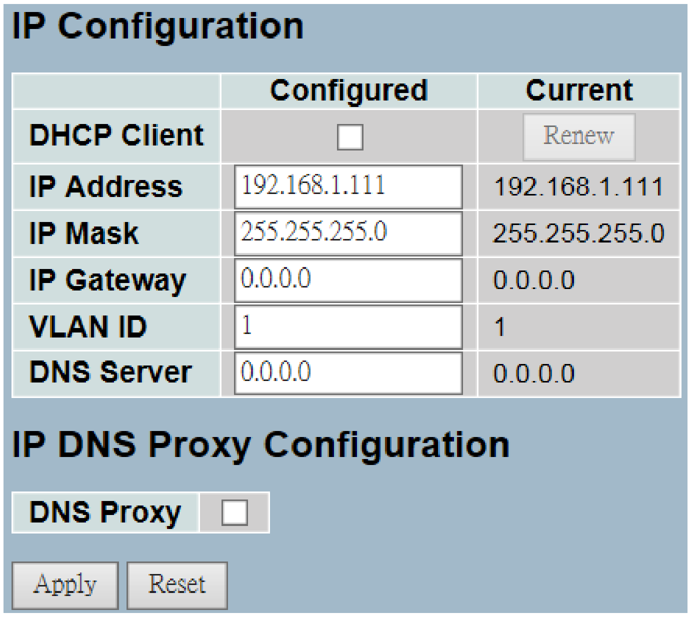
The IPv4 address for the switch could be obtained via the DHCP server for VLAN 1. To manually configure an address, you need to change the switch's default settings to values that are compatible with your network. You may also need to a establish a default gateway between the switch and management stations that exist on another network segment.

- Configure the switch-managed IP information on this page.
- The “Configured” column is used to view or change the IP configuration.
- The “Current” column is used to show the active IP configuration.

Web Interface

To configure an IP address in the web interface:

1. Click System and IP Configuration.
2. Specify the IPv4 settings, and enable DNS proxy service if required.
3. Click save.



IP Configuration

	Configured	Current
DHCP Client	□	Renew
IP Address	192.168.1.111	192.168.1.111
IP Mask	255.255.255.0	255.255.255.0
IP Gateway	0.0.0.0	0.0.0.0
VLAN ID	1	1
DNS Server	0.0.0.0	0.0.0.0

IP DNS Proxy Configuration

DNS Proxy	□

Figure2- 4.1: The IP Configuration

Parameter Description

DHCP Client: You must check this box to enable the DHCP client. If the DHCP fails and the configured IP address is zero, the DHCP will retry. If the DHCP fails and the configured IP address is non-zero, the DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured system name as the hostname to provide DNS lookup.

IP Address: This provides the IP address of this switch in dotted decimal notation.

IP Mask: This provides the IP mask of this switch dotted decimal notation.

IP Gateway: This provides the IP address of the router in dotted decimal notation.

DNS Server: This provides the IP address of the DNS Server in dotted decimal notation.

VLAN ID: This provides the managed VLAN ID. The allowed range is 1 to 4095.

DNS Proxy: When the DNS proxy is enabled, the DUT will relay the DNS requests to the current configured DNS server on the DUT, and reply as a DNS resolver to the client device on the network.

2-4.2 IPv6

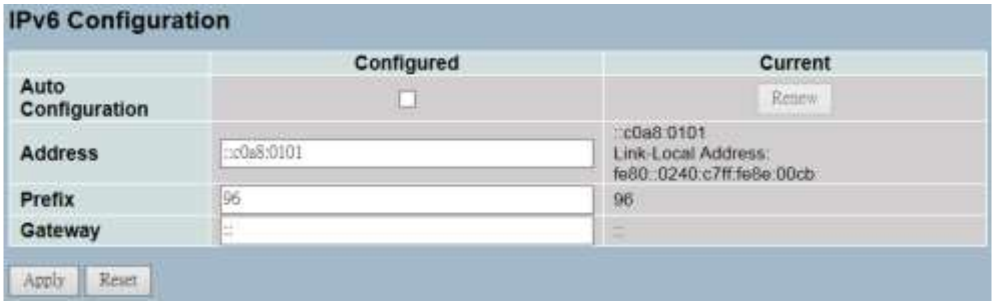
This section will guide you through the configurations of the switch-managed IPv6 information. The “Configured” column is used to view or change the IPv6 configuration. The “Current” column is used to show the active IPv6 configuration.

- Configure the switch-managed IPv6 information on this page.
- The “Configured” column is used to view or change the IPv6 configuration.
- The “Current”column is used to show the active IPv6 configuration.

Web Interface

To configure the switch’s IPv6 management in the web interface:

1. Click System andIPv6 Configuration.
2. Specify the IPv6 settings, and enable Auto Configuration service if required.
3. Click save.



IPv6 Configuration

	Configured	Current
Auto Configuration	□	Renew
Address	::c0a8:0101	::c0a8:0101 Link-Local Address: fe80::0240:c7ff:fe8e:00cb
Prefix	96	96
Gateway	::	::

Figure 2- 4.2: The IPv6 Configuration

Parameter Description

Auto Configuration: By checking this box, IPv6 auto-configuration will be enabled. If it fails, the configured IPv6 address is zero. The router may delay responds to a router solicitation for a few seconds. The total time needed to complete auto-configuration can be significantly longer.

Address: This provides the IPv6 address of the switch. The IPv6 address is in 128-bit records, represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

Prefix: This provides the IPv6 prefix of the switch. The allowed range is 1 to 128.

Gateway: This provides the IPv6 gateway address of the switch. The IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

2-5 Syslog

The Syslog is a standard for logging program messages. It allows separation of the software that generates messages from the system that stores them, and the software that reports and analyzes them. It can be used as generalized informational, analysis, and debugging messages. It is supported by a wide variety of devices and receivers across multiple platforms.

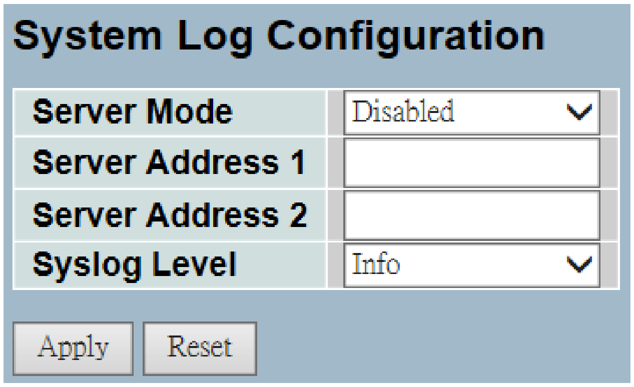
2-5.1 Configuration

This section describes how to configure the system log and provides a wide variety of devices and receivers across multiple platforms.

Web Interface

To configure the Syslog configuration in the web interface:

1. Click SYSTEM and Syslog.
2. Specify the syslog parameters including the IP address of Syslog server and port number.
3. Enable the Syslog.
4. Click save.



System Log Configuration

Server Mode	Disabled
Server Address 1	
Server Address 2	
Syslog Level	Info

Figure 2- 5.1: The System Log Configuration

Parameter Description

Server Mode: This 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 the UDP communication and received on UDP port 514. The syslog server will not send acknowledgments back to the 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**: Enables the server mode operation.
- **Disabled**: Disables the server mode operation.

Server Address 1 and 2: This indicates the IPv4 host address of syslog server 1 and server 2 (for redundancy). If the switch provides DNS feature, it also can be a host name.

Syslog Level: This indicates the type of message that will be sent to the syslog server. The possible modes are:

- **Info**: Sends informations, warnings, and errors.
- **Warning**: Sends warnings and errors.
- **Error**: Sends errors.

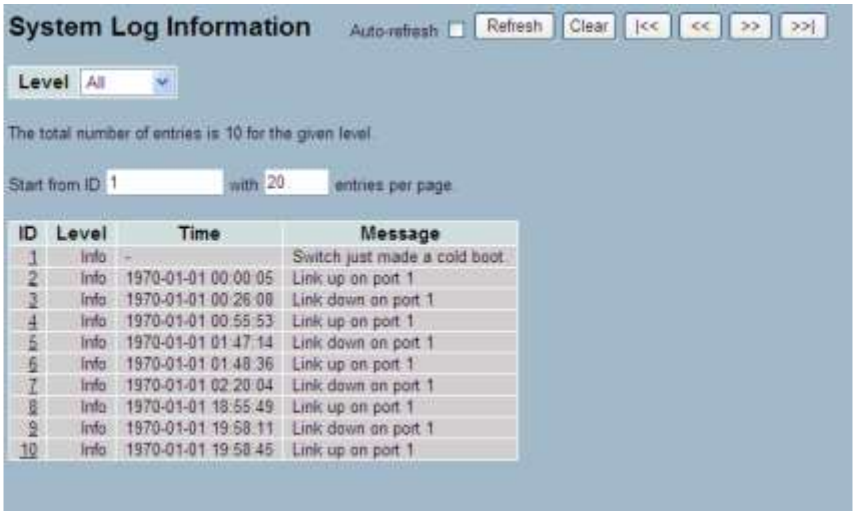
2-5.2 Log

This section provides an overview of the system log information of the switch.

Web Interface

To display the log configuration in the web interface:

1. Click Syslog and Log.
2. Display the log information.



System Log Information

Level: All

The total number of entries is 10 for the given level

Start from ID 1 with 20 entries per page

ID	Level	Time	Message
1	Info	-	Switch just made a cold boot.
2	Info	1970-01-01 00:00:05	Link up on port 1
3	Info	1970-01-01 00:26:08	Link down on port 1
4	Info	1970-01-01 00:55:53	Link up on port 1
5	Info	1970-01-01 01:47:14	Link down on port 1
6	Info	1970-01-01 01:48:36	Link up on port 1
7	Info	1970-01-01 02:20:04	Link down on port 1
8	Info	1970-01-01 18:55:49	Link up on port 1
9	Info	1970-01-01 19:58:11	Link down on port 1
10	Info	1970-01-01 19:58:45	Link up on port 1

Figure 2- 5.2: The System Log Configuration

Parameter Description

Auto-refresh: If this option is selected, the device will automatically refresh the log.

Level: This is the level of the system log entry. The following informational level types are supported:

- **Warning:** Warning level of the system log.
- **Error:** Error level of the system log.
- **All**: All levels.

ID: This is the ID (>= 1) of the system log entry.

Time: This displays the log record by the device time. It is the time of the system log entry.

Message: This displays the log detail message. It is the message of the system log entry.

Upper right icon (Refresh, clear,….): Click these buttons to manually refresh or clear the system log. Other buttons allow you to go to the next or previous page/entry.

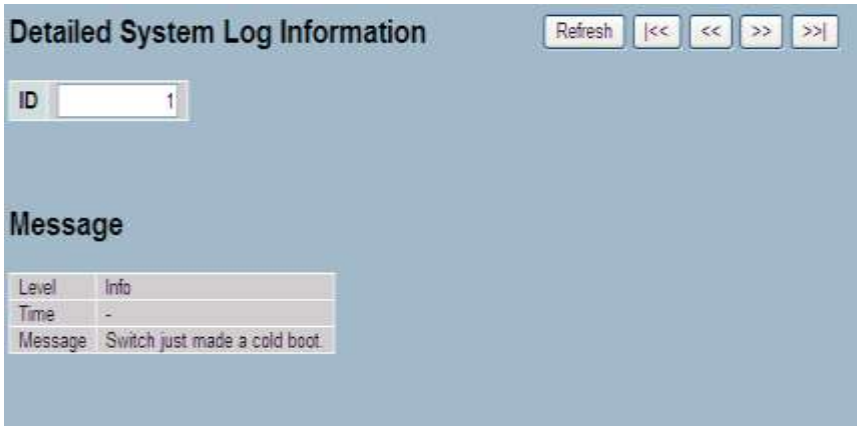
2-5.3 Detailed Log

This section provides a detailed overview of the switch's log information.

Web Interface

To display the detailed log configuration in the web interface:

1. Click Syslog and Detailed Log.
2. Display the log information.



Level	Info
Time	-
Message	Switch just made a cold boot.

Figure2- 5.3: The Detailed System Log Information

Parameter Description

ID: This is the ID (>= 1) of the system log entry.

Message: This is the detailed message of the system log entry.

Upper right icon (Refresh, clear,….): Click these buttons to manually refresh or clear the system log. Other buttons allow you to go to the next or previous page/entry.

2-6 SNMP

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the managed devices equipped with the SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. The SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent. It traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. The SNMP agent runs on the switch to respond to the request issued by the SNMP manager.

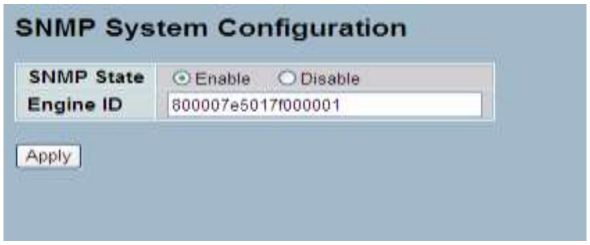
It is basically passive, except when issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP to “Enable”, the SNMP agent will start up. All supported MIB OIDs, including RMON MIB, can be accessed via the SNMP manager. If the field SNMP is set to “Disable”, the SNMP agent will be de-activated; and the related community name, trap host IP address, trap, and all MIB counters will be ignored.

2-6.1 System

This section guides you on the configurations of the SNMP system of the switch. This function is used to configure SNMP settings, community name, trap host, public traps, and the throttle of SNMP. A SNMP manager must pass the authentication by identifying both community names in order to access the MIB information of the target device. Both parties must have the same community name. In order for the setting to take effect, click the apply button after everything is completed.

Web Interface To display the SNMP system configurations in the web interface:

1. Click SNMP and System.
2. Evoke SNMP State to enable or disable the SNMP function.
3. Specify the engine ID.
4. Click apply.



SNMP System Configuration

SNMP State	● Enable ○ Disable
Engine ID	800007e5017f000001

Figure 2- 6.1: The SNMP System Configuration

Parameter Description

These parameters are displayed on the SNMP System Configuration page:

SNMP State: SNMP is used for the activation or de-activation of SNMP.

- **Enable:** Enable SNMP state operation.
- **Disable:** Disable SNMP state operation.
- **Default:** Enable.

Engine ID: This is the SNMPv3 engine ID. The syntax: 0-9, a-f, A-F, min 5 octet, max 32 octet, fifth octet. You cannot input 00. By changing the engine ID, you will clear the original user.

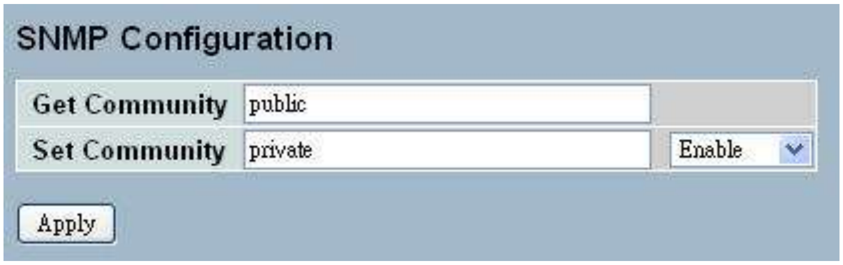
2-6.2 Configuration

By default, there are two communities: “Get Community” and “Set Community.” It is applicable to configure the “Get Community” and the “Set Community” for SNMPv1 and SNMPv2.

Web Interface

To configure the SNMP Communities in the web interface:

1. Click SNMP and Configuration.
2. Specify the parameters of “Get Community” and “Set Community”.
3. Enable or disable the function of Set Community.
4. Click apply.
5. If you want to modify or clear the setting, then click reset



SNMP Configuration

Get Community	public	
Set Community	private	Enable

Figure 2- 6.2: SNMP Configuration

Parameter Description

Get Community: This indicates the community read access string to permit access to the SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.

The field is applicable only when the SNMP version is SNMPv1 or SNMPv2c. If the SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure the security name than a SNMPv1 or SNMPv2c community string. In addition to the community string, a particular range of source addresses can be used to restrict source subnet.

Set Community: This indicates the community write access string to permit access to the SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.

The field is applicable only when SNMP version is SNMPv1 or SNMPv2c.

- **Mode**: Indicates the “Set Community” mode operation. Possible modes are -
- **Enabled**: Enables “Set Community”.
- **Disabled**: Disables “Set Community”.

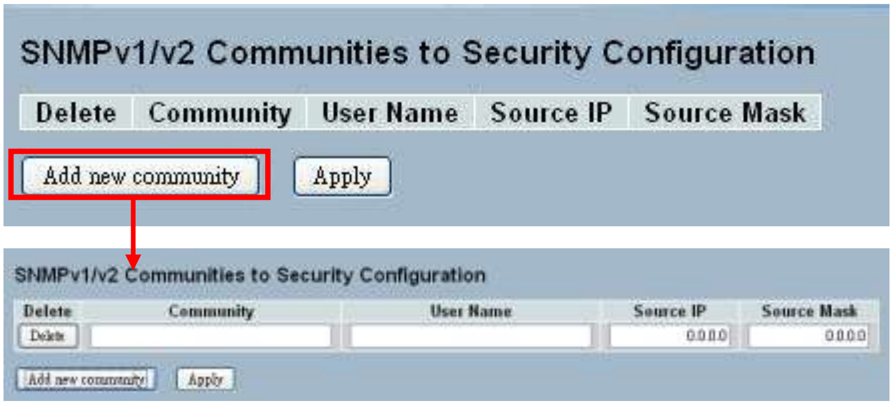
2-6.3 Communities

This section provides an overview SNMPv3 communities configurations. The community and user name are unique. To create a new community account, please click the "Add New Community" button. Enter the account information and then click save. The max group number is: 4.

Web Interface

To display the configure SNMP Communities in the web interface:

1. Click SNMP andCommunities.
2. Click add new community.
3. Specify the SNMP communities parameters.
4. Click save.
5. If you want to modify or clear the setting, then click reset.



SNMPv1/v2 Communities to Security Configuration

Delete	Community	User Name	Source IP	Source Mask

SNMPv1/v2 Communities to Security Configuration

Delete	Community	User Name	Source IP	Source Mask
Delete			0.0.0.0	0.0.0.0

Figure 2- 6.3: The SNMPv1/v2 Communities Security Configuration

Parameter Description

Delete: Click delete to remove the entry.It will be deleted during the next apply.

Community: This indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as the security name and map a SNMPv1 or SNMPv2c community string.

User Name: This is a string identifying the user name that this entry should belong to. The length of "User Name" string is restricted to 1-32, and the allowed content is ASCII characters from 33 to 126.

Source IP: This indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.

Source Mask: This indicates the SNMP access source address mask.

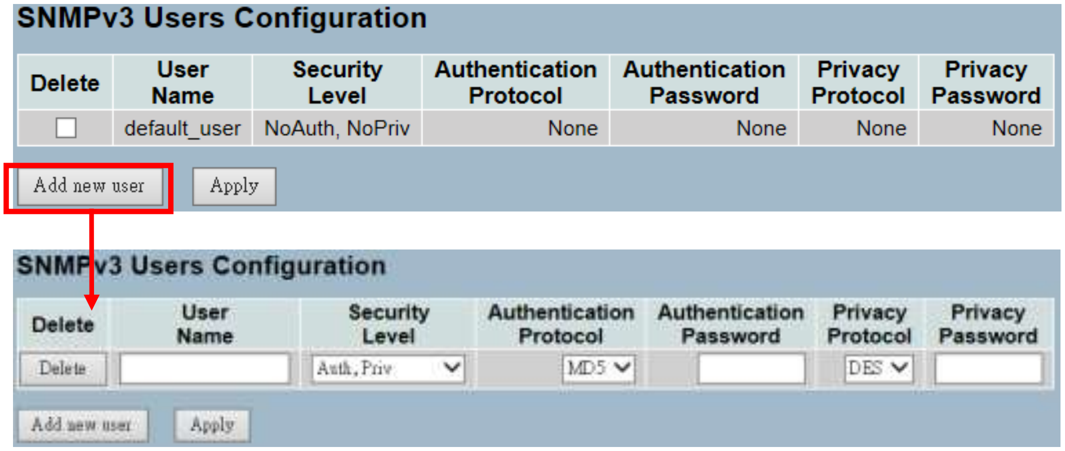
2-6.4 Users

The users function is used to configure SNMPv3 user. The entry index key is user name. To create a new user name account, click on the “Add New User” button, enter the user information, and then click “Save”. The max group number is: 10.

Web Interface

To display the configure SNMP users in the web interface:

1. Click SNMP and Users.
2. Specify the privilege parameter.
3. Click save.



SNMPv3 Users Configuration

Delete	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
□	default_user	NoAuth, NoPriv	None	None	None	None

Add new user Apply

SNMPv3 Users Configuration

Delete	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
Delete		Auth, Priv	MD5		DES	

Add new user Apply

Figure 2-6.4: The SNMP Users Configuration

Parameter Description

Delete: Click delete to remove an entry. The entry will be deleted during the next save.

User Name: This is a string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Security Level: This indicates the security model that this entry should belong to. The 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. That means it must first be ensured that the value is set correctly.

Authentication Protocol: This indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:

- **None:** No authentication protocol.
- **MD5:** An optional flag to indicate that this user uses MD5 authentication protocol.
- **SHA:** An optional flag to indicate that this user uses 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: This is 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.

Privacy Protocol: This is the privacy protocol that this entry should belong to. Possible privacy protocols are:

- **None:** No privacy protocol.
- **DES:** An optional flag to indicate that this user uses DES authentication protocol.

Privacy Password: This is a string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.

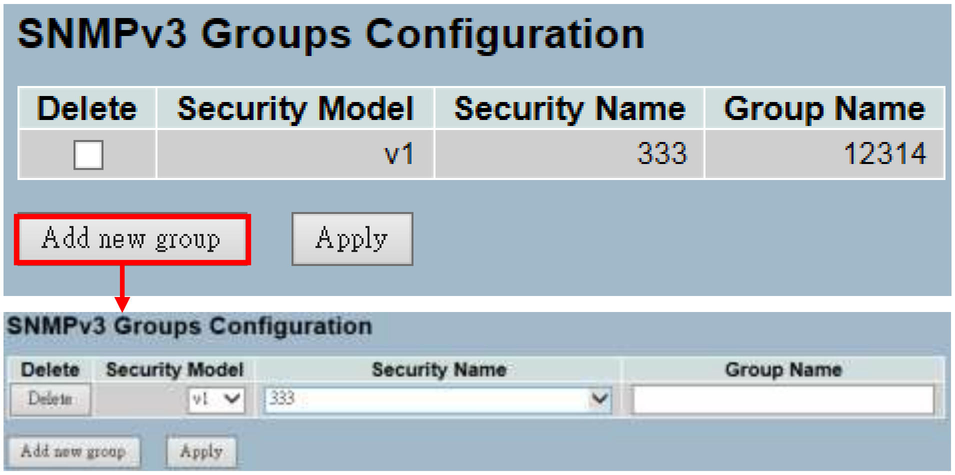
2-6.5 Groups

The groups function is used to configure SNMPv3 group. The entry index key are security model and security name. To create a new group account, click “Add New Group”, enter the group information, and then click “Save”. The max group numbers are: v1: 2, v2: 2, v3:10.

Web Interface

To display the configure SNMP groups in the web interface:

1. Click SNMP and Groups.
2. Specify the privilege parameter.
3. Click save.



SNMPv3 Groups Configuration

Delete	Security Model	Security Name	Group Name
□	v1	333	12314

SNMPv3 Groups Configuration

Delete	Security Model	Security Name	Group Name
Delete	v1	333	

Figure 2-6.5: The SNMP Groups Configuration

Parameter Description

Delete: Click delete to remove entry. It will be deleted during the next save.

Security Model: This 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: This is 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 ASCII characters from 33 to 126.

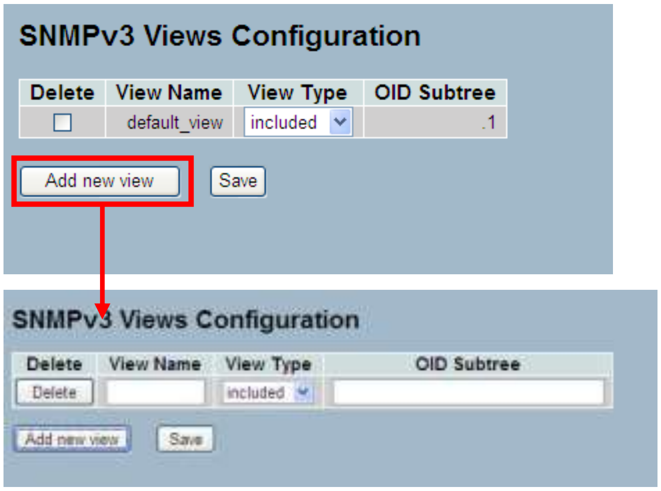
Group Name: This is a string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

2-6.6 Views

The views function is used to configure the SNMPv3 view. The entry index key are OID subtree and view name. To create a new view account, click “Add New View”, enter the view information, and then click “Save.” The max group number is: 28.

Web Interface

1. Click SNMP and Views.
2. Click add new view.
3. Specify the SNMP view parameters.
4. Click save.
5. If you want to modify or clear the setting, then click Reset.



SNMPv3 Views Configuration

Delete	View Name	View Type	OID Subtree
□	default_view	included	.1

SNMPv3 Views Configuration

Delete	View Name	View Type	OID Subtree
Delete		included	

Figure 2-6.6: The SNMP Views Configuration

Parameter Description

Delete: It will be deleted during the next save.

View Name: This is 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 ASCII characters from 33 to 126.

View Type: This indicates the view type that this entry should belong to. Possible view types are:

- **included:** An optional flag to indicate that this view subtree should be included.
- **excluded:** An optional flag to indicate that this view subtree should be excluded.
- In general, if a view entry's view type is “Excluded”, 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 defines the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).

Save: Click save to save the configuration to ROM.

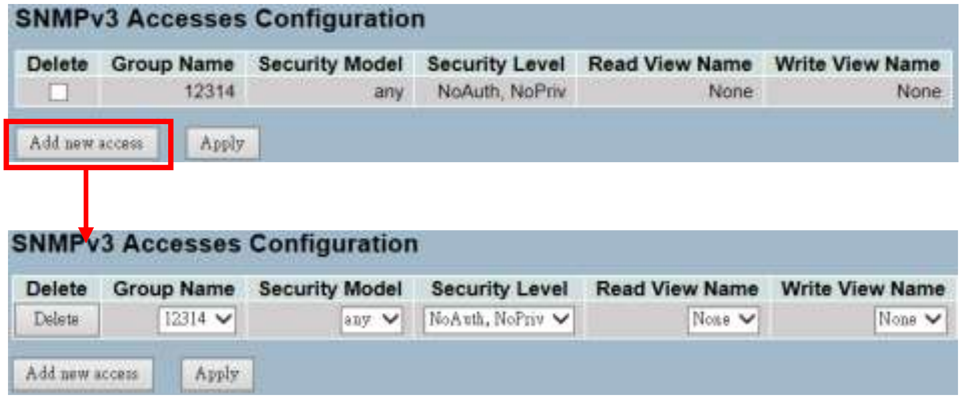
2-6.7 Access

The access function is used to configure the SNMPv3 accesses. The entry index key are group name, security model and security level. To create a new access account, click “Add New Access”, enter the access information, and then click “Save.” The max group number is: 14.

Web Interface

To display the configure SNMP Access in the web interface:

1. Click SNMP and Accesses.
2. Click add new Access.
3. Specify the SNMP access parameters.
4. Click save.
5. If you want to modify or clear the setting, then click reset.



SNMPv3 Accesses Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
□	12314	any	NoAuth, NoPriv	None	None

SNMPv3 Accesses Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
Delete	12314	any	NoAuth, NoPriv	None	None

Figure 2-6.7: The SNMP Accesses Configuration

Parameter description

Delete: Click delete to remove the entry. It will be deleted during the next save.

Group Name: This is 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 ASCII characters from 33 to 126.

Security Model: This 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: This 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: This is the name of the MIB view that defines the MIB objects, which may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Write View Name: This is the name of the MIB view that defines the MIB objects, which may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

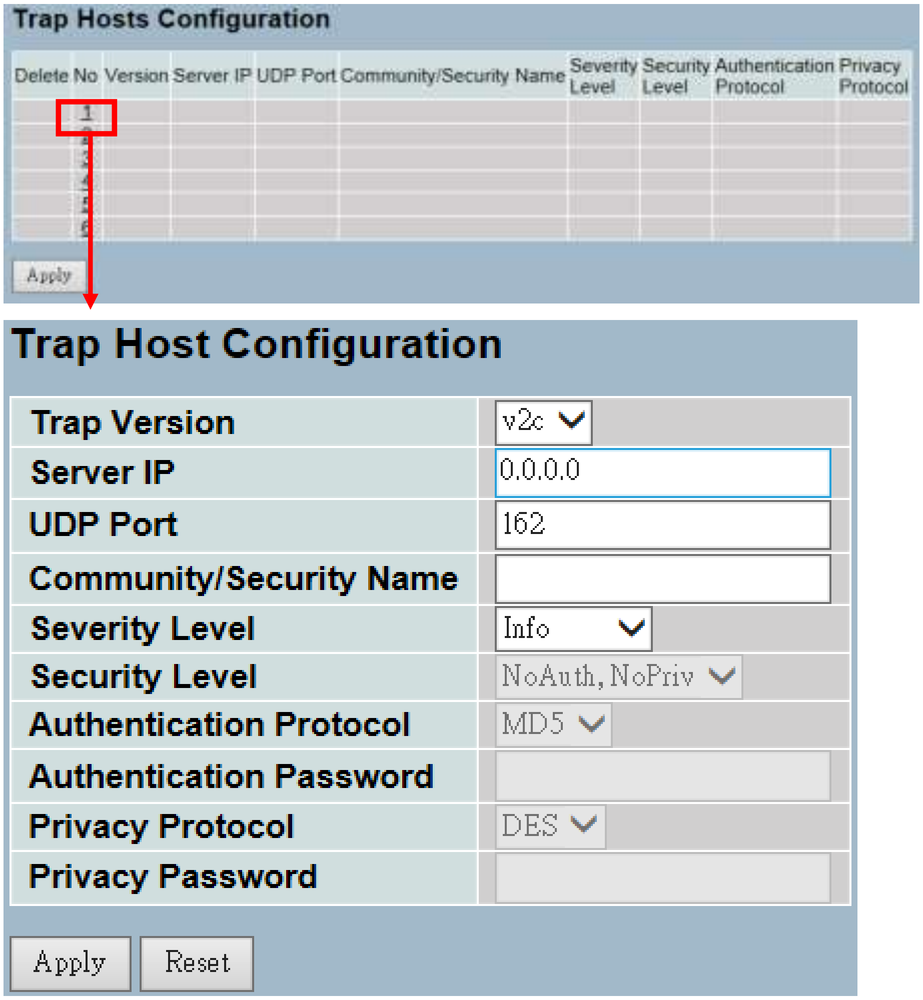
2-6.8 Trap

The trap function is used to configure the SNMP trap. To create a new trap account, click “No number”, enter the trap information and then, click “Apply. The max group number is: 6.

Web Interface

To configure SNMP Trap setting:

1. Click SNMP and Trap .
2. Display the SNMP trap hosts information table.
3. Choose an entry to display and then, modify the parameters or click delete button to delete the trap hosts entry.



Trap Hosts Configuration

Delete	No	Version	Server IP	UDP Port	Community/Security Name	Severity Level	Security Level	Authentication Protocol	Privacy Protocol
	1								
	2								
	3								
	4								
	5								
	6								

Trap Host Configuration

Trap Version	v2c
Server IP	0.0.0.0
UDP Port	162
Community/Security Name	
Severity Level	Info
Security Level	NoAuth, NoPriv
Authentication Protocol	MD5
Authentication Password	
Privacy Protocol	DES
Privacy Password	

Figure 2-6.8: The SNMP Trap Host Configuration

Parameter Description

Delete: Click delete to remove the entry.

Trap Version: You may choose v1, v2c or v3 trap.

Server IP: Use server IP to assign the SNMP host IP address.

UDP Port: Use the UDP port to assign the port number. The default is: 162

Community / Security Name: The length of “Community / Security Name” string is restricted to 1-32.

Security Level: This indicates what kind of message will send to security level. Possible modes are:

- **Info:** Send informations, warnings, and errors.
- **Warning:** Send warnings and errors.
- **Error:** Send errors.

Security Level: There are three types of security level -

- **NoAuth, NoPriv:** No authentication and no privacy.
- **Auth, NoPriv:** Authentication and no privacy.
- **Auth, Priv:** Authentication and privacy.

Authentication Protocol: There are two types of authentication protocol: MD5 or SHA.

Authentication Password: The length of “MD5 Authentication Password” is restricted to 8 – 32.The length of “SHA Authentication Password” is restricted to 8 – 40.

Privacy Protocol: Set the DES encryption for username with privacy protocol.

Privacy Password: The length of privacy password is restricted to 8 – 32.

Chapter 3: Configuration

Chapter 3 provides an overview of the basic network configuration tasks including the ports, Layer 2 network protocol (e.g. VLANs, QoS, IGMP, ACLs, and more), and any setting of the switch.

3-1 Port

This section guide you on the configurations of the detailed port parameters, enable or disable the port, and monitor the ports content or status.

3-1.1 Configuration

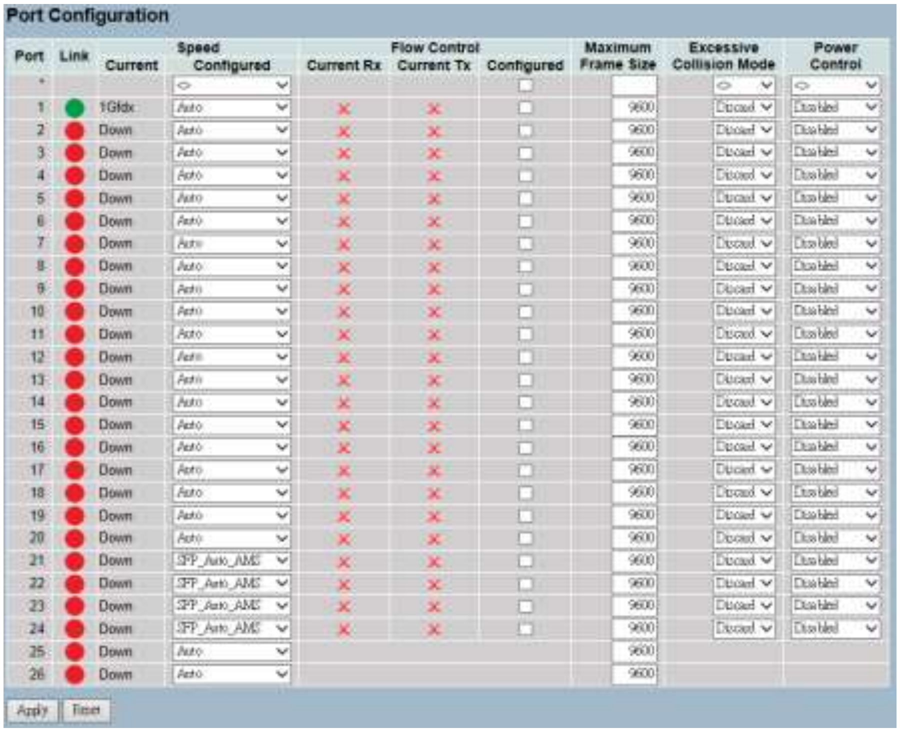
This part provides a description on viewing the current port configuration and how to configure ports to non-default settings, including:

- Linkup/Linkdown
- Speed (Current and Configured)
- Flow Control (Current Rx, Current Tx, and Configured)
- Maximum Frame Size
- Excessive Collision Mode
- Power Control

Web Interface

To configure a current port in the web interface:

1. Click Configuration, Port, and then Configuration.
2. Specify the speed configured, flow control , maximum frame size, excessive collision mode, and power control.
3. Click save.



Port Configuration

Port	Link	Speed		Flow Control			Maximum Frame Size	Excessive Collision Mode	Power Control
		Current	Configured	Current Rx	Current Tx	Configured			
*			<>			□		<>	<>
1	🟢	1Gfdx	Auto	✗	✗	□	9600	Discard	Disabled
2	🔴	Down	Auto	✗	✗	□	9600	Discard	Disabled
3	🔴	Down	Auto	✗	✗	□	9600	Discard	Disabled
4	🔴	Down	Auto	✗	✗	□	9600	Discard	Disabled
5	🔴	Down	Auto	✗	✗	□	9600	Discard	Disabled
6	🔴	Down	Auto	✗	✗	□	9600	Discard	Disabled
7	🔴	Down	Auto	✗	✗	□	9600	Discard	Disabled
8	🔴	Down	Auto	✗	✗	□	9600	Discard	Disabled
9	🔴	Down	Auto	✗	✗	□	9600	Discard	Disabled
10	🔴	Down	Auto	✗	✗	□	9600	Discard	Disabled
11	🔴	Down	Auto	✗	✗	□	9600	Discard	Disabled
12	🔴	Down	Auto	✗	✗	□	9600	Discard	Disabled
13	🔴	Down	Auto	✗	✗	□	9600	Discard	Disabled
14	🔴	Down	Auto	✗	✗	□	9600	Discard	Disabled
15	🔴	Down	Auto	✗	✗	□	9600	Discard	Disabled
16	🔴	Down	Auto	✗	✗	□	9600	Discard	Disabled
17	🔴	Down	Auto	✗	✗	□	9600	Discard	Disabled
18	🔴	Down	Auto	✗	✗	□	9600	Discard	Disabled
19	🔴	Down	Auto	✗	✗	□	9600	Discard	Disabled
20	🔴	Down	Auto	✗	✗	□	9600	Discard	Disabled
21	🔴	Down	SFP_Auto_AMS	✗	✗	□	9600	Discard	Disabled
22	🔴	Down	SFP_Auto_AMS	✗	✗	□	9600	Discard	Disabled
23	🔴	Down	SFP_Auto_AMS	✗	✗	□	9600	Discard	Disabled
24	🔴	Down	SFP_Auto_AMS	✗	✗	□	9600	Discard	Disabled
25	🔴	Down	Auto				9600		
26	🔴	Down	Auto				9600		

Figure 3-1.1: The Port Configuration

Parameter Description

Port: This is the logical port number for this row.

Link: The current link state is displayed graphically. Green indicates the link is up and red indicates that it is down.

Current Link Speed: This provides the current link speed of the port.

Configured Link Speed: This selects any available link speed for the given switch port.

- **Auto Speed:** Selects the highest speed that is compatible with a link partner.
- **Disabled:** Disables the switch port operation.

Flow Control: When "Auto Speed" is selected on a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The "Current Rx" column indicates whether pause frames on the port are obeyed, and the "Current Tx" column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last auto-negotiation.

Check the configured column to use flow control. This setting is related to the setting for configured link speed.

Maximum Frame Size: Enter the maximum frame size allowed for the switch port, including FCS.

Excessive Collision Mode: This configures the port transmit collision behavior.

Discard: This discards the frame after 16 collisions (default).

Restart: This restarts the backoff algorithm after 16 collisions.

Power Control: The "Usage" column shows the current percentage of the power consumption per port. The "Configured" column allows for changing the power savings mode parameters per port.

- **Disabled:** All power savings mechanisms disabled.
- **ActiPHY:** Link down power savings enabled.
- **PerfectReach:** Link up power savings enabled.
- **Enabled:** Both link up and link down power savings enabled.

Buttons

- **Apply** – Click to apply changes.
- **Reset**- Click to restore default settings.

Upper Right Icon (Refresh): Click refresh to manually refresh the port link status.

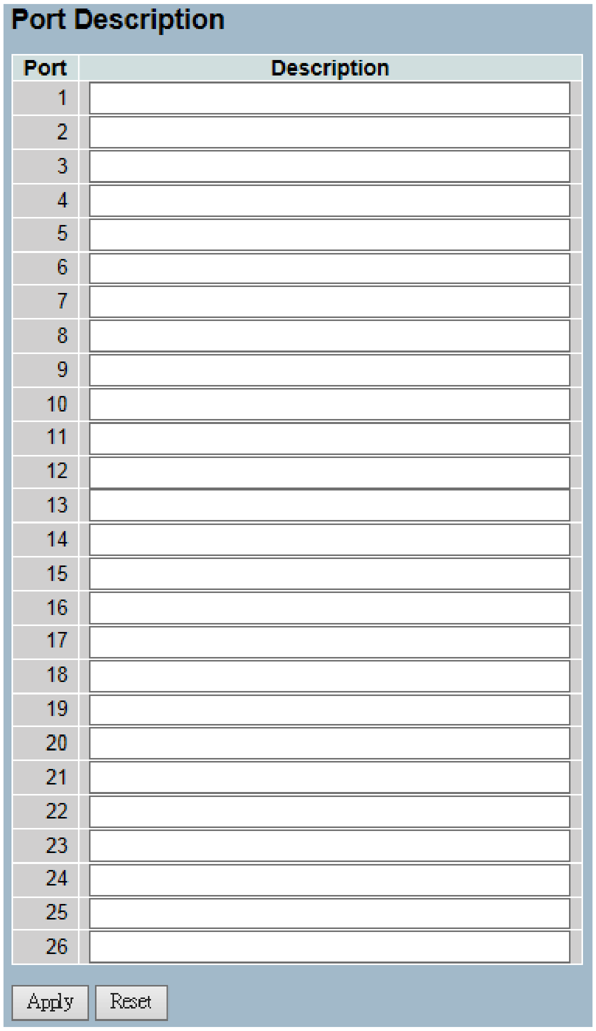
3-1.2 Port Description

The section guides you on how to configure the port's alias or descriptions for the port identity. You are able to an alphanumeric string describing the full name and version identification for the system's hardware type, software version, and networking application.

Web Interface

To configure a port description in the web interface:

1. Click Configuration, Port, and then Port Description.
2. Specify the detailed port alias or description - an alphanumeric string describing the full name and version identification for the system's hardware type, software version, and networking application.
3. Click save.



Port Description

Port	Description
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	

Figure 3-1.2: The Port Configuration

Parameter Description

Port: This is the logical port number for this row.

Description: This describes and identifies the port. Up to 47 characters are allowed.

Buttons

- **Apply** – Click to save changes.
- **Reset**- Click to restore default settings.

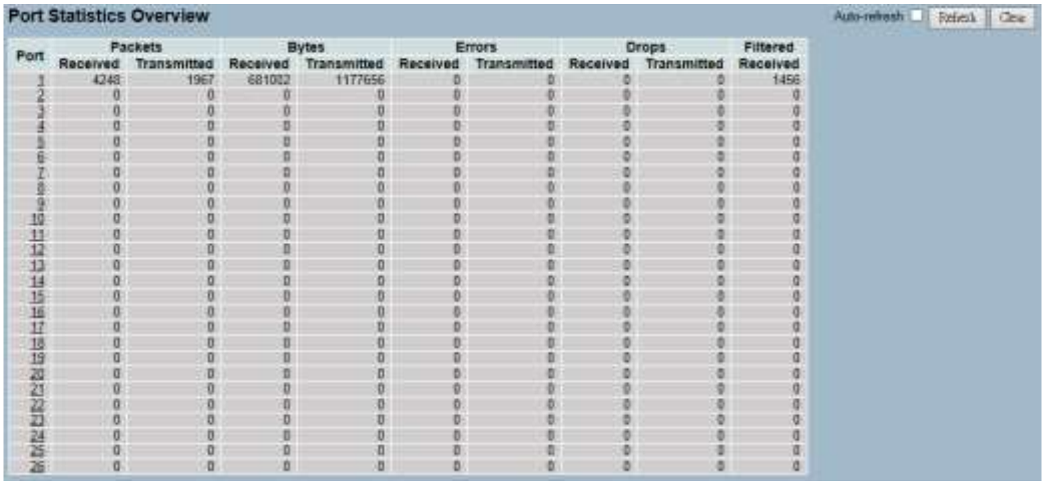
3-1.3 Traffic Overview

The section describes the port statistics information and provides an overview of general traffic statistics for all ports on the switch.

Web Interface

To display the port statistics overview in the web interface:

1. Click Configuration, Port, and then Traffic Overview.
2. Click “Auto-refresh” to automatically refresh the traffic overview.
3. Click “Refresh” to refresh the port statistics or click “Clear” to clear all information.



Port Statistics Overview

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	4248	1967	681082	1177656	0	0	0	0	1456
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	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0	0

Figure 3-1.3: The Port Statistics Overview

Parameter Description

Port: This is the logical port for the settings contained in the same row.

Packets: The number of received & transmitted packets per port.

Bytes: The number of received and transmitted bytes per port.

Errors: The number of frames received in error and the number of incomplete transmissions per port.

Drops: The number of frames discarded due to ingress or egress congestion.

Filtered: The number of received frames filtered by forwarding.

Auto-Refresh: Click auto-refresh to automatically refresh the statistics.

Upper Right Icon (Refresh, Clear): Click manually refresh or clear the port statistics.

3-1.4 Detailed Statistics

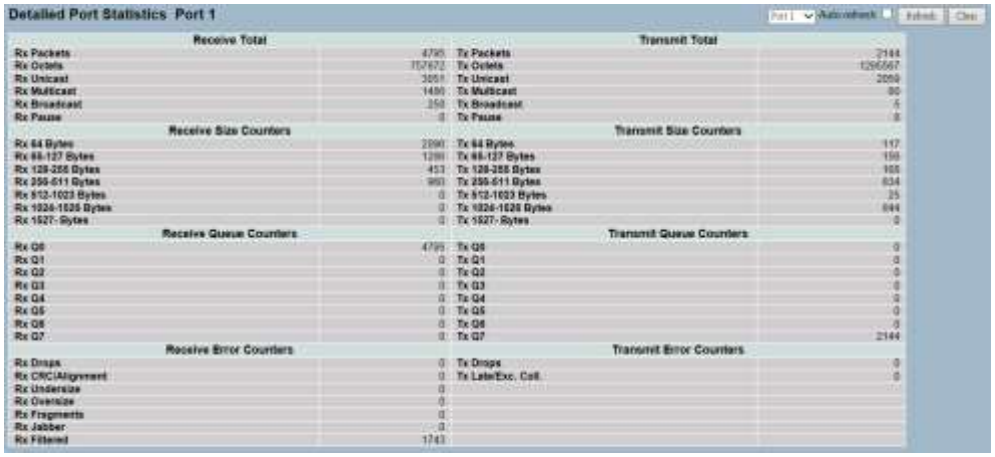
The section provides detailed traffic statistics for a specific port on the switch. Click on the port select box to display the port details.

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

Web Interface

To display the per-port detailed statistics overview in the web interface:

1. Click Configuration, Port, and then Detailed Port Statistics.
2. Scroll the port index to select which port you want to show the detailed statistics for.
3. Click auto-refresh to automatically refresh the information.
4. Click refresh to manually refresh the statistics and click clear to clear the information.



Detailed Port Statistics Port 1

Receive Total		Transmit Total	
Rx Packets	4795	Tx Packets	2144
Rx Octets	757672	Tx Octets	1296567
Rx Unicast	3051	Tx Unicast	2059
Rx Multicast	1490	Tx Multicast	80
Rx Broadcast	250	Tx Broadcast	5
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	2090	Tx 64 Bytes	117
Rx 65-127 Bytes	1290	Tx 65-127 Bytes	150
Rx 128-255 Bytes	453	Tx 128-255 Bytes	165
Rx 256-511 Bytes	960	Tx 256-511 Bytes	834
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	25
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	844
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	4795	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	2144
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	1743		

Figure 3-1.4: The Port Detail Statisitcs Overview

Parameter Description

Auto-Refresh: Click auto-refresh to automatically refresh the information.

Upper Left Scroll Bar: To scroll which port to display the statistics for with “Port-0”, “Port-1”, ...

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 to indicate a PAUSE operation.

Receive and Transmit Size Counters

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

Receive and Transmit Queue Counters

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

Receive Error Counters

Rx Drops: The number of frames dropped due to lack of receive buffers or egress congestion.

Rx CRC/Alignment: The number of frames received with CRC or alignment errors.

Rx Undersize: The number of short 1 frames received with valid CRC.

Rx Oversize: The number of long 2 frames received with valid CRC.

Rx Fragments: The number of short 1 frames 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.

- Short frames are frames that are smaller than 64 bytes.
- Long frames are frames that are longer than the configured maximum frame length for this port.

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.

Auto-refresh: Click auto-refresh to automatically refresh the queuing counters.

Upper right icon (Refresh, clear): Click these buttons to manually refresh or clear the port detail statistics.

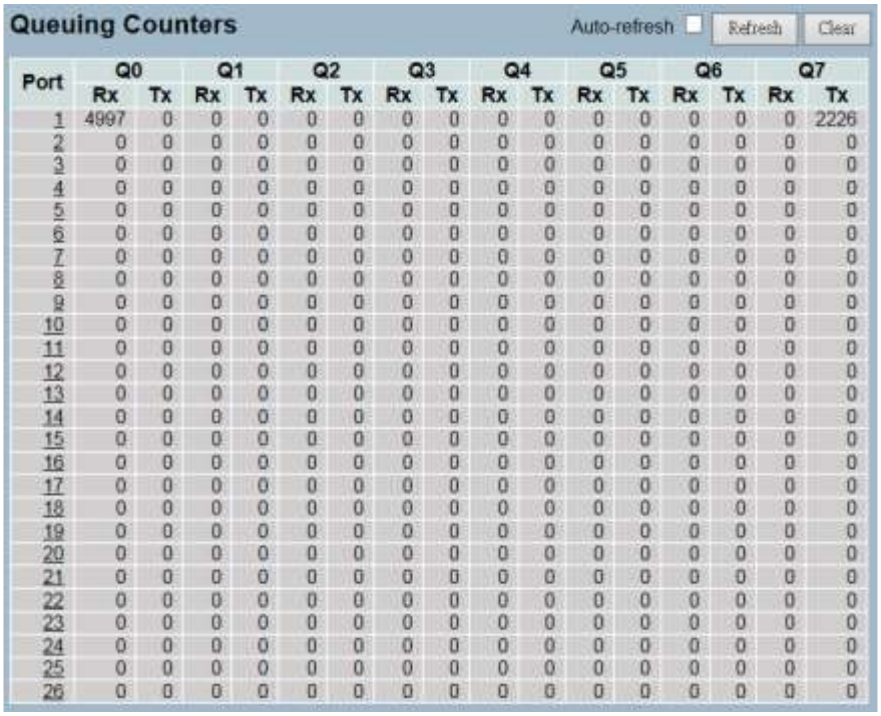
3-1.5 QoS Statistics

This section explains how the switch could display different QoS detailed queuing counters for a specific port.

Web Interface

To display the queueing counters in the web interface:

1. Click Configuration, Port, and then QoS Statistics.
2. Click auto-refresh to automatically refresh the information.
3. Click refresh or clear to manually refresh or clear the queueing counters.



Queuing Counters

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	4997	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2226
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 3-1.5: The Queuing Counters Overview

Parameter Description

Port: The logical port for the settings contained in the same row.

Qn: Qn is the Queue number and QoS queues per port. Q0 is the lowest priority queue.

Rx/Tx: The number of received and transmitted packets per queue.

Auto-Refresh: Click auto-refresh to automatically refresh the queuing counters.

Upper Right Icon (Refresh, clear): Click these buttons to manually clear or refresh the queuing counters.

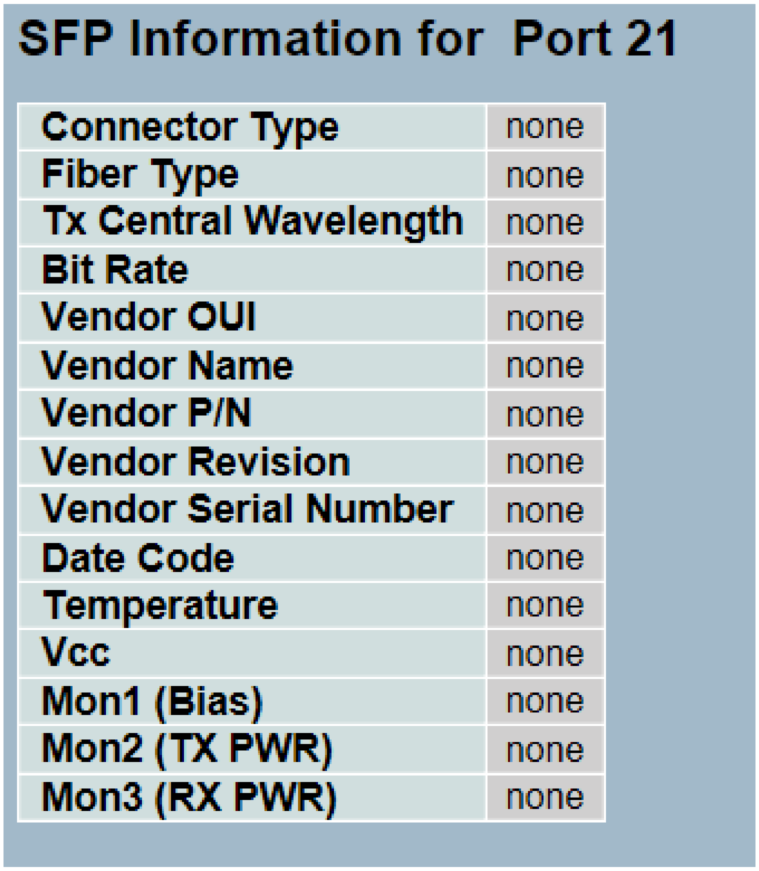
3-1.6 SFP Information

The switch could display the SFP module detail information which you connect it to the switch. The information includes connector type, fiber type, wavelength, banud rate, vendor OUI, and more.

Web Interface

To display the SFP information in the web interface:

1. Click Configuration, Port, and then SFP Information.
2. To display the SFP information.



SFP Information for Port 21

Connector Type	none
Fiber Type	none
Tx Central Wavelength	none
Bit Rate	none
Vendor OUI	none
Vendor Name	none
Vendor P/N	none
Vendor Revision	none
Vendor Serial Number	none
Date Code	none
Temperature	none
Vcc	none
Mon1 (Bias)	none
Mon2 (TX PWR)	none
Mon3 (RX PWR)	none

Figure 3-1.6: The SFP Information Overview

Parameter Description

Connector Type: This displays the connector type such as UTP, SC, ST, LC, and so on.

Fiber Type: This displays the fiber mode such as multi-mode or single-mode.

Tx Central Wavelength: This displays the fiber optical transmitting central wavelength such as 850nm, 1310nm, 1550nm, and so on.

Baud Rate: This displays the maximum baud rate of the fiber module supported such as 10M, 100M, 1G, and so on.

Vendor OUI: This displays the manufacturer's OUI code which is assigned by IEEE.

Vendor Name: This displays the company name of Vigitron, Inc.

Vendor P/N: This displays the product name by Vigitron, Inc.

Vendor Rev (Revision): This displays the module revision.

Vendor SN (Serial Number): This shows the serial number assigned Vigitron, Inc.

Date Code: This shows the date this SFP module was made.

Temperature: This shows the current temperature of SFP module.

Vcc: This shows the working DC voltage of SFP module.

Mon1(Bias) mA: This shows the Bias current of SFP module.

Mon2(TX PWR): This shows the transmit power of SFP module.

Mon3(RX PWR): This shows the receiver power of SFP module.

3-1.7 EEE

The section guides you through the inspection and configurations of the current EEE port settings.

EEE is a power saving option that reduces the power usage when there is very low traffic utilization (or no traffic).

EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted, all circuits are powered up. The time it takes to power up the circuits is called the wakeup time. The default wakeup time is 17us for 1Gbit links and 30us for other link speeds. The EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting devices have all circuits powered up when traffic is transmitted. The devices can exchange information about the devices wakeup time by using the LLDP protocol.

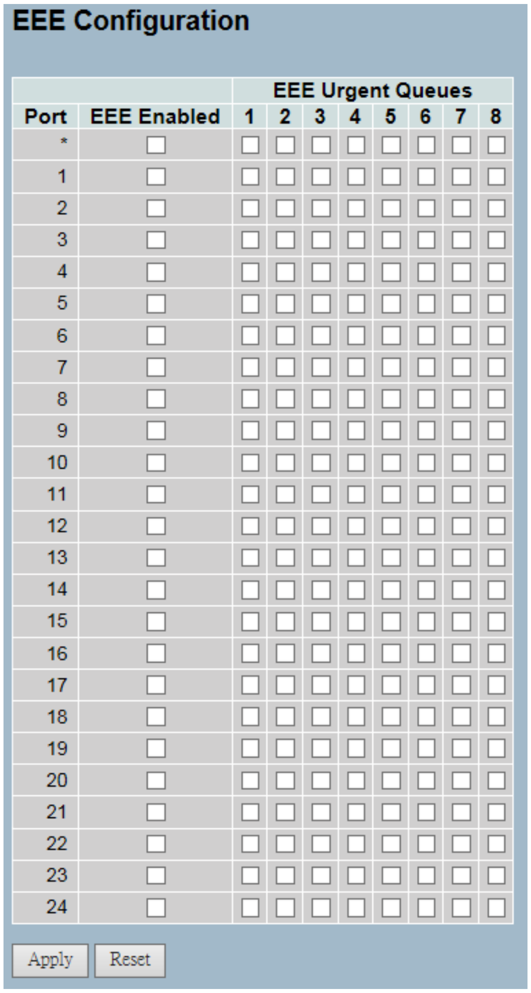
To maximize power saving, the circuit isn't started at once transmit data are ready for a port. Instead, it’s queued until 3000 bytes of data are ready to be transmitted. In case there are data less than 3000 bytes ready to be transmitted, data are always transmitted after 48us to give a maximum latency of 48 us + the wakeup time. This avoids a large delay.

It is possible to minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS) and then mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time.

Web Interface

To configure the EEE configuration in the web interface:

1. Click Configuration, Port, and then EEE.
2. Choose the port you want to enable the EEE function on and choose the EEE urgent queues level from 1 to 8. The queue will postpone the tranmission until 3000 bytes are ready to be transmitted (unless otherwise noted).
3. Click save.
4. Click reset to restore default settings.



EEE Configuration

		EEE Urgent Queues							
Port	EEE Enabled	1	2	3	4	5	6	7	8
*	□	□	□	□	□	□	□	□	□
1	□	□	□	□	□	□	□	□	□
2	□	□	□	□	□	□	□	□	□
3	□	□	□	□	□	□	□	□	□
4	□	□	□	□	□	□	□	□	□
5	□	□	□	□	□	□	□	□	□
6	□	□	□	□	□	□	□	□	□
7	□	□	□	□	□	□	□	□	□
8	□	□	□	□	□	□	□	□	□
9	□	□	□	□	□	□	□	□	□
10	□	□	□	□	□	□	□	□	□
11	□	□	□	□	□	□	□	□	□
12	□	□	□	□	□	□	□	□	□
13	□	□	□	□	□	□	□	□	□
14	□	□	□	□	□	□	□	□	□
15	□	□	□	□	□	□	□	□	□
16	□	□	□	□	□	□	□	□	□
17	□	□	□	□	□	□	□	□	□
18	□	□	□	□	□	□	□	□	□
19	□	□	□	□	□	□	□	□	□
20	□	□	□	□	□	□	□	□	□
21	□	□	□	□	□	□	□	□	□
22	□	□	□	□	□	□	□	□	□
23	□	□	□	□	□	□	□	□	□
24	□	□	□	□	□	□	□	□	□

Figure 3-1.7: The EEE Configuration

Parameter Description

EEE Port Configuration: This is the EEE port settings relate to the currently selected.

Port: This is the switch port number of the logical EEE port.

EEE Enabled: This controls whether the EEE is enabled for this switch port.

EEE Urgent Queues: This queues set will activate transmission of frames as soon as any data is available. Otherwise, the queue will postpone the transmission until 3000 bytes are ready to be transmitted.

Buttons

- **Save** – Click to save changes.
- **Reset**- Click to restore default settings.

3-2 ACL

The Vi3326 switch access control list (ACL) is probably the most commonly used object in the IOS. It is used for packet filtering and for selecting the types of traffic to be analyzed, forwarded, or influenced in some way. The ACLs are divided into EtherTypes - IPv4, ARP protocol, MAC, VLAN parameters, and more. This section gives an overview of standard and extended access lists for TCP/IP. As you create ACEs for ingress classification, you can assign a policy for each port from 1-8. However, each policy can be applied to any port. This makes it very easy to determine what type of ACL policy you will be working with.

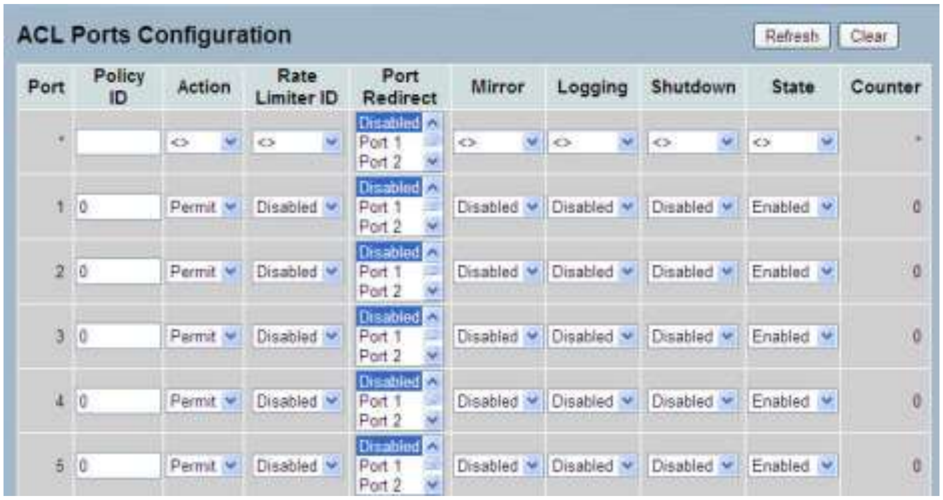
3-2.1 Ports

The section provides configurations of the ACL parameters (ACE) for each port. These parameters will affect frames received on a port, unless the frame matches a specific ACE.

Web Interface

To configure the ACL ports configuration in the web interface:

1. Click Configuration, ACL, and then Ports.
2. Scroll the specific parameter value to select the correct value for port ACL setting.
3. Click save.
4. Click reset to restore default settings.
5. After completing the configuration, you may now click refresh or clear to manually refresh or clear the counter information.



ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*		<>	<>	Disabled Port 1 Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0

Figure 3-2.1: The ACL Ports Configuration

Parameter Description

Port: This is the logical port for the settings contained in the same row.

Policy ID: This selects the policy to apply to this port. The allowed values are 0 through 255. The default value is 0.

Action: This selects whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".

Rate Limiter ID: This selects 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: This selects which port frames are redirected on. The allowed values are disabled or a specific port number. The default value is "Disabled".

Mirror: This specifies the mirror operation of the 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: This specifies the logging operation of the 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: This specifies the port shut down operation of the port. The allowed values are:

- **Enabled:** If a frame is received on the port, the port will be disabled.
- **Disabled:** Port shut down is disabled.
- The default value is "Disabled".

State: This specifies the port state of the 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: This counts the number of frames that match this ACE.

Buttons

- **Apply** – Click to save changes.
- **Reset** - Click to restore default settings.
- **Refresh** – Click refresh to manually refresh information.
- **Clear** - Click to manually clear the counters.

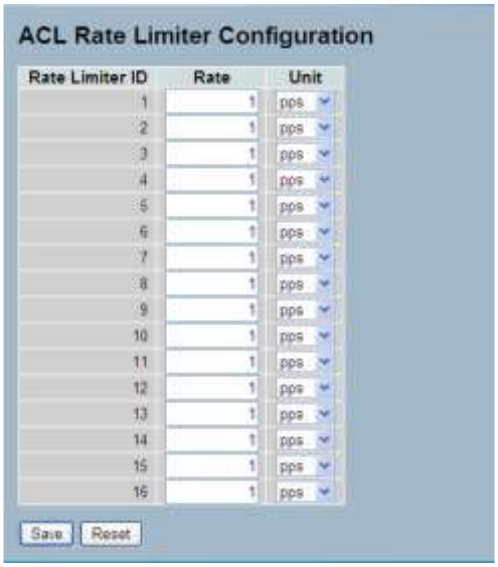
3-2.2 Rate Limiters

The section provides configurations for the switch’s ACL rate limiter parameters. The rate limiter level is from 1 to 16. You can set the rate limiter value and units with pps or kbps.

Web Interface

To configure ACL rate limiter in the web interface:

1. Click Configuration, ACL, and then Rate Limiter.
2. Specify the rate field from 0 to 3276700.
3. Choose the unit - pps or kbps.
4. Click save.
5. Click reset to restore default settings.



ACL Rate Limiter Configuration

Rate Limiter ID	Rate	Unit
1	1	pps
2	1	pps
3	1	pps
4	1	pps
5	1	pps
6	1	pps
7	1	pps
8	1	pps
9	1	pps
10	1	pps
11	1	pps
12	1	pps
13	1	pps
14	1	pps
15	1	pps
16	1	pps

Figure 3-2.2: The ACL Rate Limiter Configuration

Parameter Description

Rate Limiter ID: The rate limiter ID for the settings contained in the same row.

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.
- **Kbps:** Kbits per second.

Buttons

- **Apply** – Click to save changes.
- **Reset**- Click to restore default settings.

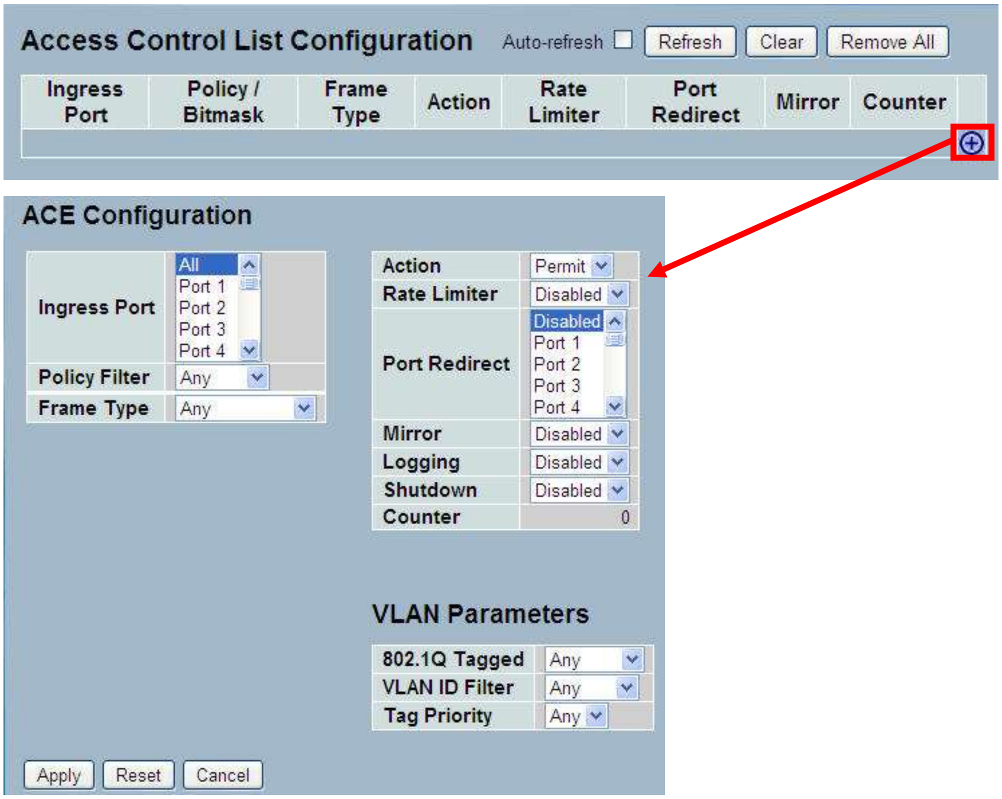
3-2.3 Access Control List

The section provides configurations for the access control list rule. An Access Control List (ACL) is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other specific criteria. This switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the frame is accepted. Other actions can also be invoked when a matching packet is found including rate limiting, copying matching packets to another port or to the system log, or shutting down a port. Each row of the ACL describes the ACE that is defined. The maximum number of ACEs on each switch is 256. Click on the lower 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 Interface

To configure access control list in the web interface:

1. Click Configuration, ACL, and then Configuration.
2. Click the ⊕ button to add a new ACL, or use the other ACL modification buttons to specify the editing action such as edit, delete, or moving the relative position of an entry in the list.
3. Specify the parameters of the ACE.
4. Click save.
5. Click reset to restore default settings.
6. When editing an entry on the ACE configuration page, note that the items displayed depend on various selections such as frame type and ip protocol type. Specify the relevant criteria to be matched for this rule, and set the actions to take when a rule is matched such as rate limiter, port copy, logging, and shutdown.



Access Control List Configuration

Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter

ACE Configuration

Ingress Port	All Port 1 Port 2 Port 3 Port 4
Policy Filter	Any
Frame Type	Any

Action	Permit
Rate Limiter	Disabled
Port Redirect	Disabled Port 1 Port 2 Port 3 Port 4
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

VLAN Parameters

802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any

Figure 3-2.3: The ACL Rate Limiter Configuration

Parameter Description

Ingress Port: This 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: This indicates the policy number and bitmask of the ACE.

Frame Type: This 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: This indicates the forwarding action of the ACE.

- **Permit:** Frames matching the ACE may be forwarded and learned.
- **Deny:** Frames matching the ACE are dropped.

Rate Limiter: This 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: This indicates the port redirect operation of the ACE. Frames matching the ACE are copied to the port number. The allowed values are disabled or a specific port number. When “Disable” is displayed, the port copy operation is disabled.

Mirror: This specifies the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are:

- **Enabled:** Frames received on the port are mirrored.
- **Disabled:** Frames received on the port are not mirrored.
- The default value is "Disabled".

Counter: The counter indicates the number of times the ACE was hit by a frame.

Modification Buttons: Modify each ACE (Access Control Entry) in the table using the following buttons:

⊕ Inserts a new ACE before the current row.

ⓔ Edits the ACE row.

⬆ Moves the ACE up the list.

⬇ Moves the ACE down the list.

⊗ Deletes the ACE.

⊕ (Lower plus sign) Adds a new entry to the bottom of the list.

Buttons

- **Auto-refresh** - Click to automatically refresh the page.
- **Refresh** - Click refresh to manually refresh the page.
- **Clear** - Click to clear the counters.
- **Remove All** - Click to remove all ACEs.

___ Parameter Description

Ingress Port: This selects the ingress port to apply the ACE on.

- **All:** The ACE applies to all port.
- **Port n:** The ACE applies to this port number, where n is the number of the switch port.

Policy Filter: This specifies 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 an policy value and bitmask appears.

Policy Value: When "Specific" is selected for the policy filter, you can enter a specific policy value. The allowed range is 0 to 255.

Policy Bitmask: When "Specific" is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is 0x0 to 0xff.

Frame Type: Select the frame type for this ACE. These frame types 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).
- **ARP:** Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with ethernet type.
- **IPv4:** Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with ethernet type.
- **IPv6:** Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with ehternet type.

Action: This specifies 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.

Rate Limiter: This specifies the rate limiter in number of base units. The allowed range is 1 to 16. Disabled indicates that the rate limiter operation is disabled.

Port Redirect: Frames that hit the ACE are redirected to the port number specified here. The allowed range is the same as the switch port number range. Disabled indicates that the port redirect operation is disabled.

Mirror: This specifies 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".

Logging: This indicates the logging operation of the ACE. Possible values are:

- **Enabled:** Frames matching the ACE are stored in the System Log.
- **Disabled:** Frames matching the ACE are not logged.
- Please note that the system log memory size and logging rate is limited.

Shutdown: This indicates the port shut down operation of the ACE. Possible values are:

- **Enabled:** If a frame matches the ACE, the ingress port will be disabled.
- **Disabled:** Port shut down is disabled for the ACE.

Counter: The counter indicates the number of times the ACE was hit by a frame.

Buttons

- **Apply** – Click to save changes.
- **Reset**- Click to restore to default settings.

VLAN Parameter Description

802.1Q Tagged: This specifies 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: This specifies 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: This specifies the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7. The value “Any” means that no tag priority is specified (tag priority is "don't-care").

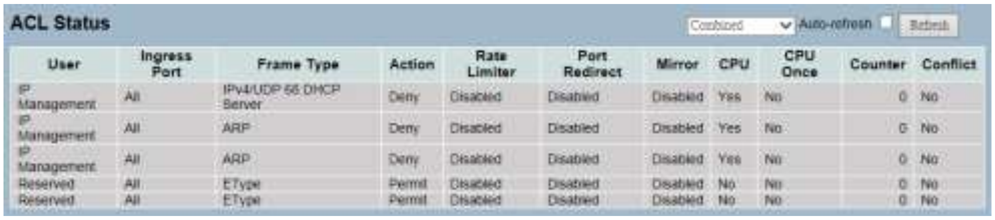
3-2.4 ACL Status

The section provides information on how to show 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 Interface

To display the ACL status in the web interface:

1. Click Configuration, ACL, and then ACL status.
2. Click auto-refresh to automatically refresh the information.
3. Click refresh to manually refresh the information.



ACL Status

User	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	CPU	CPU Once	Counter	Conflict
IP Management	All	IPv4/UDP 68 DHCP Server	Deny	Disabled	Disabled	Disabled	Yes	No	0	No
IP Management	All	ARP	Deny	Disabled	Disabled	Disabled	Yes	No	0	No
IP Management	All	ARP	Deny	Disabled	Disabled	Disabled	Yes	No	0	No
Reserved	All	EType	Permit	Disabled	Disabled	Disabled	No	No	0	No
Reserved	All	EType	Permit	Disabled	Disabled	Disabled	No	No	0	No

Figure 3-2.4: The ACL Rate Limiter Configuration

Parameter Description

User: This indicates the ACL user.

Ingress Port: This 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.

Frame Type: This 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: This indicates the forwarding action of the ACE.

- **Permit:** Frames matching the ACE may be forwarded and learned.
- **Deny:** Frames matching the ACE are dropped.

Rate Limiter: This 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: This indicates the port redirect operation of the ACE. Frames matching the ACE are copied to the port number. The allowed values are "Disabled" or a specific port number. When "Disabled" is displayed, the port copy operation is disabled.

Mirror: This specifies 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".

CPU: This forwards packet that matched the specific ACE to CPU.

CPU Once: This forwards first packet that matched the specific ACE to CPU.

Counter: The counter indicates the number of times the ACE was hit by a frame.

Conflict: This indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

Auto-refresh: Click to automatically refresh the information.

Upper right icon (Refresh): Click refresh to manually refresh the ACL status information.

3-3 Aggregation

Aggregation is used to configure the settings of Link Aggregation. You can bundle more than one port with the same speed, full duplex, and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipment's to build the bandwidth aggregation. For example, if there are three fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth three times as high as a single fast Ethernet port has.

3-3.1 Static Trunk

Aggregation configuration is used to configure the settings of link aggregation. You can bundle more than one port with the same speed, full duplex, and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipment's to build the bandwidth aggregation.

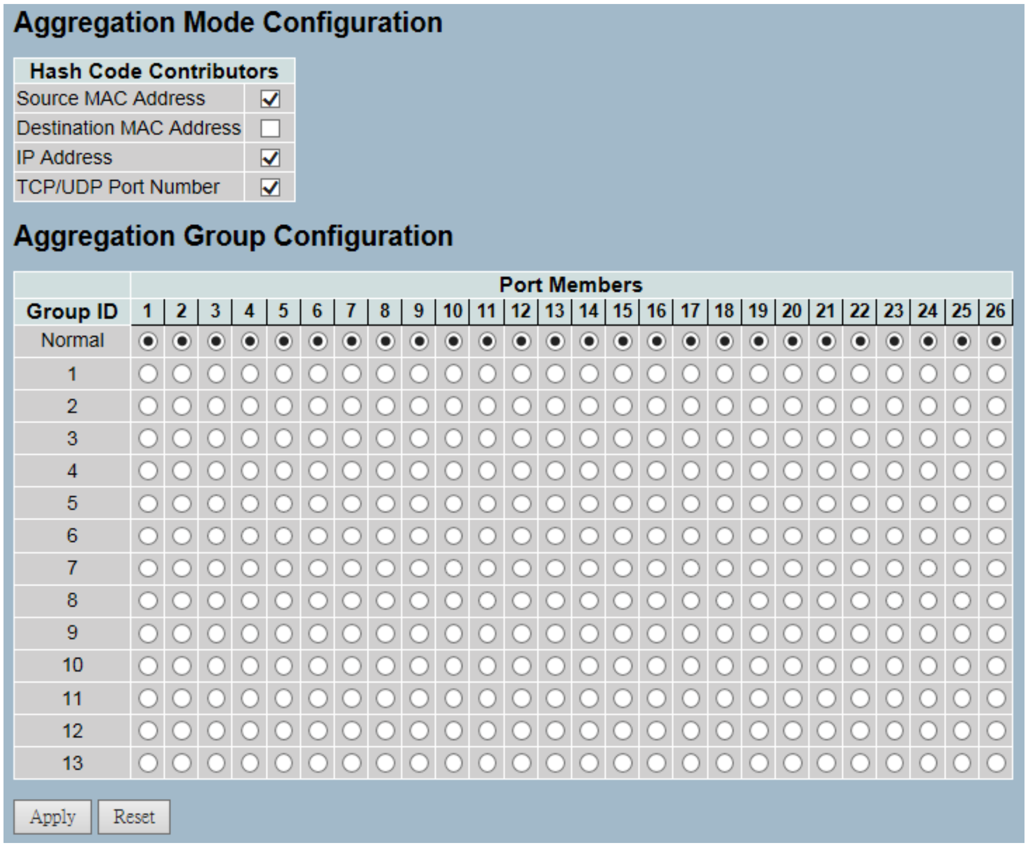
3-1.1.1 Static Trunk

Ports using static trunk as their trunk method can choose their unique Static GroupID to form a logic "trunked port". The benefit of using the static trunk method is that a port can immediately become a member of a trunk group without any handshaking with its peer port. This is also a disadvantage because the peer ports of the static trunk group may not know that they should be aggregate together to form a "logic trunked port". Using static trunk on both end of a link is strongly recommended. Please also note that low speed links will stay in the "not ready" state when using static trunk to aggregate with high speed links.

Web Interface

To configure the trunk aggregation hash mode and aggregation group in the web interface:

1. Click Configuration, Static Trunk, and then Aggregation Mode Configuration.
2. Click to enable or disable the aggregation mode function.
3. Choose the aggregation group ID and port members.
4. Click save.
5. Click reset to restore default settings.



Aggregation Mode Configuration

Hash Code Contributors	
Source MAC Address	☑
Destination MAC Address	□
IP Address	☑
TCP/UDP Port Number	☑

Aggregation Group Configuration

	Port Members																									
Group ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Normal	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
1	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
2	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
3	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
4	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
5	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
6	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
7	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
8	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
9	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
10	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
11	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
12	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
13	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Figure 3-3.1.1: The Aggregation Mode Configuration

Parameter Description

<u>**Hash Code Contributors**</u>

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, the source MAC address is enabled.

Destination MAC Address: The destination MAC address can be used to calculate the destination port for the frame. Check to enable the use of the destination MAC address, or uncheck to disable. By default, the 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, the IP dddress is enabled.

TCP/UDP Port Number: The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP port number, or uncheck to disable. By default, the TCP/UDP port number is enabled.

Aggregation Group Configuration

Group ID: This 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.

Buttons

- **Save** – Click to save changes.
- **Reset**- Click to restore default seetings.

3-3.2 LACP

Ports, using link aggregation control protocol (according to IEEE 802.3ad specification) as their trunking method, can choose their unique LACP GroupID to form a logic "trunked port". The benefit of using LACP is that a port makes an agreement with its peer port before it becomes a ready member of a "trunk group" (also called aggregator). LACP is safer than the other trunking method - static trunk.

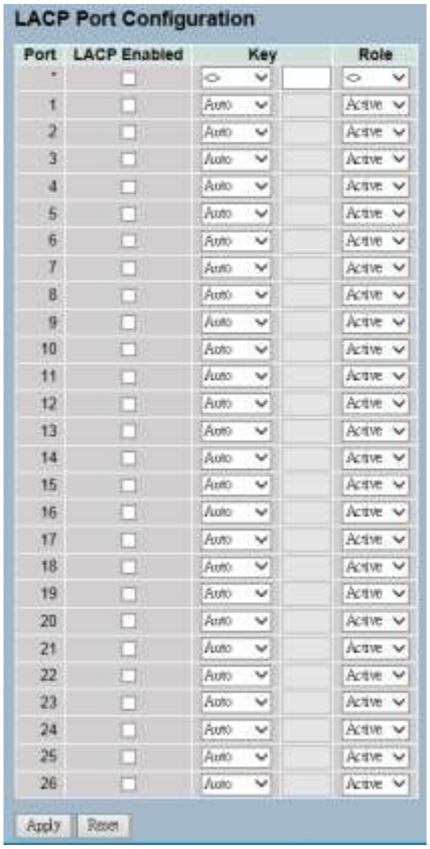
3-3.2.1 Configuration

This page allows the user to inspect the current LACP port configurations, and possibly change them. An LACP trunk group with more than one ready member-ports is a "real trunked" group. An LACP trunk group with only one or less than one ready member-ports is not a "real trunked" group.

Web Interface

To configure the trunk aggregation LACP parameters in the web interface:

1. Click Configuration, LACP, and Configuration.
2. Click to enable or disable the LACP on the port.
3. Click to choose auto or specific for the key parameter. The default is auto.
4. Click to choose active or passive for the role. The default is active.
5. Click save.
6. Click reset to restore default settings.



LACP Port Configuration

Port	LACP Enabled	Key		Role
*	□	<>		<>
1	□	Auto		Active
2	□	Auto		Active
3	□	Auto		Active
4	□	Auto		Active
5	□	Auto		Active
6	□	Auto		Active
7	□	Auto		Active
8	□	Auto		Active
9	□	Auto		Active
10	□	Auto		Active
11	□	Auto		Active
12	□	Auto		Active
13	□	Auto		Active
14	□	Auto		Active
15	□	Auto		Active
16	□	Auto		Active
17	□	Auto		Active
18	□	Auto		Active
19	□	Auto		Active
20	□	Auto		Active
21	□	Auto		Active
22	□	Auto		Active
23	□	Auto		Active
24	□	Auto		Active
25	□	Auto		Active
26	□	Auto		Active

Figure 3-3.2.1: The LACP Port Configuration

Parameter Description

Port: The switch port number.

LACP Enabled: This controls whether the LACP is enabled on this switch port. The LACP will form an aggregation when 2 or more ports are connected to the same partner. LACP can form max 12 LLAGs per switch and 2 GLAGs.

Key: The key value incurred by the port from 1 to 65535 . The auto setting will set the key as appropriate by the physical link speed - 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same key value can participate in the same aggregation group, while ports with different keys cannot.

Role: The role shows the LACP activity status. Active will transmit LACP packets each second, while passive will wait for a LACP packet from a partner (speak if spoken to).

Buttons

- **Save** – Click to save changes.
- **Reset**- Click to restore default settings.

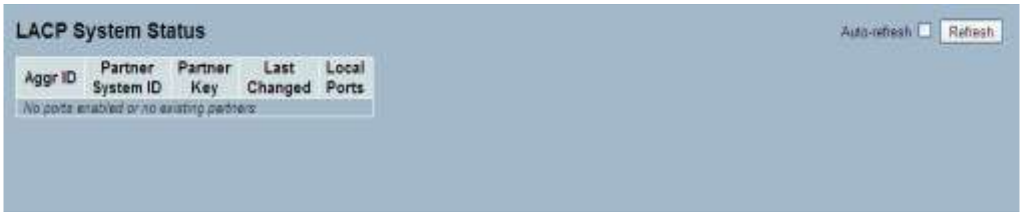
3-3.2.2 System Status

This section provides the status overview for all LACP instances after completing the LACP function set-up.

Web Interface

To display the LACP system status in the web interface:

1. Click Configuration, LACP, and System Status.
2. Click auto-refresh to automatically refresh the LACP system status.
3. Click refresh to manually refresh the LACP system status.



LACP System Status

Auto-refresh □ Refresh

Aggr ID	Partner System ID	Partner Key	Last Changed	Local Ports
No ports enabled or no existing partners				

Figure 3-3.2.2: The LACP System Status

Parameter Description

Aggr ID: The aggregation ID associated with this aggregation instance. For LLAG, the ID is shown as “isid:aggr-id” and for GLAGs, the ID is shown as “aggr-id”.

Partner System ID: This is the system ID (MAC address) of the aggregation partner.

Partner Key: The key that the partner has assigned to this aggregation ID.

Last Changed: This is the time since this aggregation changed.

Local Ports: This shows which ports are a part of this aggregation for this switch. The format is: "Switch ID:Port".

Auto-Refresh: Click to automatically refresh the information.

Upper Right Icon (Refresh): Click refresh to manually refresh the information.

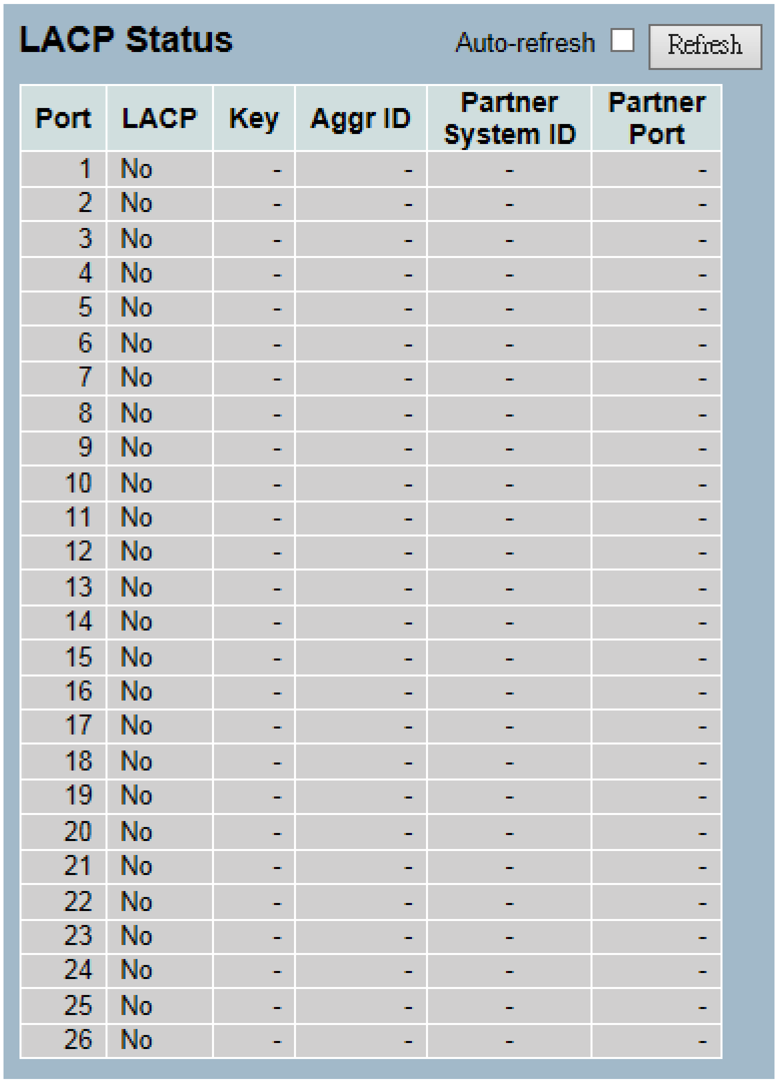
3-3.2.3 Port Status

Once you've completed the LACP function set-up, this section provides information on the port status overview for all LACP instances.

Web Interface

To display the LACP port status in the web interface:

1. Click Configuration, LACP, and Port Status.
2. Click auto-refresh to automatically refresh all LACP port status.
3. Click refresh to manually refresh all LACP port status.



Port	LACP	Key	Aggr ID	Partner System ID	Partner Port
1	No	-	-	-	-
2	No	-	-	-	-
3	No	-	-	-	-
4	No	-	-	-	-
5	No	-	-	-	-
6	No	-	-	-	-
7	No	-	-	-	-
8	No	-	-	-	-
9	No	-	-	-	-
10	No	-	-	-	-
11	No	-	-	-	-
12	No	-	-	-	-
13	No	-	-	-	-
14	No	-	-	-	-
15	No	-	-	-	-
16	No	-	-	-	-
17	No	-	-	-	-
18	No	-	-	-	-
19	No	-	-	-	-
20	No	-	-	-	-
21	No	-	-	-	-
22	No	-	-	-	-
23	No	-	-	-	-
24	No	-	-	-	-
25	No	-	-	-	-
26	No	-	-	-	-

Figure 3-3.2.3: The LACP Status

Parameter Description

Port: This is the switch port number.

LACP: “Yes” means that LACP is enabled and the port link is up. “No” means that LACP is not enabled or that the port link is down. “Backup” means that the port could not join the aggregation group, but will join if other port leaves. Meanwhile, the LACP status is disabled.

Key: The key assigned to this port. Only ports with the same key can aggregate together.

Aggr ID: The aggregation ID assigned to this aggregation group. IDs 1 and 2 are GLAGs, while IDs 3-14 are LLAGs.

Partner System ID: This is the partner's system ID (MAC address).

Partner Port: This is the partner's port number connected to this port.

Auto-refresh: Click to automatically refresh the information.

Upper right icon (Refresh): Click refresh to manually refresh the LACP port status information.

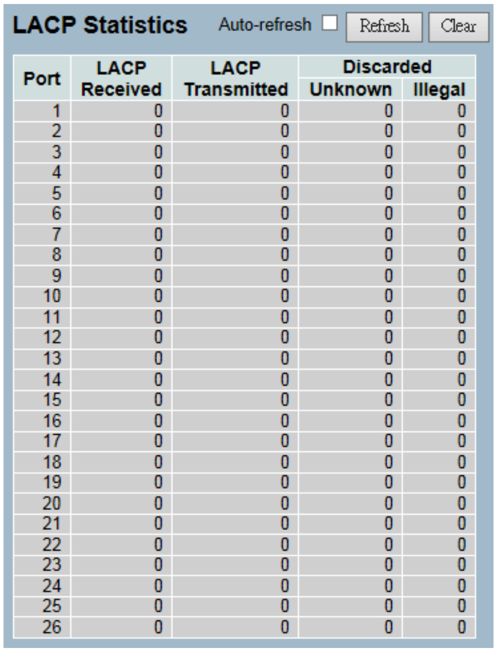
3-3.2.4 Port Statistics

After completing the LACP function set-up, this section provides a port statistics overview for all LACP instances.

Web Interface

To display the LACP port status in the web interface:

1. Click Configuration, LACP, and Port Statistics.
2. Click auto-refresh to automatically refresh the information.
3. Click refresh to manually refresh the information.



LACP Statistics

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0
21	0	0	0	0
22	0	0	0	0
23	0	0	0	0
24	0	0	0	0
25	0	0	0	0
26	0	0	0	0

Figure 3-3.2.4: The LACP Statistics

Parameter Description

Port: This is the switch port number.

LACP Received: This shows how many LACP frames have been received at each port.

LACP Transmitted: This shows how many LACP frames have been sent from each port.

Discarded: This shows how many unknown or illegal LACP frames have been discarded at each port.

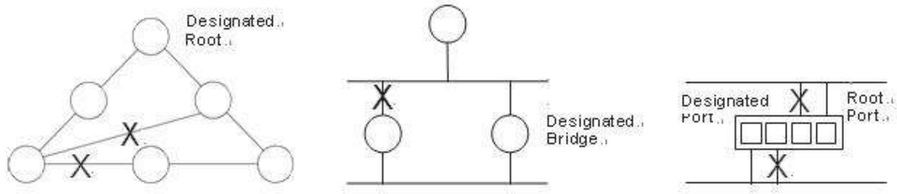
Auto-refresh: Click to automatically refresh the information.

Upper right icon (Refresh, Clear): Click manually refresh or clear the information.

3-4 Spanning Tree

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges, or routers. This allows the switch to interact with other bridging devices (STP-compliant switch, bridge, or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

STP - STP uses a distributed algorithm to select a bridging device (STP-compliant switch, bridge, or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device), which incurs the lowest path cost when forwarding a packet from that device to the root device. Then, it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated port to eliminate any possible network loops.



Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the root bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

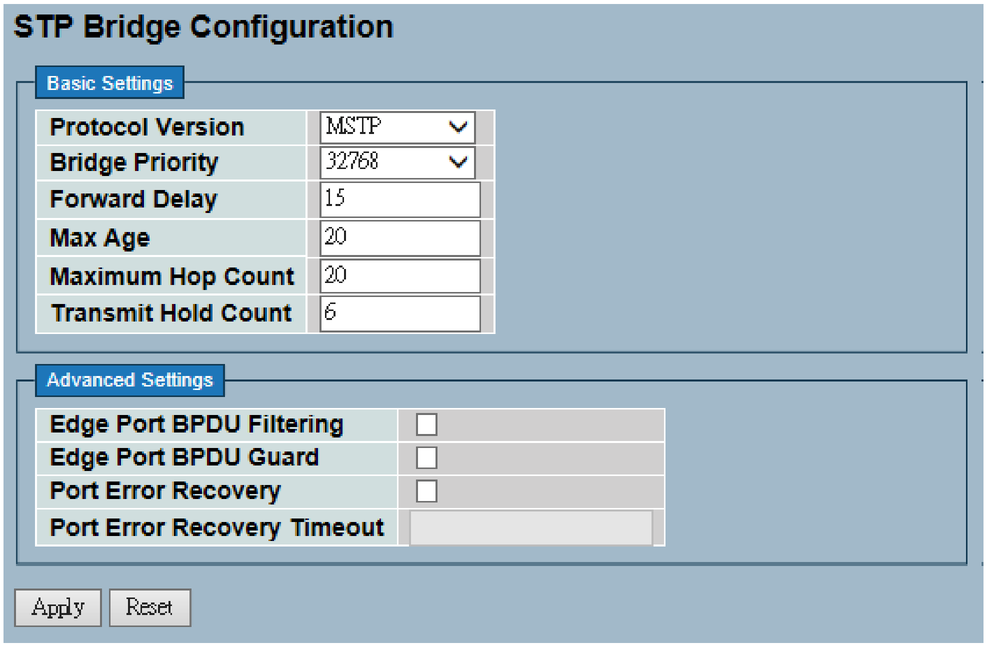
3-4.1 Bridge Settings

The section provides information on the configurations of the spanning tree bridge and STP system settings. It allows you to configure STP system settings are used by all STP bridge instance.

Web Interface

To configure the spanning tree bridge settings parameters in the web interface:

1. Click Configuration, Spanning Tree, and Bridge Settings.
2. Select the parameters and write the available parameter values under "Basic Settings."
3. Click to enable or disable the parameters and write down available parameter values under "Advanced Settings".
4. Click save.
5. Click reset to restore default settings.



STP Bridge Configuration

Basic Settings

Protocol Version	MSTP
Bridge Priority	32768
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings

Edge Port BPDU Filtering	□
Edge Port BPDU Guard	□
Port Error Recovery	□
Port Error Recovery Timeout	

Figure 3-4.1: The STP Bridge Configuration

Parameter Description

Basic Settings

Protocol Version: This is the STP protocol version setting. The valid values are STP, RSTP, and MSTP.

Bridge Priority: This 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.

Forward Delay: The delay used by STP bridges to transit root and designated ports to forwarding (used in STP compatible mode). The 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. The valid values are in the range 6 to 40 seconds, and the MaxAge must be <= (FwdDelay-1)*2.

Maximum Hop Count: This defines the initial value of remaining hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.

Transmit Hold Count: The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.

Advanced Settings

Edge Port BPDU Filtering: This controls whether a port explicitly configured as Edge will transmit and receive BPDUs.

Edge Port BPDU Guard: This controls 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: This controls whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.

Port Error Recovery Timeout: The time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

Buttons

- **Save** – Click to save changes.
- **Reset**- Click to restore default settings.

3-4.2 MSTI Mapping

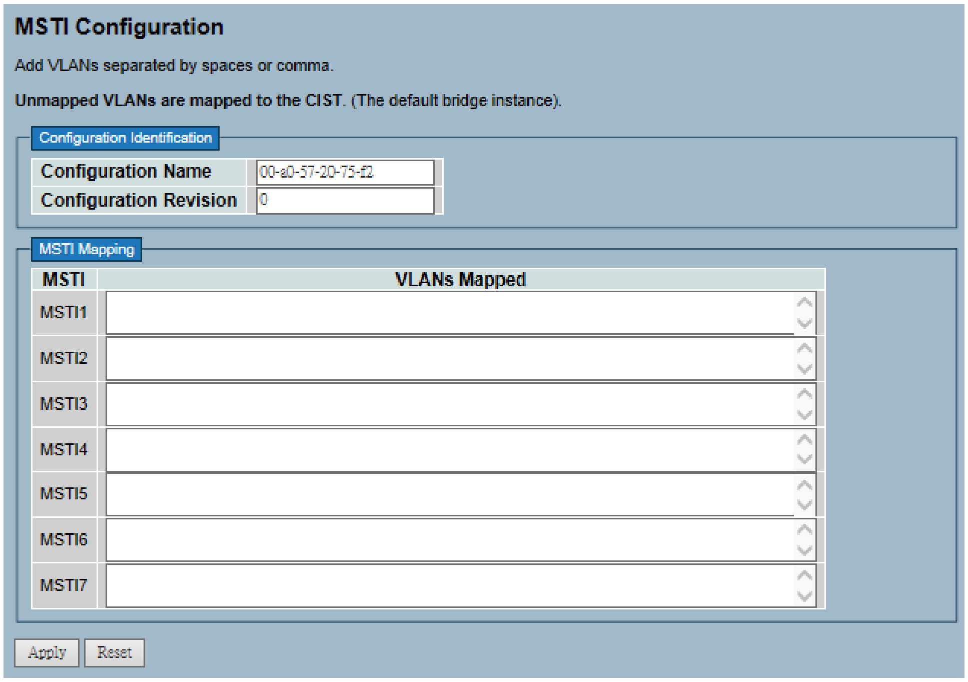
MSTI mapping is when you implement an Spanning Tree protocol on the switch that the bridge instance. The CIST is not available for explicit mapping because it will receive the VLANs not explicitly mapped. Due to that reason, you need to set the list of VLANs mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty (not having any VLANs mapped to it).

This section provides information on the current STP MSTI bridge instance priority configurations.

Web Interface

To configure the spanning tree MSTI mapping parameters in the web interface:

1. Click Configuration, Spanning Tree, and MSTI Mapping.
2. Specify the configuration identification parameters in the field.
3. Specify the VLANs Mapped blank field.
4. Click save.
5. Click reset to restore default settings.



MSTI Configuration

Add VLANs separated by spaces or comma.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Configuration Identification

Configuration Name	00-a0-57-20-75-f2
Configuration Revision	0

MSTI Mapping

MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

Figure 3-4.2: The MSTI Configuration

Parameter Description

Configuration Identification

Configuration Name: This is the name that identifies the VLAN to MSTI mapping. Bridges must share the name, revision (see below), and 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: This is the bridge instance. The CIST is not available for explicit mapping because it will receive the VLANs not explicitly mapped.

VLANs Mapped: The list of VLANs mapped to the MSTI. The VLANs 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 (e.g. not having any VLANs).

Buttons

- **Save** – Click to save changes.
- **Reset**- Click to restore default settings.

3-4.3 MSTI Priorities

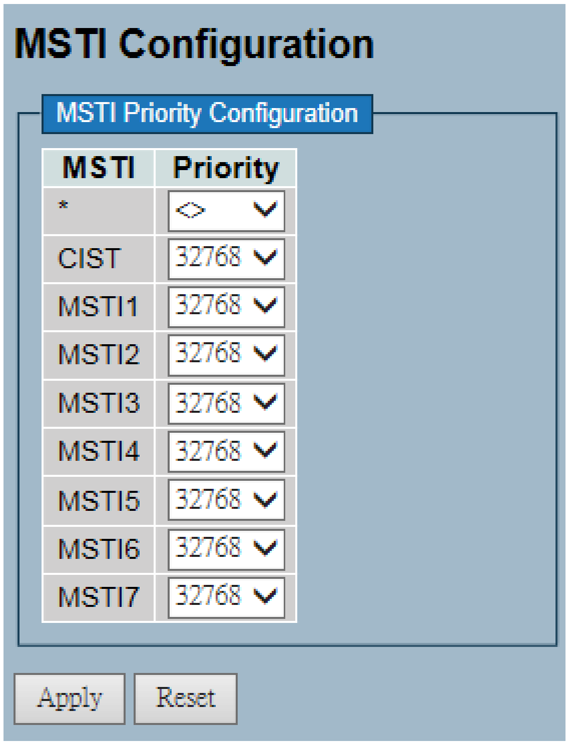
MSTI priorities is when you implement an spanning tree protocol on the switch that the bridge instance. The CIST is the default instance, which is always active. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch, forms a bridge identifier.

The section provides information on how to inspect and change the current STP MSTI bridge instance priority configurations.

Web Interface

To configure the spanning tree MSTI priorities parameters in the web interface:

1. Click Configuration, Spanning Tree, and MSTI Priorities.
2. Choose the priority. The maximum is 240. The default is 128.
3. Click save.
4. Click reset to restore default settings.



MSTI Configuration

MSTI Priority Configuration

MSTI	Priority
*	<>
CIST	32768
MSTI1	32768
MSTI2	32768
MSTI3	32768
MSTI4	32768
MSTI5	32768
MSTI6	32768
MSTI7	32768

Figure 3-4.3: The MSTI Configuration

Parameter Description

MSTI: This is the bridge instance. The CIST is the default instance, which is always active.

Priority: This 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.

Buttons

- **Save** – Click to save changes.
- **Reset**- Click to restore default settings.

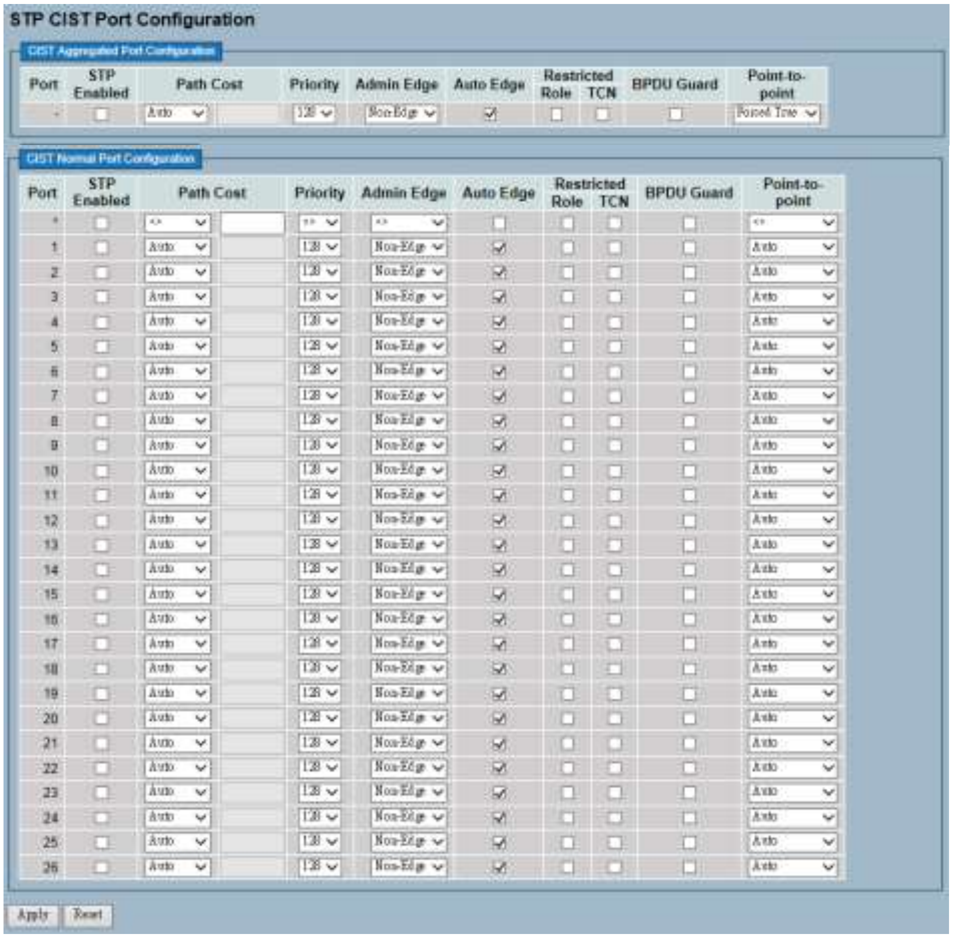
3-4.4 CIST Ports

When you implement an Spanning Tree protocol on the switch that the bridge instance. You need to configure the CIST Ports. The section describes it allows the user to inspect the to inspect the current STP CIST port configurations, and possibly change them as well.

Web Interface

To configure the spanning tree CIST ports parameters in the web interface:

1. Click Configuration, Spanning Tree, and then CIST Ports.
2. Scroll and evoke to set all parameters of CIST aggregated port configuration.
3. Click to enable or disable the STP.
4. Scrool and set all parameters of the CIST normal port configuration.
5. Click save.
6. Click to restore default settings.



STP CIST Port Configuration

CIST Aggregated Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
-	□	Auto		128	Non-Edge	☑	□	□	□	Forced True

CIST Normal Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
*	□	<>		<>	<>	□	□	□	□	<>
1	□	Auto		128	Non-Edge	☑	□	□	□	Auto
2	□	Auto		128	Non-Edge	☑	□	□	□	Auto
3	□	Auto		128	Non-Edge	☑	□	□	□	Auto
4	□	Auto		128	Non-Edge	☑	□	□	□	Auto
5	□	Auto		128	Non-Edge	☑	□	□	□	Auto
6	□	Auto		128	Non-Edge	☑	□	□	□	Auto
7	□	Auto		128	Non-Edge	☑	□	□	□	Auto
8	□	Auto		128	Non-Edge	☑	□	□	□	Auto
9	□	Auto		128	Non-Edge	☑	□	□	□	Auto
10	□	Auto		128	Non-Edge	☑	□	□	□	Auto
11	□	Auto		128	Non-Edge	☑	□	□	□	Auto
12	□	Auto		128	Non-Edge	☑	□	□	□	Auto
13	□	Auto		128	Non-Edge	☑	□	□	□	Auto
14	□	Auto		128	Non-Edge	☑	□	□	□	Auto
15	□	Auto		128	Non-Edge	☑	□	□	□	Auto
16	□	Auto		128	Non-Edge	☑	□	□	□	Auto
17	□	Auto		128	Non-Edge	☑	□	□	□	Auto
18	□	Auto		128	Non-Edge	☑	□	□	□	Auto
19	□	Auto		128	Non-Edge	☑	□	□	□	Auto
20	□	Auto		128	Non-Edge	☑	□	□	□	Auto
21	□	Auto		128	Non-Edge	☑	□	□	□	Auto
22	□	Auto		128	Non-Edge	☑	□	□	□	Auto
23	□	Auto		128	Non-Edge	☑	□	□	□	Auto
24	□	Auto		128	Non-Edge	☑	□	□	□	Auto
25	□	Auto		128	Non-Edge	☑	□	□	□	Auto
26	□	Auto		128	Non-Edge	☑	□	□	□	Auto

Figure 3-4.4: The STP CIST Port Configuration

Parameter Description

Port: This is the switch port number of the logical STP port.

STP Enabled: This controls whether STP is enabled on this switch port.

Path Cost: This 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. By using the specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.

Priority: This controls the port priority. This can be used to control priority of ports having identical port cost (see above).

operEdge (state flag): Operational flag describes whether the port is connecting directly to edge devices (no Bridges attached). Transition to the forwarding state is faster for edge ports (having operEdge true) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as edge in Monitor->Spanning Tree -> STP Detailed Bridge Status.

AdminEdge: This controls whether the operEdge flag should start as set or cleared. The initial operEdge state when a port is initialized.

AutoEdge: This controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.

Restricted Role: If enabled, it causes the port not to be selected as root port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an alternate port after the root port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology because those bridges are not under the full control of the administrator. This feature is also known as root guard.

Restricted TCN: If enabled, it causes the port not to propagate received topology change notifications and topology changes to other ports. If set, it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

BPDU Guard: If enabled, it 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 an error-disabled state due to this setting is subject to the bridge port error recovery setting.

Point to Point: This controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced to either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

Buttons

- **Save** – Click to save changes.
- **Reset**- Click to restore default settings.

3-4.5 MSTI Ports

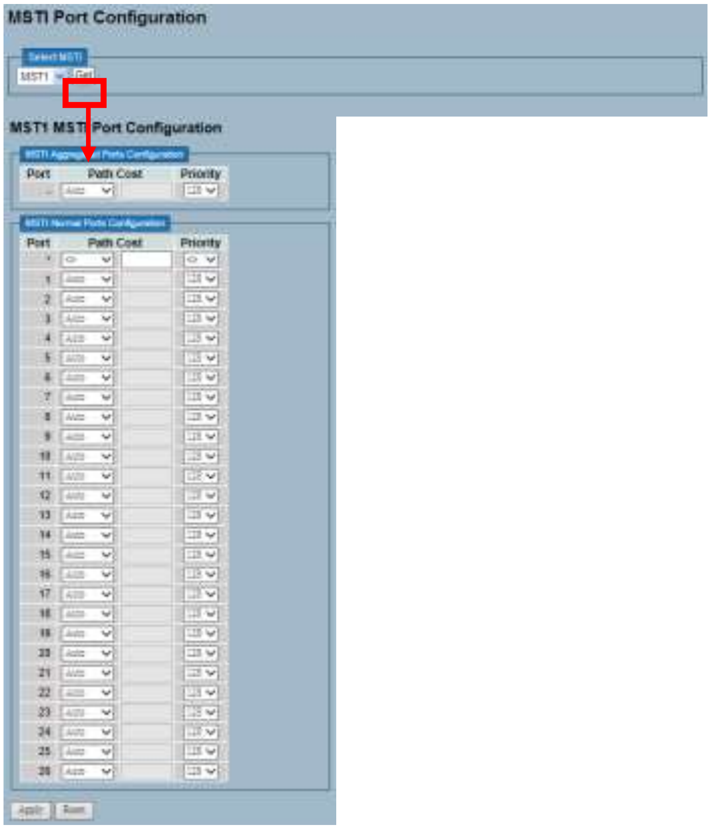
The section provides inspection information on the current STP MSTI port configurations.

An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options. It contains MSTI port settings for physical and aggregated ports.

Web Interface

To configure the spanning tree MSTI port configuration parameters in the web interface:

1. Click Configuration, Spanning Tree, and MSTI Ports.
2. Select MST1 or other for the MSTI port.
3. Click "Get" to set the detail parameters of the MSTI Ports.
4. Scroll to set all parameters of the MSTI port configuration.
5. Click save.
6. Click reset to restore default settings.



MSTI Port Configuration

Select MSTI

MSTI Get

MST1 MSTI Port Configuration

MSTI Aggregated Ports Configuration

Port	Path Cost		Priority
-	Auto		128

MSTI Normal Ports Configuration

Port	Path Cost		Priority
*	<>		<>
1	Auto		128
2	Auto		128
3	Auto		128
4	Auto		128
5	Auto		128
6	Auto		128
7	Auto		128
8	Auto		128
9	Auto		128
10	Auto		128
11	Auto		128
12	Auto		128
13	Auto		128
14	Auto		128
15	Auto		128
16	Auto		128
17	Auto		128
18	Auto		128
19	Auto		128
20	Auto		128
21	Auto		128
22	Auto		128
23	Auto		128
24	Auto		128
25	Auto		128
26	Auto		128

Figure 3-4.5: The MSTI Port Configuration

Parameter Description

Port: The switch port number of the corresponding STP CIST (and MSTI) port.

Path Cost: This 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. By using the specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. The valid values are in the range 1 to 200000000.

Priority: This controls the port priority. This can be used to control priority of ports having identical port cost (see above).

Buttons

- **Save** – Click to save changes.
- **Reset**- Click to restore default settings.

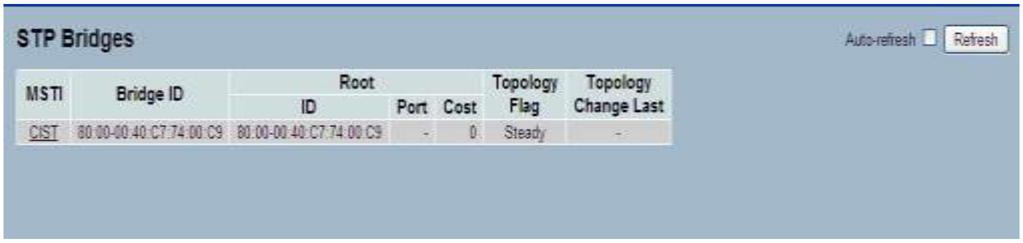
3-4.6 Bridge Status

After completing the MSTI port configurations, the switch is able to display the bridge status. This section provides a status overview of all STP bridge instances. The displayed table contains a row for each STP bridge instance.

Web Interface

To display the STP Bridges status in the web interface:

1. Click Configuration, Spanning Tree, and STP Bridges.
2. Click auto-refresh to automatically refresh the information.
3. Click refresh to manually refresh the STP Bridges.



MSTI	Bridge ID	Root			Topology	Topology
		ID	Port	Cost	Flag	Change Last
CIST	80:00-00:40:C7:74:00:C9	80:00-00:40:C7:74:00:C9	-	0	Steady	-

Figure 3-4.6: The STP Bridges Status

Parameter Description

MSTI: This is the bridge instance. This is also a link to the STP detailed bridge status.

Bridge ID: The bridge ID of this bridge instance.

Root ID: The bridge ID of the currently elected root bridge.

Root Port: The switch port currently assigned the root port role.

Root Cost: This is the 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: This is the current state of the topology change flag of this bridge instance.

Topology Change Last: This is the time since last topology change occurred.

Auto-Refresh: Click to automatically refresh the information.

Upper Right Icon (Refresh): Click to manually refresh the STP Bridges status information.

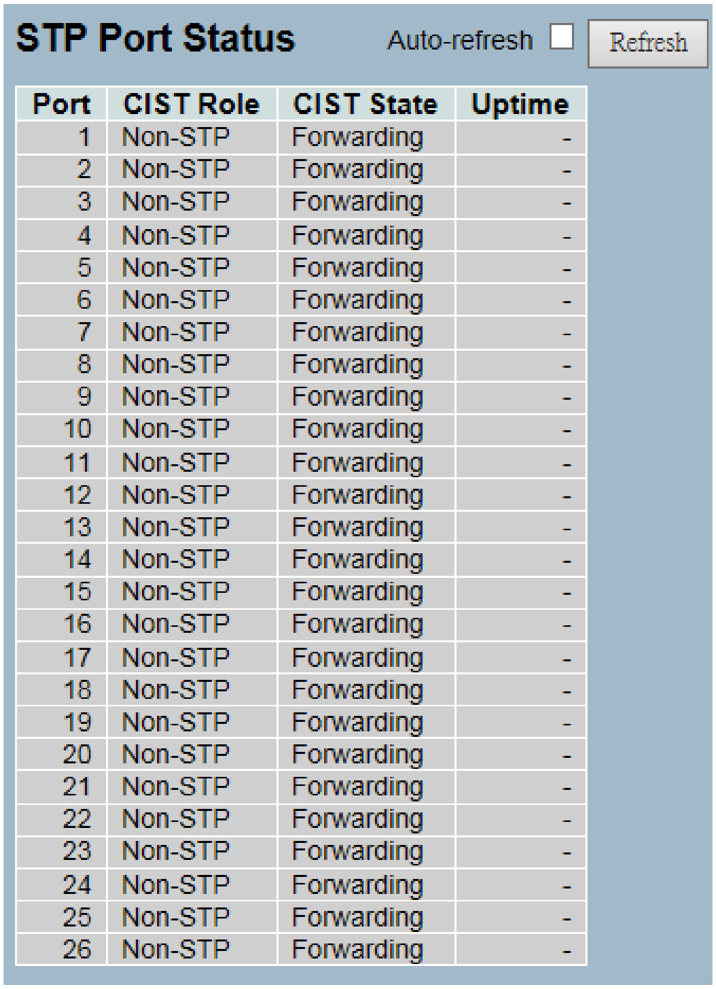
3-4.7 Port Status

After completing the STP configuration, the switch is able to display the STP port status. This section provides information on how to display the STP CIST port status for physical ports.

Web Interface

To display the STP port status in the web interface:

1. Click Configuration, Spanning Tree, and STP Port Status.
2. Click auto-refresh to automatically refresh the STP bridges.
3. Click refresh to manually refresh the STP bridges.



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	-
8	Non-STP	Forwarding	-
9	Non-STP	Forwarding	-
10	Non-STP	Forwarding	-
11	Non-STP	Forwarding	-
12	Non-STP	Forwarding	-
13	Non-STP	Forwarding	-
14	Non-STP	Forwarding	-
15	Non-STP	Forwarding	-
16	Non-STP	Forwarding	-
17	Non-STP	Forwarding	-
18	Non-STP	Forwarding	-
19	Non-STP	Forwarding	-
20	Non-STP	Forwarding	-
21	Non-STP	Forwarding	-
22	Non-STP	Forwarding	-
23	Non-STP	Forwarding	-
24	Non-STP	Forwarding	-
25	Non-STP	Forwarding	-
26	Non-STP	Forwarding	-

Figure 3-4.7: The STP Port Status

Parameter Description	**Port:** This is the switch port number of the logical STP port. **CIST Role:** This is the current STP port role of the CIST port. The port role can be one of the following values: alternate port, backup port, rootport, or designated port disabled. **CIST State:** This is the current STP port state of the CIST port. The port state can be one of the following values: blocking, learning, or forwarding. **Uptime:** This is the time since the bridge port was last initialized. **Auto-refresh:** Click to automatically refresh the information. **Upper Right Icon (Refresh):** Click to manually refresh the information.

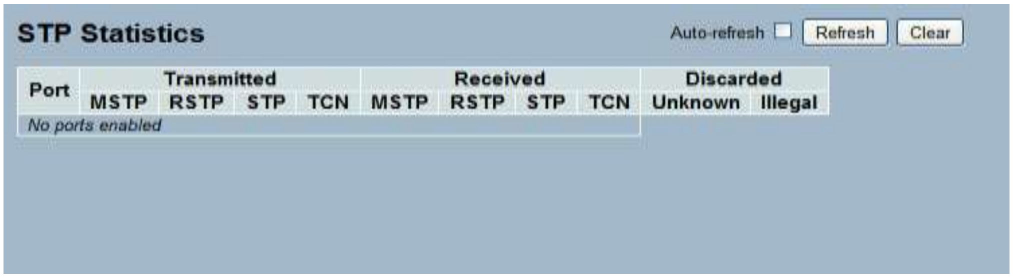
3-4.8 Port Statistics

After completing the STP configuration, the switch is able to display the STP statistics. This section provides information on how to display the STP statistics detail counters of bridge ports.

Web Interface

To display the STP port status in the web interface:

1. Click Configuration, Spanning Tree, and Port Statistics.
2. Click auto-refresh to automatically refresh the STP bridges.
3. Click refresh to manually refresh the STP bridges.



STP Statistics

Auto-refresh □ Refresh Clear

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

Figure 3-4.8: The STP Statistics

Parameter Description

Port: This is the switch port number of the logical STP port.

MSTP: This is the number of MSTP configuration BPDU's received/transmitted on the port.

RSTP: This is the number of RSTP configuration BPDU's received/transmitted on the port.

STP: This is the number of legacy STP configuration BPDU's received/transmitted on the port.

TCN: This is the number of (legacy) topology change notification BPDU's received/transmitted on the port.

Discarded Unknown: This is 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.

Auto-refresh: Click to automatically refresh the information.

Upper right icon (Refresh, Clear): Click to manually clear or refresh the information.

3-5 IGMP Snooping

IGMP snooping is used to establish multicast groups in order to forward the multicast packet to the member ports. It’s also used to avoid wasting bandwidth while IP multicast packets are running over the network. If a switch does not support IGMP or IGMP snooping and cannot tell the multicast packet apart from the broadcast packet, it treats everything as broadcast packets. Without IGMP snooping, the multicast packet forwarding function is nothing different from the broadcast packet.

A switch that supports IGMP snooping (with functions such as query, report and leave, and packet exchanged between IP multicast router/switch and IP multicast host) can update the information of the multicast table when a member (port) joins or leaves an IP multicast destination address. Once a switch receives an IP multicast packet, it will forward the packet to the members who joined in a specified IP multicast group before.

The packets will be discarded by the IGMP snooping if the user transmits multicast packets to the multicast group that had not been built up in advance. IGMP mode enables the switch to issue IGMP function that you enable IGMP proxy or snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

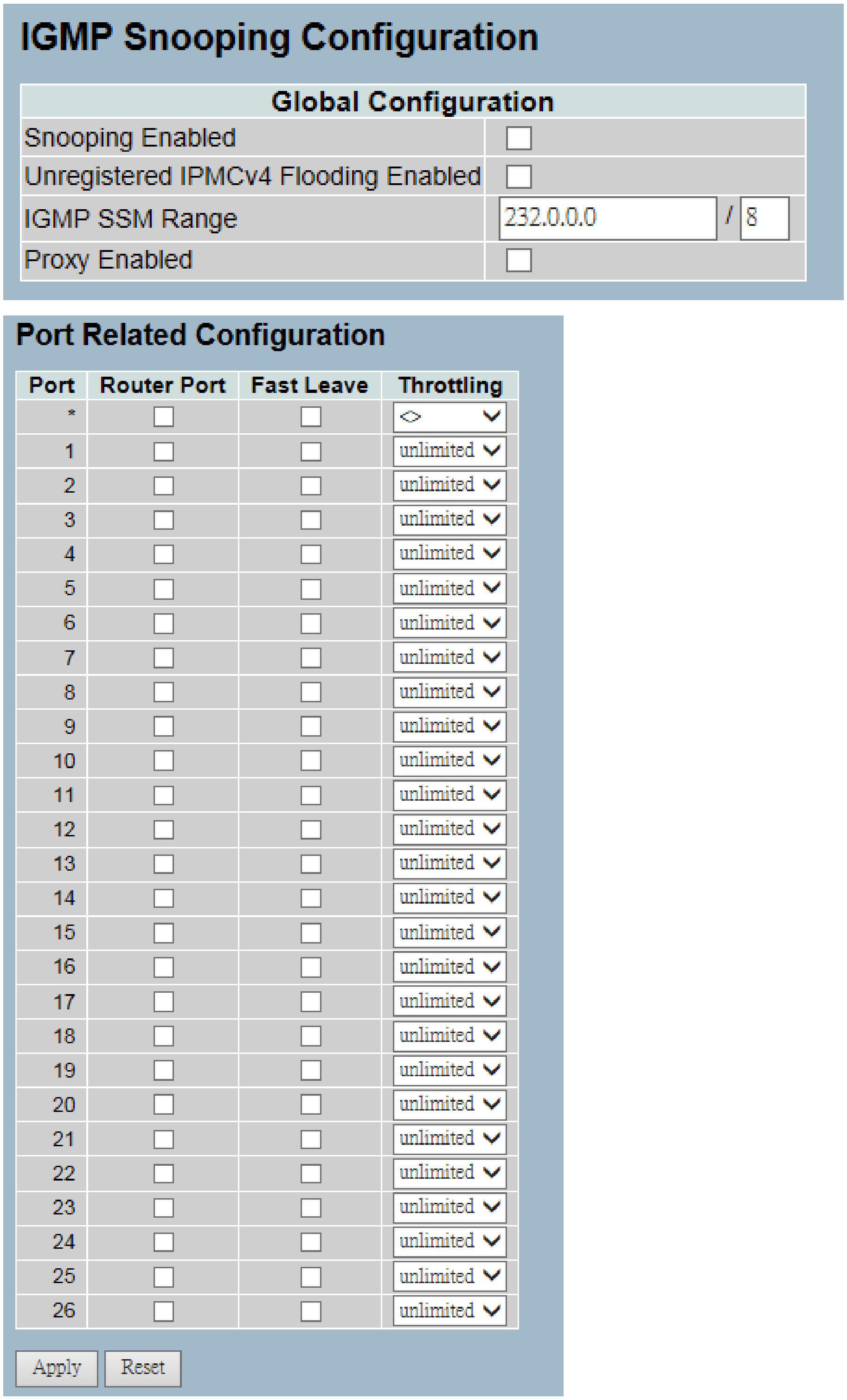
3-5.1 Basic Configuration

The section provides information on how to set the basic IGMP snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

Web Interface

To configure the IGMP snooping parameters in the web interface:

1. Click Configuration, IGMP Snooping, and Basic Configuration.
2. Click to select enable or disable for global configuration.
3. Select which port to become a router port, or enable/disable the fast leave function.
4. Set the throtting parameter.
5. Click save.
6. Click reset to restore default settings.



IGMP Snooping Configuration

Global Configuration	
Snooping Enabled	□
Unregistered IPMCv4 Flooding Enabled	□
IGMP SSM Range	232.0.0.0 / 8
Proxy Enabled	□

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	□	□	<>
1	□	□	unlimited
2	□	□	unlimited
3	□	□	unlimited
4	□	□	unlimited
5	□	□	unlimited
6	□	□	unlimited
7	□	□	unlimited
8	□	□	unlimited
9	□	□	unlimited
10	□	□	unlimited
11	□	□	unlimited
12	□	□	unlimited
13	□	□	unlimited
14	□	□	unlimited
15	□	□	unlimited
16	□	□	unlimited
17	□	□	unlimited
18	□	□	unlimited
19	□	□	unlimited
20	□	□	unlimited
21	□	□	unlimited
22	□	□	unlimited
23	□	□	unlimited
24	□	□	unlimited
25	□	□	unlimited
26	□	□	unlimited

Figure 3-5.1: The IGMP Snooping Configuration

Parameter Description

Snooping Enabled: This enables the global IGMP snooping.

Unregistered IPMCv4 Flooding Enabled: This enables unregistered IPMCv4 traffic flooding.

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. Format: (IP address/ sub mask)

Proxy Enabled: This enables IGMP proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Port: It shows the physical port index of switch.

Router Port: This specifies 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: This enables the fast leave on the port.

Throttling: This enables to limit the number of multicast groups to which a switch port can belong.

Buttons

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

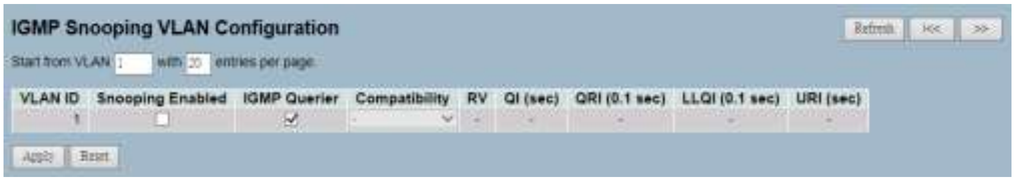
3-5.2 VLAN Configuration

The section provides information on the VLAN configuration setting process integrated with IGMP snooping function. Each setting page shows up to 99 entries from the VLAN table. The default is 20 and can be selected through the "Entries Per Page" input field. When you first visit this page, 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 button will update the displayed table starting from that or the next closest VLAN table match.

Web Interface

To configure the IGMP snooping VLAN configuration in the web interface:

1. Click Configuration, IGMP Snooping, VLAN Configuration.
2. Click to select enable or disable snooping.
3. Click IGMP Querier and specify the parameters in the blank field.
4. Click the refresh to update the data, or click << or >> to display previous or next entry.
5. Click save.
6. Click reset to restore default settings.



IGMP Snooping VLAN Configuration

Start from VLAN 1 with 20 entries per page.

VLAN ID	Snooping Enabled	IGMP Querier	Compatibility	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
1	□	☑	-	-	-	-	-	-

Figure 3-5.2: The IGMP Snooping VLAN Configuration.

Parameter Description

VLAN ID: This displays the VLAN ID of the entry.

Snooping Enabled: This enables the Per-VLAN IGMP snooping. Only up to 32 VLANs can be selected.

IGMP Querier: A router sends IGMP query messages onto a particular link. This router is called the querier. Enable the IGMP querier in the VLAN.

Compatibility: Compatibility is maintained by hosts and routers that take 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, and Forced IGMPv3. The default compatibility value is IGMP-Auto.

Rv: This is robustness variable. The robustness variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255. The default robustness variable value is 2.

QI: This is query interval. The query interval is the interval between general queries sent by the querier. The allowed range is 1 to 31744 seconds. The default query interval is 125 seconds.

QRI: This is query response interval. The max response time used to calculate the Max Resp Code inserted into the periodic general queries. The allowed range is 0 to 31744 in tenths of seconds. The default query response interval is 100 in tenths of seconds (10 seconds).

LLQI (LMQI for IGMP): This is 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. The default last member query interval is 10 in tenths of seconds (1 second).

URI: This is 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. The default unsolicited report interval is 1 second. .

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

Upper right icon (Refresh, |<<, >>): Click refresh to manually update the displayed table. Click “|<<” to update the table, starting from the first entry in the VLAN table. Click “>>” to update the table, starting with the entry after the last entry currently displayed.

3-5.3 Port Group Filtering

The section provides information on seting up the IGMP port group filtering. With the IGMP filtering feature, an user can exert this type of control. In some network application environments (e.g. the metropolitan or multiple-dwelling unit (MDU) installations), an user might want to control the multicast groups on a switch port. It allows the user to control the distribution of multicast services, such as IP/TV, based on some type of subscription or service plan.

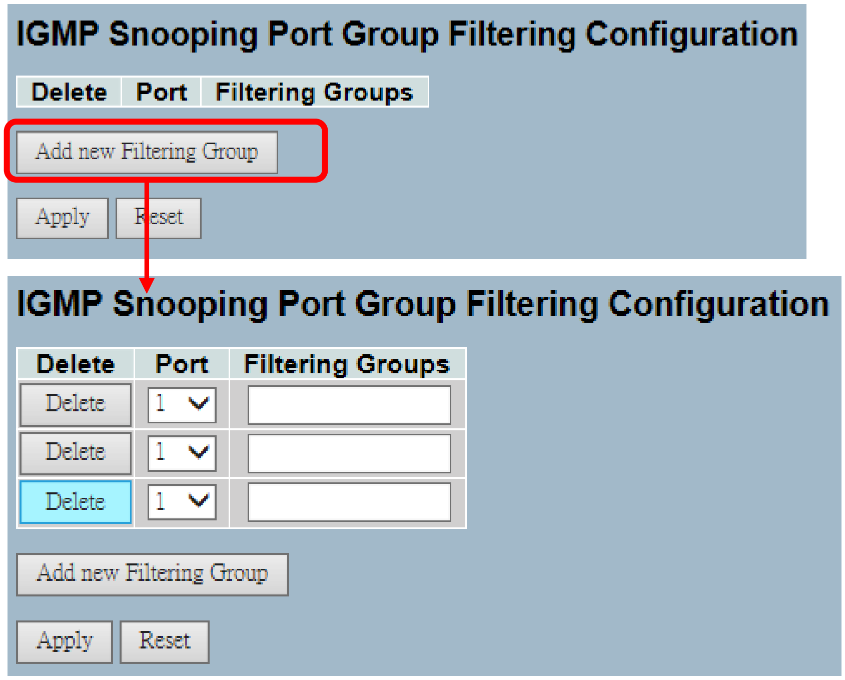
You can filter multicast joins on a per-port basis by configuring the IP multicast profiles and associating them with individual switch ports. An IGMP profile can contain one or more multicast groups and specifies whether access to the group is permitted or denied. If an IGMP profile denies access to a multicast group, the IGMP join report requesting the stream of IP multicast traffic is dropped and the port is not allowed to receive IP multicast traffic from that group. If the filtering action permits access to the multicast group, the IGMP report from the port is forwarded for normal processing.

IGMP filtering controls only IGMP membership join reports and has no relationship to the function that directs the forwarding of IP multicast traffic.

Web Interface

To configure the IGMP snooping port group configuration in the web interface:

1. Click Configuration, IGMP Snooping, and Port Group Filtering.
2. Click add new filtering group.
3. Click which the port to enable the port group filtering on and specify the filtering groups in the blank field.
4. Click save.
5. Click reset to restore default settings.


IGMP Snooping Port Group Filtering Configuration
Delete
Port
Filtering Groups
Add new Filtering Group
Apply
Reset
IGMP Snooping Port Group Filtering Configuration

Delete	Port	Filtering Groups
Delete	1	
Delete	1	
Delete	1	

Add new Filtering Group
Apply
Reset

Figure 3-5.3: The IGMP Snooping Port Group Filtering Configuration

Parameter Description

Delete: Click delete to remove the entry.

Port: Click which port to enable the igmp snooping port group filtering function on.

Filtering Groups: This is the IP multicast group that will be filtered.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

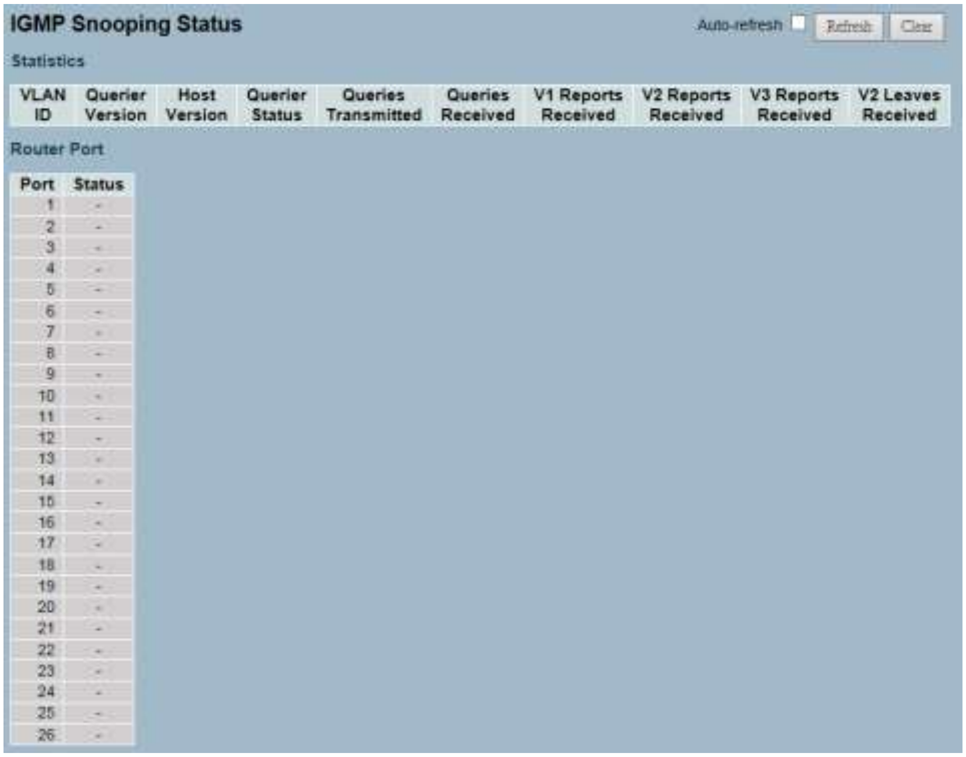
3-5.4 Status

After completing the IGMP snooping configuration, the switch is able to display the IGMP snooping status.

Web Interface

To display the IGMP snooping status in the web interface:

1. Click Configuration, IGMP Snooping, and Status.
2. Click auto-refresh to automatically refresh the IGMP snooping status.
3. Click refresh to manually refresh the IGMP snooping status.
4. Click clear to clear the IGMP snooping status.



IGMP Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-
13	-
14	-
15	-
16	-
17	-
18	-
19	-
20	-
21	-
22	-
23	-
24	-
25	-
26	-

Figure 3-5.4: The IGMP Snooping Status

Parameter Description

VLAN ID: This is the VLAN ID of the entry.

Querier Version: This is the working querier version currently.

Host Version: This is the working host version currently.

Querier Status: This shows the querier status is "ACTIVE" or "IDLE".

Queries Transmitted: This is the number of transmitted queries.

Queries Received: This is the number of received queries.

V1 Reports Received: This is the number of received V1 reports.

V2 Reports Received: This is the number of received V2 reports.

V3 Reports Received: This is the number of received V3 reports.

V2 Leaves Received: This is the number of received V2 leaves.

Auto-refresh: Click to automatically refresh the information.

Upper right icon (Refresh, clear): Click to manually refresh or clear the status.

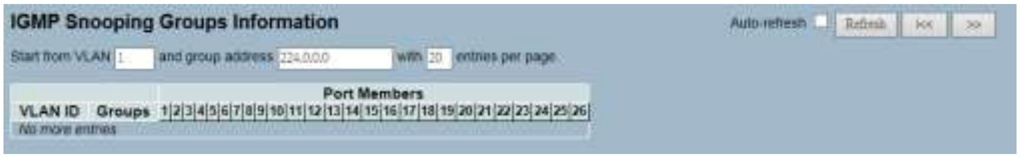
3-5.5 Group Information

After completing the IGMP snooping function set-up, the switch is able to display the IGMP snooping group information. The IGMP group table is sorted first by VLAN ID, and then by group. The table 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. Use the button to start over.

Web Interface

To display the IGMP snooping group information in the web interface:

1. Click Configuration, IGMP Snooping, and Group Information.
2. Click auto-refresh to automatically refresh an entry.
3. Click refresh to manually refresh an entry of the IGMP snooping groups information.
4. Click “<< or >>” to move to the previous or next entry.



IGMP Snooping Groups Information

Start from VLAN 1 and group address 224.0.0.0 with 20 entries per page

		Port Members																								
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
No more entries																											

Figure 3-5.5: The IGMP Snooping Groups Information

Parameter Descripton

<u>**Navigating the IGMP Group Table**</u>

The "Start from VLAN" and "group" input fields allow the user to select the starting point in the IGMP group table. The table 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.

<u>**IGMP Group Table Columns**</u>

VLAN ID: This is VLAN ID of the group.

Groups: This is group address of the group displayed.

Port Members: This is ports under this group.

Auto-Refresh: If this option is selected, the device will automatically refresh the log.

Upper Right Icon (Refresh, <<, >>): Click to manually refresh the entries, or move to the previous or next page.

3-5.6 IPv4 SSM Information

Source Specific Multicast (SSM) is a datagram delivery model that best supports one-to-many applications, also known as, broadcast applications. SSM is a core network technology of IP multicast targeted for audio and video broadcast application environments.

For the SSM delivery mode, an IP multicast receiver host must use IGMP Version 3 (IGMPv3) to subscribe to channel (S, G). By subscribing to this channel, the receiver host indicates that it wants to receive IP multicast traffic sent by source host S to group G. The network will deliver IP multicast packets from source host S to group G to all hosts in the network that have subscribed to the channel (S, G).

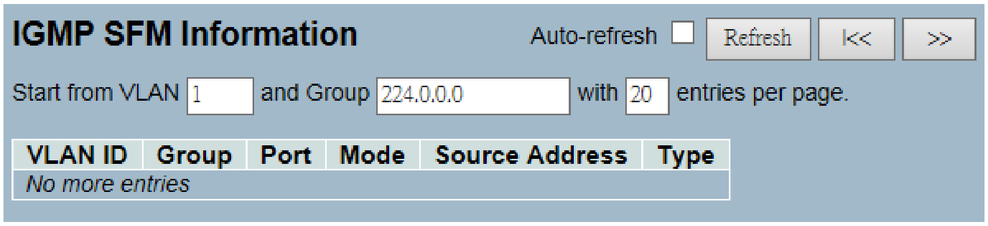
SSM does not require group address allocation within the network, only within each source host. Different applications running on the same source host must use different SSM groups. Different applications running on different source hosts can arbitrarily reuse SSM group addresses without causing any excess traffic on the network.

Address in the range 232.0.0.0/8 (232.0.0.0 to 232.255.255.255) are reserved for SSM by IANA. In the switch, you can configure SSM for arbitrary IP multicast addresses also.

Web Interface

To display the IGMPv3 IPv4 SSM information in the web interface:

1. Click Configuration, IGMP Snooping, and IPv4 SSM Information.
2. Click auto-refresh to automatically refresh the entry.
3. Click refresh to manually refresh the entry.
4. Click "<< or >>" to move to the previous or next entry.



IGMP SFM Information

Start from VLAN 1 and Group 224.0.0.0 with 20 entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type
No more entries					

Figure 3-6.6: The IGMPv3 IPv4 SSM Information

Parameter Description

Navigating the IGMPv3 Information Table

Each page shows up to 99 entries from the IGMPv3 SSM (Source Specific Multicast) information table. The default is 20 and can selected through the "entries per page" input field. When you first visit the page, it will show the first 20 entries from the beginning of the IGMPv3 information table.

The "Start from VLAN", and "Group" input fields allow the user to select the starting point in the IGMPv3 information table. Clicking "Refresh" button will update the displayed table starting from that or the closest next IGMPv3 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.

IGMPv3 Information Table Columns

VLAN ID: This is VLAN ID of the group.

Group: This is group address of the group displayed.

Port: This is switch port number.

Mode: This indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either "Include" or "Exclude".

Source Address: This is IP address of the source. Currently, the system limits the total number of IP source addresses for filtering to be 128.

Type: This indicates the type. It can be either "Allow" or "Deny".

Auto-refresh: If this option is selected, the device will automatically refresh the log.

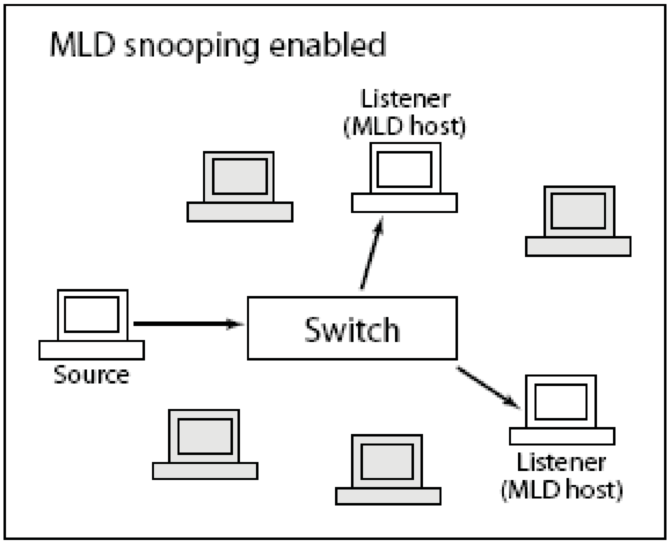
Upper right icon (Refresh, <<, >>): Click to manually refresh the entry, or move to the next or previous page.

3-6 MLD Snooping

A network node that acts as a source of IPv6 multicast traffic is only an indirect participant in MLD snooping. It just provides multicast traffic and MLD doesn't interact with it. Note: However, in an application like desktop conferencing, a network node may act as both a source and an MLD host; but MLD interacts with that node only in its role as an MLD host.

A source node creates multicast traffic by sending packets to a multicast address. In IPv6, addresses with the first eight bits set ("FF" as the first two characters of the address) are multicast addresses, and any node that listens to such an address will receive the traffic sent to that address. Application software running on the source and destination systems cooperates to determine what multicast address to use. Note: This is a function of the application software, not of MLD.

When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports on the VLAN that have no MLD hosts.



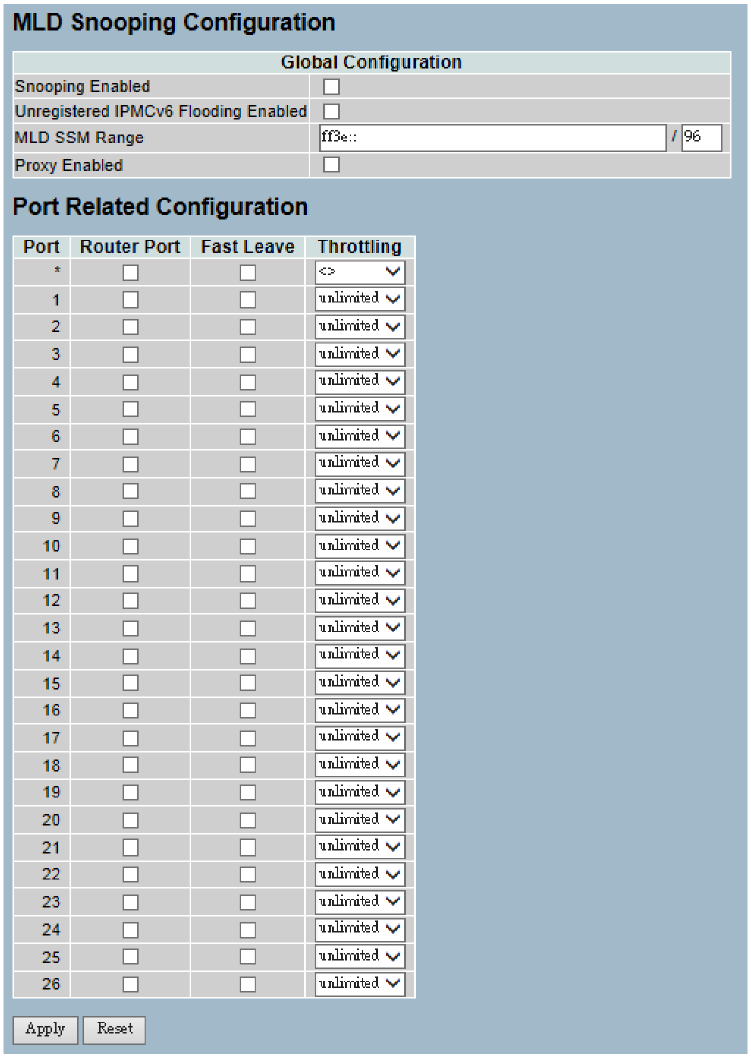
3-6.1 Basic Configuration

The section provides configurations to MLD snooping.

Web Interface

To configure the MLD snooping configuration in the web interface:

1. Click Configuration, MLD Snooping, and Basic Configuration.
2. Click to enable or disable the global configuration parameters.
3. Evoke the port to join the router port and fast leave.
4. Select between unlimited or 1 to 10 for the throtting mode.
5. Click save.
6. Click reset to restore default settings.



MLD Snooping Configuration

Global Configuration	
Snooping Enabled	☐
Unregistered IPMCv6 Flooding Enabled	☐
MLD SSM Range	ff3e:: / 96
Proxy Enabled	☐

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	☐	☐	<>
1	☐	☐	unlimited
2	☐	☐	unlimited
3	☐	☐	unlimited
4	☐	☐	unlimited
5	☐	☐	unlimited
6	☐	☐	unlimited
7	☐	☐	unlimited
8	☐	☐	unlimited
9	☐	☐	unlimited
10	☐	☐	unlimited
11	☐	☐	unlimited
12	☐	☐	unlimited
13	☐	☐	unlimited
14	☐	☐	unlimited
15	☐	☐	unlimited
16	☐	☐	unlimited
17	☐	☐	unlimited
18	☐	☐	unlimited
19	☐	☐	unlimited
20	☐	☐	unlimited
21	☐	☐	unlimited
22	☐	☐	unlimited
23	☐	☐	unlimited
24	☐	☐	unlimited
25	☐	☐	unlimited
26	☐	☐	unlimited

Figure 3-6.1: The MLD Snooping Basic Configuration

Parameter Description

Snooping Enabled : This enables the global MLD snooping.

Unregistered IPMCv6 Flooding Enabled: This enables unregistered IPMCv6 traffic flooding. Please note that disabling unregistered IPMCv6 traffic flooding may lead to failure of neighbor discovery.

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 (using IPv6 Address) range.

Proxy Enabled: This enables MLD proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Port: This is the port index you choose to enable or disable the MLD snooping function on.

Fast Leave: Click to enable the fast leave on the port.

Router Port: This specifies 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.

Throttling: This enables to limit the number of multicast groups to which a switch port can belong.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

3-6.2 VLAN Configuration

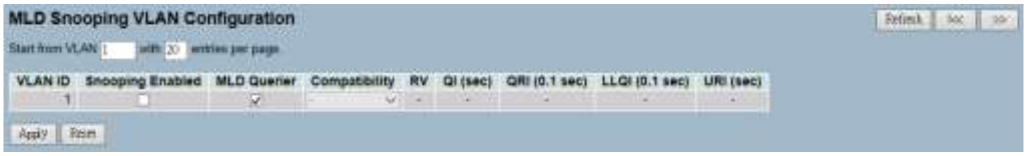
When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports on the VLAN that have no MLD hosts.

The table 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.

Web Interface

To configure the MLD snooping VLAN configuration in the web interface:

1. Click Configuration, MLD Snooping, and VLAN Configuration.
2. Specify the VLAN ID with entries per page.
3. Click refresh to manually refresh an entry of the MLD snooping VLAN configuration information.
4. Click “<< or >>” to move to the previous or next entry.



MLD Snooping VLAN Configuration

Start from VLAN 1 with 20 entries per page

VLAN ID	Snooping Enabled	MLD Querier	Compatibility	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
1	□	☑	-	-	-	-	-	-

Figure 3-7.2: The MLD Snooping VLAN Configuration.

VLAN ID: This is the VLAN ID of the entry.

Snooping Enabled: This enables the per-VLAN MLD snooping. Only up to 32 VLANs can be selected.

MLD Querier: A router sends MLD query messages onto a particular link. This router is called the querier. Enable the MLD querier in the VLAN.

Compatibility: Compatibility is maintained by hosts and routers. They take appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The allowed selection is MLD-Auto, Forced MLDv1, or Forced MLDv2. The default compatibility value is MLD-Auto.

Rv: This is robustness variable. The robustness variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255. The default robustness variable value is 2.

QI: This is the query interval. The query interval is the interval between general queries sent by the querier. The allowed range is 1 to 31744 seconds. The default query interval is 125 seconds.

QRI: This is the 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. The default query response interval is 100 in tenths of seconds (10 seconds).

LLQI (LMQI for IGMP): This is the 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. The default last listener query interval is 10 in tenths of seconds (1 second).

URI: This is the 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. The default unsolicited report interval is 1 second.

Upper right icon (Refresh, <<, >>): Click to manufally refresh the status, or move to the next or previous page.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

3-6.3 Port Group Filtering

The section provides information on setting up the port group filtering in the MLD snooping function. You can add new filtering group and safety policy on the UI.

Web Interface

To configure the MLD snooping port group configuration in the web interface:

1. Click Configuration, MLD Snooping, and Port Group Filtering Configuration.
2. Click add new filtering group.
3. Specify the filtering groups.
4. Click save.
5. Click reset to restore default settings.

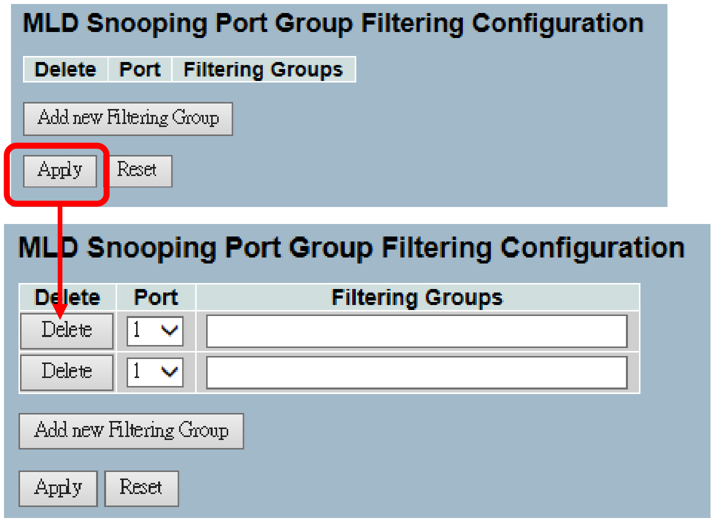


Figure 3-7.3: The MLD Snooping Port Group Filtering Configuration

Parameter Description

Delete: Click delete to remove the entry.

Port: This is the logical port for the settings. Select to enable the port to join filtering group.

Filtering Groups: This is the IP multicast group that will be filtered.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

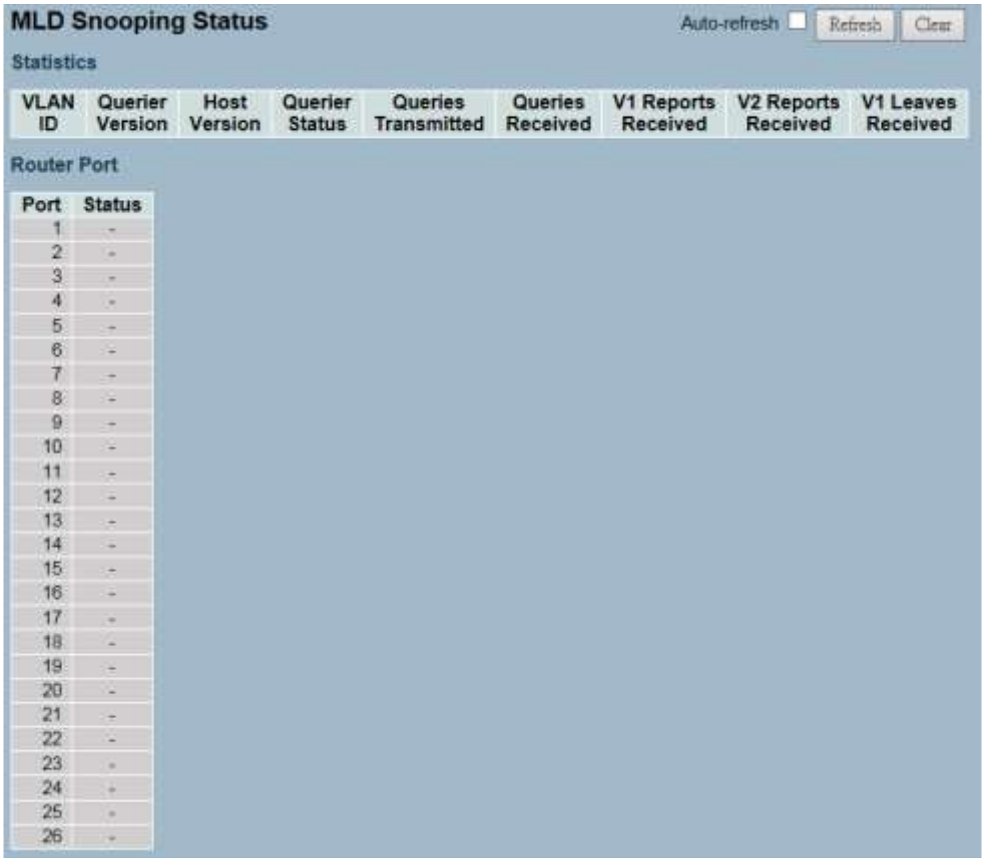
3-6.4 Status

The section provides information on the MLD snooping, its status and other detailed information.

Web Interface

To display the MLD snooping status in the web interface:

1. Click Configuration, MLD Snooping, and Status.
2. Click auto-refresh to automatically refresh the information.
3. Click refresh to manually refresh an entry.
4. Click clear to remove the MLD snooping status..



MLD Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V1 Leaves Received

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-
13	-
14	-
15	-
16	-
17	-
18	-
19	-
20	-
21	-
22	-
23	-
24	-
25	-
26	-

Figure 3-6.4: The MLD Snooping Status

Parameter Description

VLAN ID: This is the VLAN ID of the entry.

Querier Version: This is the working querier version currently.

Host Version: This is the working host version currently.

Querier Status: This shows how the querier status is "ACTIVE" or "IDLE".

Queries Transmitted: This is the number of transmitted queries.

Queries Received: This is the number of received queries.

V1 Reports Received: This is the number of received V1 reports.

V2 Reports Received: This is the number of received V2 reports.

V1 Leaves Received: This is the number of received V1 leaves.

Auto-Refresh: If this option is selected, the device will automatically refresh the log.

Upper Right Icon (Refresh, <<, >>): Click to manually refresh the status, or move to the next or previous page.

3-6.5 Group Information

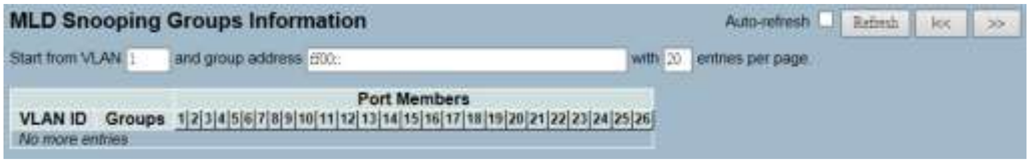
The section provides information on setting up the MLD snooping groups information. The “Start from VLAN” and “Group” input fields allow the user to select the starting point in the MLD group table.

Each page shows up to 99 entries from the MLD group table. The default is 20 and can be selected through the "Entries Per Page" input field. When you first visit the page, it will show the first 20 entries from the beginning of the MLD group table.

Web Interface

To display the MLD snooping group information in the web interface:

1. Click Configuration, MLD Snooping, and Group Information.
2. Click auto-refresh to automatically refresh the information.
3. Click refresh to manually refresh an entry.
4. Click clear to remove the MLD snooping groups information.



MLD Snooping Groups Information

Start from VLAN 1 and group address ff00:: with 20 entries per page.

		Port Members																									
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
No more entries																											

Figure 3-6.5: The MLD Snooping Groups Information

Parameter Description

Navigating the MLD Group Table

Each page shows up to 99 entries from the MLD Group table. The default is 20 and can be selected through the "Entries Per Page" input field. When you first visit the page, it 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 “Refresh” button will update the displayed table starting from that or the next closest.

In addition, the two input fields will (upon a “Refresh” button click) assume the value of the first displayed entry to allow for continuous refresh with the same start address. The “>>” will use the last entry of the currently displayed as a basis for the next lookup. When the end is reached the text "No More Entries" is shown. Use the “l<<” button to start over.

MLD Snooping Information Table Columns

VLAN ID: This is VLAN ID of the group.

Groups: This is group address of the group displayed.

Port Members: This is ports under this group.

Auto-refresh: If this option is selected, the device will automatically refresh the log.

Upper right icon (Refresh, <<, >>): Click to manually refresh the group status, or move to the next or previous page.

3-6.6 IPv6 SSM Information

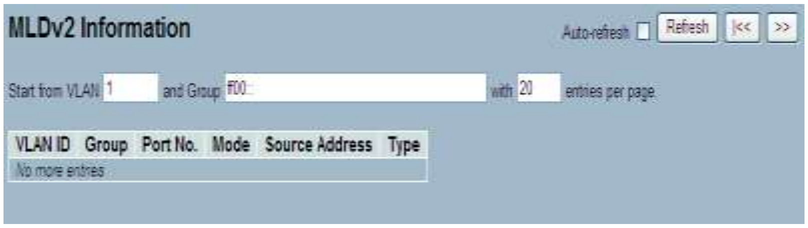
The section provides information on configurating the MLDv2 information entries. The MLDv2 information table is sorted first by VLAN ID, then by group, and then by port number. Diffrent source addresses belong to the same group are treated as single entry.

Each page shows up to 64 entries from the MLDv2 SSM (Source Specific Multicast) information table. The default is 20 and can be selected through the "Entries Per Page" input field. When you first visit the page, it will show the first 20 entries from the beginning of the MLDv2 information table. The "Start from VLAN" and "Group" input fields allow the user to select the starting point in the MLDv2 information table.

Web Interface

To display the MLDv2 IPv6 SSM information in the web interface:

1. Click Configuration, MLD Snooping, and IPv6 SSM Information.
2. Click auto-refresh to automatically refresh the information.
3. Click refresh to manually refresh an entry of the MLDv2 IPv6 SSM information.
4. Click “<< or >>” to move to the previous or next entry.



MLDv2 Information

Auto-refresh □ Refresh |<< >>

Start from VLAN 1 and Group ff00:: with 20 entries per page.

VLAN ID	Group	Port No.	Mode	Source Address	Type
No more entries					

Figure 3-6.6: The IPv6 SSM Information

Parameter Description

MLDv2 Information Table Columns

VLAN ID: This is VLAN ID of the group.

Group: This is group address of the group displayed.

Port: This is switch port number.

Mode: This indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either “Include” or “Exclude”.

Source Address: This is IP address of the source. Currently, the system limits the total number of IP source addresses for filtering to be 128.

Type: This indicates the type. It can be either “Allow” or “Deny”.

3-7 MVR

The MVR feature enables multicast traffic forwarding on the Multicast VLAN. In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP join message to switch A to join the appropriate multicast. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

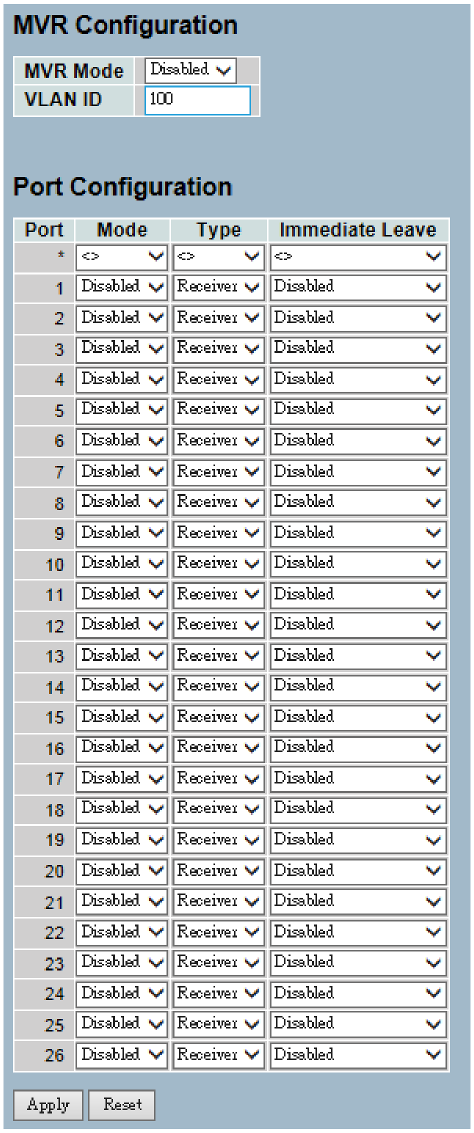
3-7.1 Configuration

The section provides information on how to configure MVR and its parameters.

Web Interface

To configure the MLD snooping port group configuration in the web interface:

1. Click Configuration, MVR, and Configuration.
2. Select enable or disable for the MVR mode, and then set all parameters.
3. Click save.
4. Click reset to restore default settings.



MVR Configuration

MVR Mode	Disabled
VLAN ID	100

Port Configuration

Port	Mode	Type	Immediate Leave
*	<>	<>	<>
1	Disabled	Receiver	Disabled
2	Disabled	Receiver	Disabled
3	Disabled	Receiver	Disabled
4	Disabled	Receiver	Disabled
5	Disabled	Receiver	Disabled
6	Disabled	Receiver	Disabled
7	Disabled	Receiver	Disabled
8	Disabled	Receiver	Disabled
9	Disabled	Receiver	Disabled
10	Disabled	Receiver	Disabled
11	Disabled	Receiver	Disabled
12	Disabled	Receiver	Disabled
13	Disabled	Receiver	Disabled
14	Disabled	Receiver	Disabled
15	Disabled	Receiver	Disabled
16	Disabled	Receiver	Disabled
17	Disabled	Receiver	Disabled
18	Disabled	Receiver	Disabled
19	Disabled	Receiver	Disabled
20	Disabled	Receiver	Disabled
21	Disabled	Receiver	Disabled
22	Disabled	Receiver	Disabled
23	Disabled	Receiver	Disabled
24	Disabled	Receiver	Disabled
25	Disabled	Receiver	Disabled
26	Disabled	Receiver	Disabled

Figure 3-7.1: The MVR Configuration

Parameter Description

MVR Mode: This enables/disables the global MVR.

VLAN ID: This specifies the multicast VLAN ID.

Mode: This enables MVR on the port.

Type: This specifies the MVR port type on the port.

Immediate Leave: This enables the fast leave on the port.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

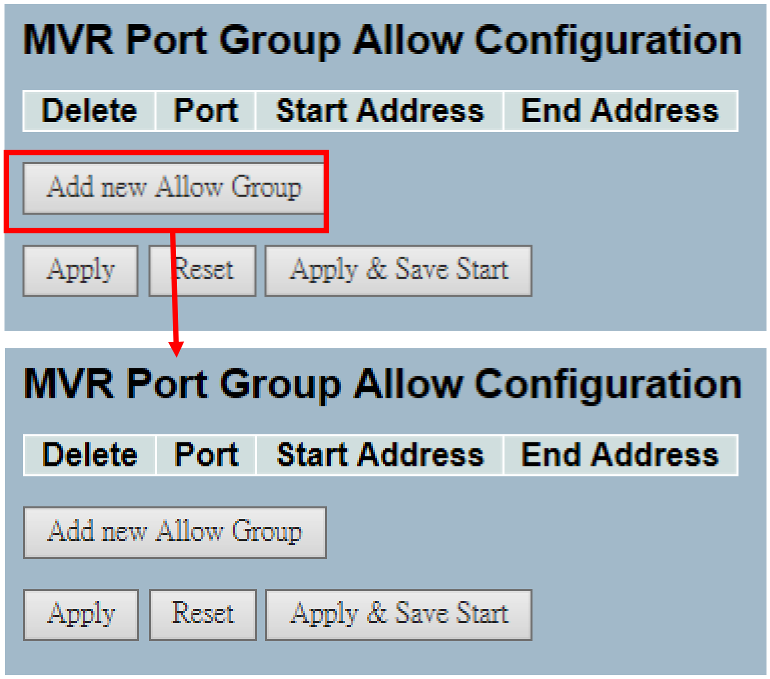
3-7.2 MVR Port Group Allow Configuration

The section provides information on adding the IP multicast group, which is allowed to receive the multicast stream. The MVR port group table is sorted first by port, and then by IP address.

Web Interface

To display the MVR groups information in the web interface:

1. Click Configuration, MVR, and Port Groups Allow.
2. If you want to add a new allowed group, click “Add New Allow Group”.
3. Select the “Port No.”, “Start Address”, and “End Address”.
4. Click “Apply” to apply the configuration of MVR port group allow table.



MVR Port Group Allow Configuration

Delete	Port	Start Address	End Address

MVR Port Group Allow Configuration

Delete	Port	Start Address	End Address

Figure 3-7.2: The MVR Groups Information

Parameter Description

Delete: Click delete to remove the entry.

Port: This is the logical port for the settings.

Allow Groups: This is the IP multicast group that will be allowed.

Adding New Allow Group: Click “Add New Allow Group” to add a new entry to the group allow table. Specify the port and allow group of the new entry. Click "Apply".

Buttons:

- **Apply** – Click to save changes.
- **Reset-** Click to restore default settings.

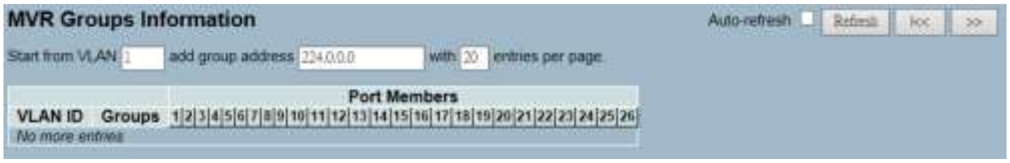
3-7.2 Groups Information

The section provides information on how to display the MVR group detailed information. The MVR group table is sorted first by VLAN ID and then by group.

Web Interface

To display the MVR groups information in the web interface:

1. Click Configuration, MVR, and Groups Information.
2. Click auto-refresh to automatically refresh the information.
3. Click refresh to manually refresh the entry.
4. Click “<< or >>” to move to the previous or next entry.



MVR Groups Information

Start from VLAN 1 add group address 224.0.0.0 with 20 entries per page

		Port Members																									
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
No more entries																											

Figure 3-7.2: The MVR Groups Information

Parameter Description

<u>**MVR Group Table Columns**</u>

VLAN ID: This is the VLAN ID of the group.

Groups: This is the group ID of the group displayed.

Port Members: These are ports under this group.

Auto-Refresh: Click auto-refresh to automatically refresh the information.

Upper Right Icon (Refresh, <<, >>): Click to manually refresh the MVR group information, or to move to the previous or next page.

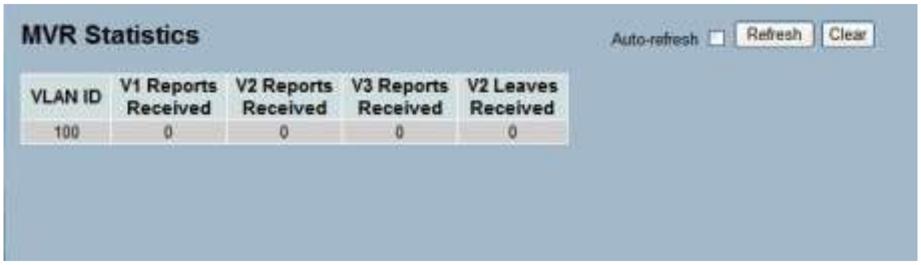
3-7.3 Statistics

The section provides information on how to display the MVR statistics in details.

Web Interface

To display the MVR statistics information in the web interface:

1. Click Configuration, MVR, and Statistics.
2. Click auto-refresh to automatically refresh the information.
3. Click refresh to manually refresh the information.
4. Click “<< or >>” to move to the previous or next entry.



VLAN ID	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
100	0	0	0	0

Figure 3-7.3: The MVR Statistics Information

Parameter Description

VLAN ID: This is the multicast VLAN ID.

V1 Reports Received: This is the number of received V1 reports.

V2 Reports Received: This is the number of received V2 reports.

V3 Reports Received: This is the number of received V3 reports.

V2 Leaves Received: This is the number of received V2 leaves.

Auto-Refresh: Click to automatically refresh the information.

Upper Right Icon (Refresh, <<, >>): Click to manually refresh the group information, or to move to the previous or next page.

3-8 LLDP

The switch supports the LLDP. The Link Layer Discovery Protocol (LLDP) provides a standards-based method for enabling switches to advertise themselves to adjacent devices and to learn about adjacent LLDP devices. The Link Layer Discovery Protocol (LLDP) is a vendor-neutral link layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on a IEEE 802 local area network, principally wired Ethernet. The protocol is formally referred to by the IEEE as station and media access control connectivity discovery specified in standards document IEEE 802.1AB.

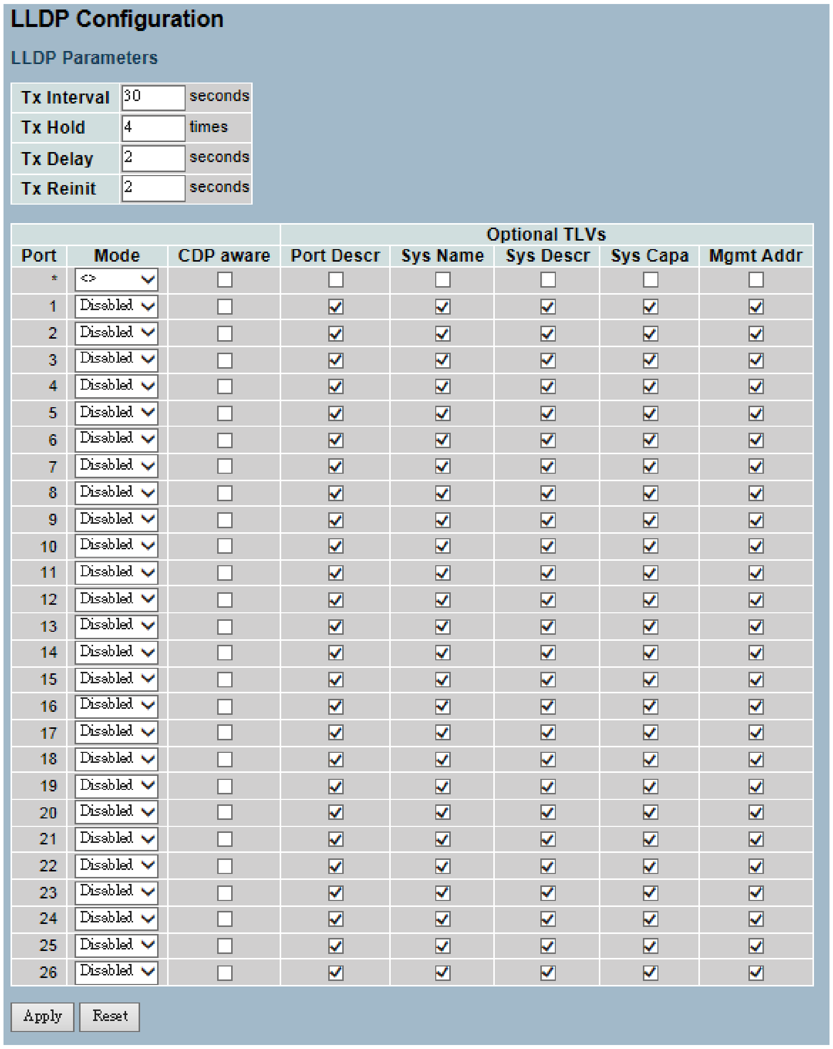
3-8.1 LLDP Configuration

You can per port to do the LLDP configuration and the detail parameters, the settings will take effect immediately. This section provides inspection and configuration settings for the current LLDP port.

Web Interface

To configure LLDP:

1. Click LLDP configuration.
2. Modify the LLDP timing parameters.
3. Set the required mode for transmitting or receiving LLDP messages.
4. Specify the information to include in the TLV field of advertised messages.
5. Click save.



LLDP Configuration

LLDP Parameters

Tx Interval	30	seconds
Tx Hold	4	times
Tx Delay	2	seconds
Tx Reinit	2	seconds

			Optional TLVs				
Port	Mode	CDP aware	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	□	□	□	□	□	□
1	Disabled	□	☑	☑	☑	☑	☑
2	Disabled	□	☑	☑	☑	☑	☑
3	Disabled	□	☑	☑	☑	☑	☑
4	Disabled	□	☑	☑	☑	☑	☑
5	Disabled	□	☑	☑	☑	☑	☑
6	Disabled	□	☑	☑	☑	☑	☑
7	Disabled	□	☑	☑	☑	☑	☑
8	Disabled	□	☑	☑	☑	☑	☑
9	Disabled	□	☑	☑	☑	☑	☑
10	Disabled	□	☑	☑	☑	☑	☑
11	Disabled	□	☑	☑	☑	☑	☑
12	Disabled	□	☑	☑	☑	☑	☑
13	Disabled	□	☑	☑	☑	☑	☑
14	Disabled	□	☑	☑	☑	☑	☑
15	Disabled	□	☑	☑	☑	☑	☑
16	Disabled	□	☑	☑	☑	☑	☑
17	Disabled	□	☑	☑	☑	☑	☑
18	Disabled	□	☑	☑	☑	☑	☑
19	Disabled	□	☑	☑	☑	☑	☑
20	Disabled	□	☑	☑	☑	☑	☑
21	Disabled	□	☑	☑	☑	☑	☑
22	Disabled	□	☑	☑	☑	☑	☑
23	Disabled	□	☑	☑	☑	☑	☑
24	Disabled	□	☑	☑	☑	☑	☑
25	Disabled	□	☑	☑	☑	☑	☑
26	Disabled	□	☑	☑	☑	☑	☑

Figure 3-8.1: The LLDP Configuration

Parameter Description

LLDP Parameters

Tx Interval: The switch periodically transmits LLDP frames to its neighbours 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 how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2 - 10 times.

Tx Delay: If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than 1/4 of the Tx Interval value. Valid values are restricted to 1 - 8192 seconds.

Tx Reinit: When a port is disabled, the LLDP is disabled, or the switch is rebooted, an LLDP shutdown frame is transmitted to the neighboring units to signal that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.

LLDP Port Configuration

The LLDP port settings relate to the currently selected, as reflected by the page header.

Port: This is the switch port number of the logical LLDP port.

Mode: This selects 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: This selects the CDP awareness.

- The CDP operation is restricted to decoding incoming CDP frames. The switch doesn't transmit CDP frames. CDP frames are only decoded if LLDP on the port is enabled.
- Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded. Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics. CDP TLVs are mapped onto LLDP neighbors' table as shown below.
- CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.
- CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors' table.
- CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.
- CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.
- Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP 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, all enabled CDP frames are terminated by the switch.

NOTE: When CDP awareness on a port is disabled, the CDP information isn't removed immediately, but gets when the hold time is exceeded.

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.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

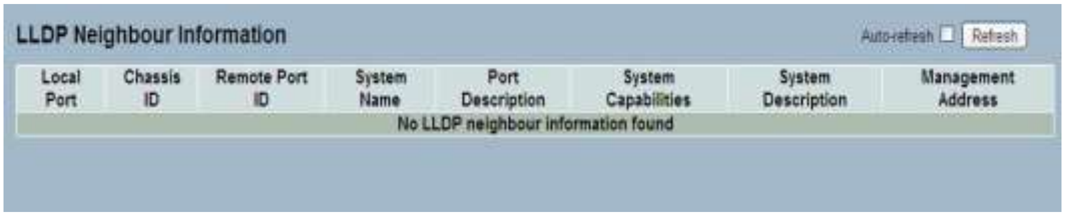
3-8.2 LLDP Neighbours

This section provides a status overview for all LLDP neighbours. The displayed table contains a row for each port, which an LLDP neighbour is detected on.

Web Interface

To show LLDP neighbours:

1. Click LLDP Neighbours.
2. Click refresh for manually update the web screen.
3. Click auto-refresh for automatically update the web screen.



LLDP Neighbour Information

Auto-refresh □ Refresh

Local Port	Chassis ID	Remote Port ID	System Name	Port Description	System Capabilities	System Description	Management Address
No LLDP neighbour information found							

Figure 3-8.2: The LLDP Neighbours Information

NOTE: If your network is without any device and supports LLDP, then the table will show “No LLDP Neighbour Information Found”.

Parameter Description

Local Port: This is the port that receives the LLDP frame.

Chassis ID: The chassis ID is the identification of the neighbour's LLDP frames.

Remote Port ID: The remote port ID is the identification of the neighbour port.

System Name: System name is the name advertised by the neighbour unit.

Port Description: Port description is the port description advertised by the neighbour unit.

System Capabilities: System capabilities describes the neighbour unit's capabilities. The possible capabilities are:

1. Other
2. Repeater
3. Bridge

4. WLAN Access Point
5. Router
6. Telephone
7. DOCSIS Cable Device
8. Station Only
9. Reserved

When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).

System Description: System description is the port description advertised by the neighbour unit.

Management Address: Management address is the neighbour unit's address that is used for higher layer entities to assist discovery by the network management. This could hold the neighbour's IP address.

Auto-Refresh: Click auto-refresh to automatically refresh the LLDP neighbours information.

Upper Right Icon (Refresh): Click refresh to manually refresh the LLDP neighbours information.

3-8.3 LLDP-MED Configuration

Media Endpoint Discovery is an enhancement of LLDP, also known as LLDP-MED, that provides the following facilities:

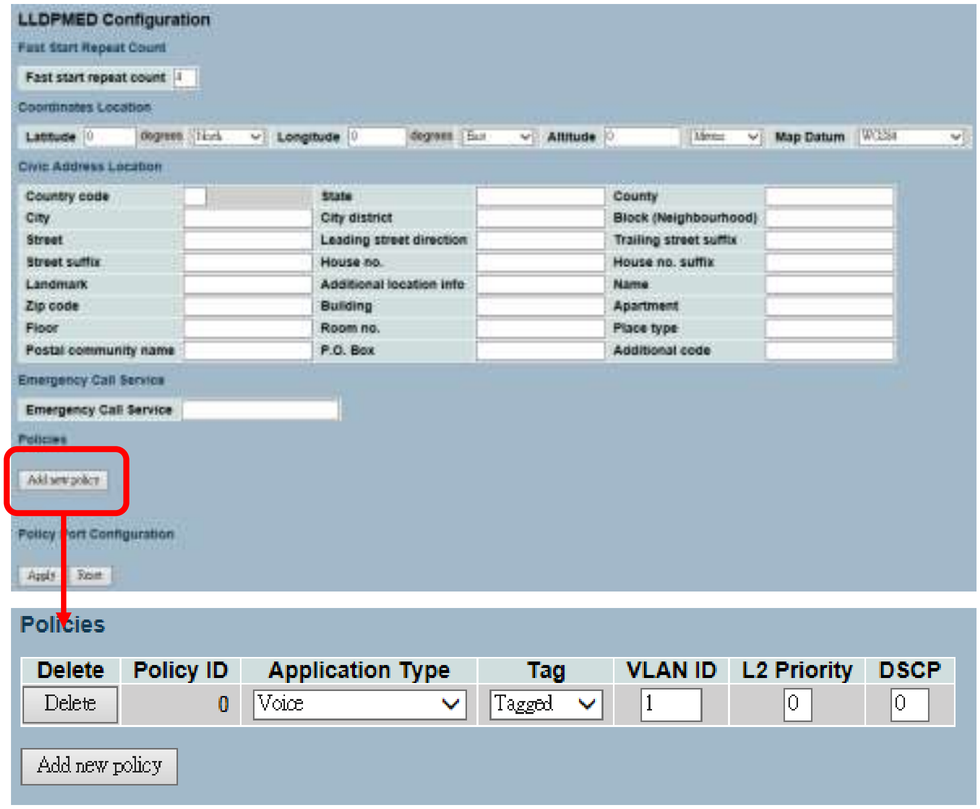
- Auto-discovery of LAN policies (VLAN, Layer 2 Priority and Differentiated services [Diffserv] settings) enables plug-and-play networking.
- Device location discovery allowa creation of location databases and, in the case of Voice over Internet Protocol [VoIP], enhanced 911 services.
- Inventory management allows network administrators to track their network devices and to determine their characteristics (manufacturer, software and hardware versions, serial or asset number).

This sections provides configuration information for the LLDP-MED. This function applies to VoIP devices that support LLDP-MED.

Web Interface

To configure LLDP-MED:

1. Click LLDP-MED Configuration.
2. Modify the fast start repeat count parameter. The default is 4.
3. Modify the coordinates location parameters.
4. Fill in the civic address location parameters.
5. Add new policy.
6. Click save.
7. Select the policy ID for each port.
8. Click save.



LLDPMED Configuration

Fast Start Repeat Count

Fast start repeat count: 4

Coordinates Location

Latitude: 0 degrees North | Longitude: 0 degrees East | Altitude: 0 Meters | Map Datum: WGS84

Civic Address Location

Country code		State		County	
City		City district		Block (Neighbourhood)	
Street		Leading street direction		Trailing street suffix	
Street suffix		House no.		House no. suffix	
Landmark		Additional location info		Name	
Zip code		Building		Apartment	
Floor		Room no.		Place type	
Postal community name		P.O. Box		Additional code	

Emergency Call Service

Emergency Call Service:

Policies

Policy Port Configuration

Policies

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
Delete	0	Voice	Tagged	1	0	0

Figure 3-8.3: The LLDP-MED Configuration

Parameter Description

<u>Fast start repeat count</u>

In general, rapid startup and emergency call service location identification discovery of endpoints is a critically important aspect of VoIP systems. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy.

With this in mind, LLDP-MED defines an LLDP-MED fast start interaction between the protocol and the application layers on top of the protocol in order to achieve these related properties. Initially, a network connectivity device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED endpoint device is detected, will an LLDP-MED capable network connectivity device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbour has been detected in order share LLDP-MED information as fast as possible to new neighbours.

Because there is a risk of an LLDP frame being lost during transmission between neighbours, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbours receiving the LLDP frame. With fast start repeat count, it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted when an LLDP frame with new information is received.

It should be noted that LLDP-MED and the LLDP-MED fast start mechanism is only intended to run on links between LLDP-MED network connectivity devices and endpoint devices. This does not apply to links between LAN infrastructure elements including network connectivity devices or other types of links.

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 -32767 to 32767 with a maximum of 4 digits.

It is possible to select between two altitude types (floors or meters).

- **Meters**: This represents meters of Altitude defined by the vertical datum specified.
- **Floors**: This represents 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).

Country Code: This is the two-letter ISO 3166 country code in capital ASCII letters. Examples: DK, DE, or US.

State: This is the national subdivisions (state, canton, region, province, prefecture).

County: This is county, parish, gun (Japan), or district.

City: This is city, township, or shi (Japan). Example: Copenhagen.

City District: This is city division, borough, city district, ward, orchou (Japan).

Block (Neighbourhood): This is neighbourhood or block.

Street: This is street. Example: Poppelvej.

Leading Street Direction: This is the leading street direction. Example: N.

Trailing Street Suffix: This is trailing street suffix. Example: SW.

Street Suffix: This is the street suffix. Example: Ave, Platz.

House No.: This is the house number. Example: 21.

House No. Suffix: This is the house number suffix. Example: A, 1/2.

Landmark: This is the landmark or vanity address. Example: Columbia University.

Additional Location Info: This is the additional location info. Example: South Wing.

Name: This is the name (residence and office occupant). Example: Flemming Jahn.

Zip Code: This is the postal/zip code. Example: 2791.

Building: This is the building (structure). Example: Low Library.

Apartment: This is the unit (Apartment, suite). Example: Apt 42.

Floor: This is the floor. Example: 4.

Room No.: This is the room number. Example: 450F.

Place Type: This is the place type. Example: Office.

Postal Community Name: This is the postal community name. Example: Leonia.

P.O. Box : This is the post office box (P.O. BOX). Example: 12345.

Additional Code : This is the additional code. Example: 1320300003.

Emergency Call Service: This is the emergency call service (e.g. E911 and others), such as defined by TIA or NENA.

Emergency Call Service: Emergency call service ELIN identifier data format is defined to carry the ELIN identifier, as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Policies

Network policy discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated layer 2 and layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service.

Policies are only intended for use with applications that have specific “real-time” network policy requirements, such as interactive voice and/or video services.

The network policy attributes advertised are:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)
2. Layer 2 Priority Value (IEEE 802.1D-2004)
3. Layer 3 Diffserv Code Point (DSCP) Value (IETF RFC 2474)

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:

1. Voice
2. Guest Voice
3. Softphone Voice
4. Video Conferencing
5. Streaming Video
6. Control / Signalling (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. Therefore, it does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

Delete: Click to delete the policy.

Policy ID: This is the auto-generated ID for the policy. It shall be used when selecting the polices that shall be mapped to the specific ports.

Application Type: Intended use of the application types:

1. **Voice** – This is to be used by dedicated IP telephony handsets and other similar appliances that support 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 Signalling (Conditional)** - This is to be used in network topologies that require a different policy for the voice signalling 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** – This supports a separate "limited feature-set" voice service for guest users and visitors with their own IP telephony handsets and other similar appliances that support interactive voice services.
4. **Guest Voice Signalling (Conditional)** - This is to be used in network topologies that require a different policy for the guest voice signalling 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** - This is to be used by softphone applications on typical data centric devices such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs 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 below), then the L2 priority field is ignored and only the DSCP value has relevance.
6. **Video Conferencing** - This is to be used by dedicated video conferencing equipment and other similar appliances that support real-time interactive video/audio services.
7. **Streaming Video** - This is to be used by broadcast or multicast based video content distribution and other similar applications that support streaming video services that require specific network policy treatment. Video applications that rely on TCP with buffering would not be an intended use of this application type.
8. **Video Signalling (Conditional)** - This is to be used in network topologies that require a separate policy for the video signalling 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**: This indicates that the device is using an untagged frame format and 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**: This indicates that the device is using the IEEE 802.1Q tagged frame format. Both the VLAN ID, the layer 2 priority values, and the DSCP value are being used.

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: This is the 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: The DSCP value provides Diffserv node behaviour 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 a new policy. Specify the application type, tag, VLAN ID, L2 priority, and DSCP for the new policy.

Port Policies Configuration: Every port may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or port configuration.

Port: This is the port number to which the configuration applies.

Policy ID: This is 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.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

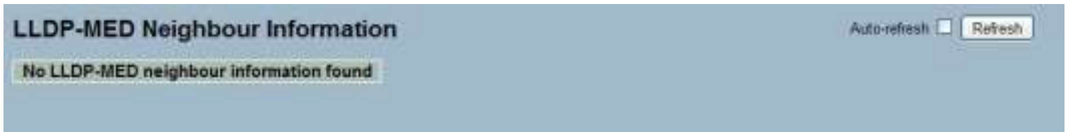
3-8.4 LLDP-MED Neighbours

This sections provides a status overview of all LLDP-MED neighbours. The displayed table contains a row for each port which an LLDP neighbour is detectedon. This function applies to VoIP devices that support LLDP-MED.

Web Interface

To show LLDP-MED neighbor:

1. Click LLDP-MED Neighbor.
2. Click refresh to manually update the web screen.
3. Click auto-refresh to automatically update the web screen



LLDP-MED Neighbour Information

No LLDP-MED neighbour information found

Figure 3-9.4: The LLDP-MED Neighbours Information

NOTE: If your network supports LLDP-MED without any device, then the table will show "No LLDP-MED Neighbour Information Found".

Parameter Description

Port: This is the port where 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, any LLDP-MED endpoint device that claims compliance as a media endpoint (Class II) also support all aspects of TIA-1057 applicable to generic endpoints (Class I). Any LLDP-MED endpoint device that claims 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, they 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, it 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. They 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 neighborhood unit's LLDP-MED capabilities. The possible capabilities are:

1. LLDP-MEDCcapabilities
2. Network Policy
3. Location Identification
4. Inventory
5. Reserved

Application Type: Application type indicates 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.

1. **Voice** – This is to be used by dedicated IP telephony handsets and other similar appliances that support 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 Signalling** - This is to be used in network topologies that require a different policy for the voice signalling than for the voice media.
3. **Guest Voice** – This supports a separate limited feature-set voice service for guest users and visitors with their own IP

telephony handsets and other similar appliances that support interactive voice services.

4. **Guest Voice Signalling** - This is to be used in network topologies that require a different policy for the guest voice signalling than for the guest voice media.
5. **Softphone Voice** - This is to be used by softphone applications on typical data centric devices, such as PCs or laptops.
6. **Video Conferencing** - This is to be used by dedicated video conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
7. **Streaming Video** - This is to be used by broadcast or multicast based video content distribution and other similar applications that support 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 Signalling** - This is to be used in network topologies that require a separate policy for the video signalling than for the video media.

Policy: Policy indicates that an endpoint device wants to explicitly advertise that the policy is required by the device. It 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. It can be “Tagged” or “Untagged”.

- **Untagged**: The device is using an untagged frame format and 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: The 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. This means 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. It contains one of 64 code point values (0 through 63).

3-8.5 EEE

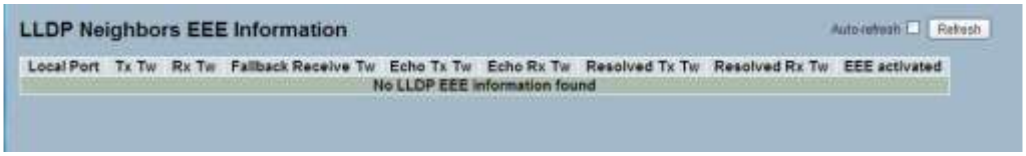
By using EEE, power savings can be achieved at the expense of traffic latency. This latency occurs when the circuits EEE turn off to save power and need time to boot up before sending traffic over the link. This time is called "wakeup time". To achieve minimal latency, devices can use LLDP to exchange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

This page provides an overview of EEE information exchanged by LLDP.

Web Interface

To show LLDP EEE neighbors:

1. Click LLDP, than click EEE to show discover EEE devices.
2. Click refresh for manually update the web screen.
3. Click auto-refresh for automatically update the web screen.



LLDP Neighbors EEE Information

Local Port	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE activated
No LLDP EEE information found								

Figure 3-8.5: The LLDP Neighbors EEE Information

NOTE: If your network enables the EEE function without any devices, then the table will show “No LLDP EEE Information Found”.

Parameter Description

Local Port: This is the port that receives or transmits the LLDP frames.

Tx Tw: This is the link partner’s maximum time to transmit path and hold off sending data after reassertion of LPI.

Rx Tw: Thi is the link partner’s time to receive data and to tell the transmitter to hold off in order to allow time for the receiver to wake up from sleep.

Fallback Receive Tw: This is the link partner’s fallback 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 may be used for a more efficient allocation. If systems do not implement this option, the default value is the same as the Receive Tw_sys_tx.

Echo Tx Tw: This is the link partner's Echo Tx Tw value.

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 or not 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: This is the link partner's Echo Rx Tw value.

Resolved Tx Tw: This is the resolved Tx Tw for this link. **Note**: NOT the link partner.

The resolved value is the actual "tx wakeup time" used for this link (based on EEE information exchanged via LLDP).

Resolved Rx Tw: This is the resolved Rx Tw for this link. **Note:** NOT the link partner.

The resolved value is the actual "tx wakeup time" used for this link (based on EEE information exchanged via LLDP).

EEE Activated: This shows if the switch and the link partner have agreed upon the wakeup times.

- **Red -** Switch and link partner have not agreed upon wakeup time.
- **Green -** Switch and link partner have agreed upon wakeup time.

Auto-Refresh: Click to automatically refresh the information.

Upper Right Icon (Refresh): Click to manually refresh the LLDP Neighbors information.

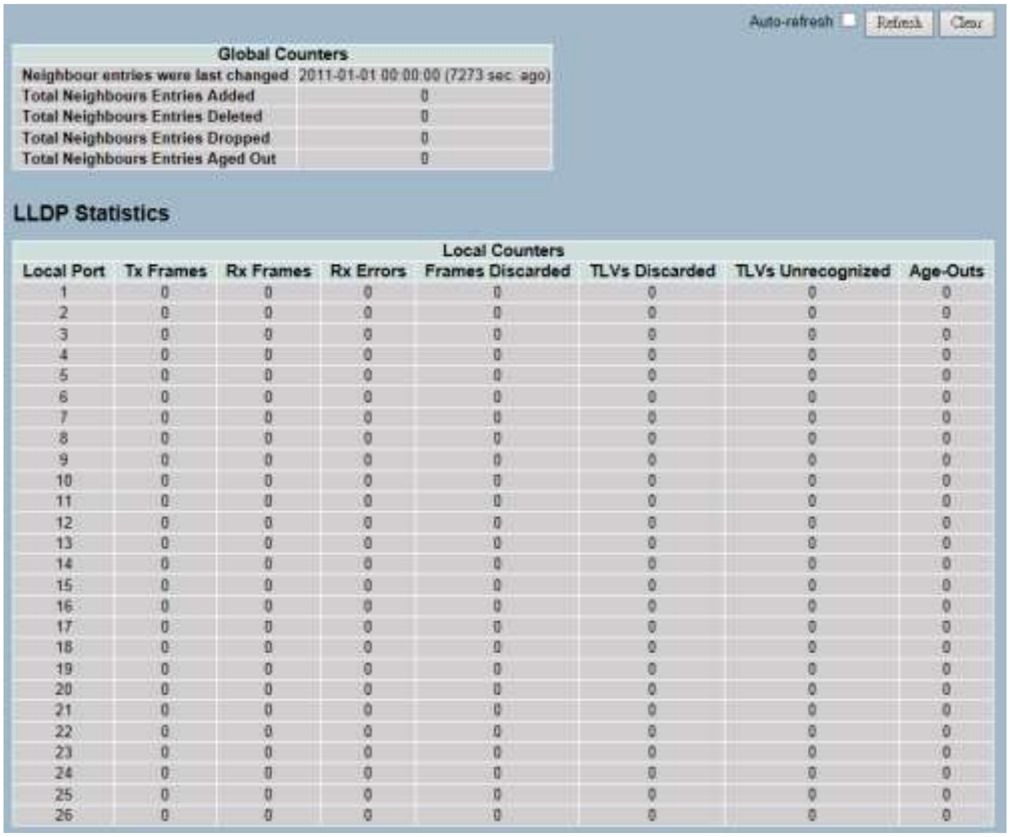
3-8.6 Port Statistics

There are two types of counters for port statistics – global and local. Global counters are counters that refer to the whole switch, while local counters refer to per port.

Web Interface

To show LLDP Statistics:

1. Click LLDP, than click Port Statistics to show LLDP counters.
2. Click refresh to manually update the web screen.
3. Click auto-refresh to automatically update the web screen.
4. Click clear to clear all counters.



Global Counters	
Neighbour entries were last changed	2011-01-01 00:00:00 (7273 sec. ago)
Total Neighbours Entries Added	0
Total Neighbours Entries Deleted	0
Total Neighbours Entries Dropped	0
Total Neighbours Entries Aged Out	0

LLDP Statistics

Local Counters							
Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Age-Outs
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0

Figure 3-8.6: The LLDP Port Statistics Information

Parameter Description

Global Counters

Neighbour Entries Were Last Changed At: This shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.

Total Neighbours Entries Added: This shows the number of new entries added since switch reboot.

Total Neighbours Entries Deleted: This shows the number of new entries deleted since switch reboot.

Total Neighbours Entries Dropped: This shows the number of LLDP frames dropped due to the entry table being full.

Total Neighbours Entries Aged Out: This shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

The displayed table contains a row for each port. The columns hold the following information:

- **Local Port:** This shows the port that receives or transmits the LLDP frames.
- **Tx Frames:** This shows the number of LLDP frames transmitted on the port.
- **Rx Frames:** This shows the number of LLDP frames received on the port.
- **Rx Errors:** This shows the number of received LLDP frames that contains some kind of error.

Frames Discarded: If an LLDP frame is received on a port and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbours" in the LLDP standard. LLDP frames require a new entry in the table when the chassis ID or remote port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received or when the entry ages out.

TLVs Discarded: Each LLDP frame contains multiple pieces of information, known as TLVs (Type Length Value). If a TLV is malformed, it is counted and discarded.

TLVs Unrecognized: This is the number of well-formed TLVs, but with an unknown type value.

Age-Outs: Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed and the age-out counter is incremented.

Auto-Refresh: Click to automatically refresh the information.

Upper Right Icon (Refresh, Clear): Click to manually refresh or clear the LLDP port statistics information.

3-9 Filtering Data Base

Filtering data base configuration gathers many functions including MAC table information and static MAC learning, which cannot be categorized to some function type.

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 in order to know 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 has been seen after a configurable age time.

3-9.1 Configuration

This sections provides information on the MAC address table configurations, along with setting entries timeouts for dynamic MAC table and other static MAC table configurations.

Web Interface

To configure MAC Address Table in the web interface:

Aging Configuration

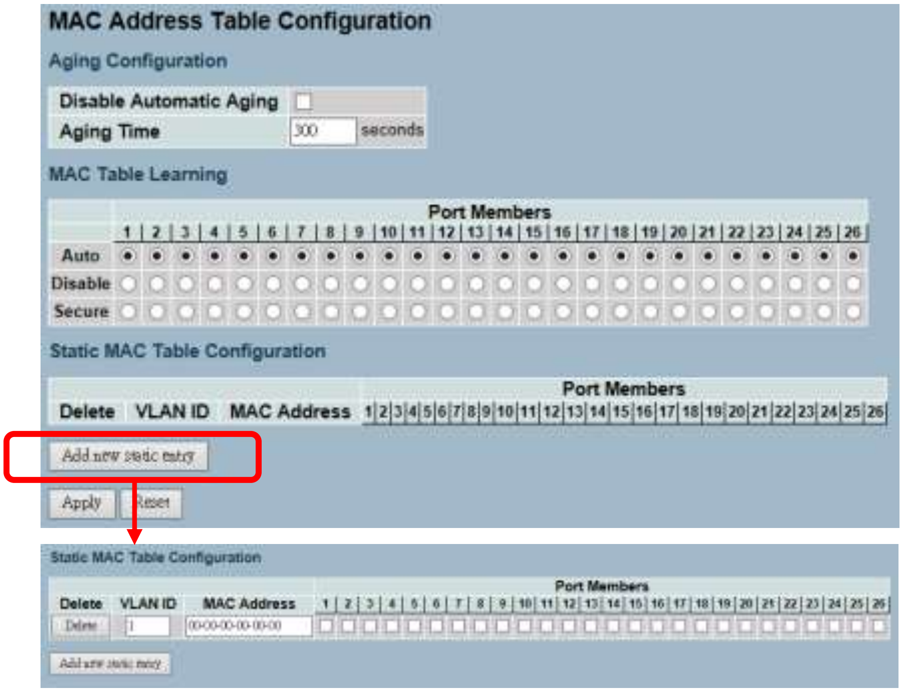
1. Click configuration.
2. Specify the disable automatic aging and aging time.
3. Click save.

MAC Table Learning

1. Click configuration.
2. Specify the port members (Auto, Disable, or Secure).
3. Click save.

Static MAC Table Configuration

1. Click configuration and add new static entry.
2. Specify the VLAN IP, MAC address, and port members.
3. Click save.



MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	☐	
Aging Time	300	seconds

MAC Table Learning

	Port Members																									
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Auto	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Static MAC Table Configuration

			Port Members																									
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Static MAC Table Configuration

			Port Members																									
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Delete	1	00-00-00-00-00-00	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Figure 3- 9.1: The MAC Address Table Configuration

Parameter Description

Aging Configuration

By default, the dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging.

- Configure the aging time by entering a value in seconds. For example, Age Time □ seconds.
- The allowed range is 10 to 1000000 seconds.
- Disable the automatic aging of dynamic entries by checking ☑ Disable Automatic Aging.

MAC Table Learning

If the learning mode for a given port is greyed out, another module is in control of the mode and cannot be changed by the user. An example of such a module is the MAC-based authentication under 802.1X. Each port can do learning based upon the following settings:

- **Auto:** Learning is done automatically when a frame with unknown SMAC is received.
- **Disable:** No learning is done.

- **Secure:** Only static MAC entries are learned, while all other frames are dropped.

NOTE: Make sure that the link used for managing the switch is added to the static MAC table before changing to secure learning mode. Otherwise, the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries.

The MAC table is sorted first by VLAN ID and then by MAC address.

Delete: Click delete to remove the entry.

VLAN ID: This is the VLAN ID of the entry.

MAC Address: This is the MAC address of the entry.

Port Members: Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

Adding a New Static Entry: Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

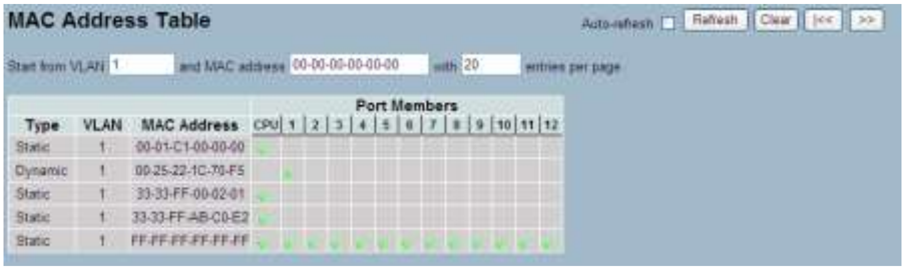
3-9.2 Dynamic MAC Table

This sections provides information about entries in the MAC table. It contains up to 8192 entries. It is sorted first by VLAN ID and then, by MAC address.

Web Interface

To display MAC address table in the web interface:

1. Click Dynamic MAC Table.
2. Specify the VLAN and MAC address.
3. Display MAC address table.



MAC Address Table

Auto-refresh □ Refresh Clear |<< >>

Start from VLAN 1 and MAC address 00-00-00-00-00-00 with 20 entries per page

			Port Members												
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9	10	11	12
Static	1	00-01-C1-00-00-00	✓												
Dynamic	1	00-25-22-1C-70-F5		✓											
Static	1	33-33-FF-00-02-01	✓												
Static	1	33-33-FF-AB-C0-E2	✓												
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Figure 3- 9.2: The Dynamic MAC Address Table Information

Parameter Description

<u>**MAC Table Columns**</u>

Type: This indicates whether the entry is a static or a dynamic entry.

VLAN: This is the VLAN ID of the entry.

MAC Address: This is the MAC address of the entry.

Port Members: These ports that are members of the entry.

Auto-Refresh: Click to automatically refresh the information.

Upper Right Icon (Refresh, Clear, <<, >>): Click to manually refresh or clear the MAC address entries, or to move to the previous or next page.

NOTE:

00-40-C7-73-01-29: The switch MAC address (for IPv4).

33-33-00-00-00-01: Destination MAC for IPv6 router advertisement (reference IPv6 RA.JPG).

33-33-00-00-00-02: Destination MAC for IPv6 router solicitation (reference IPv6 RS.JPG).

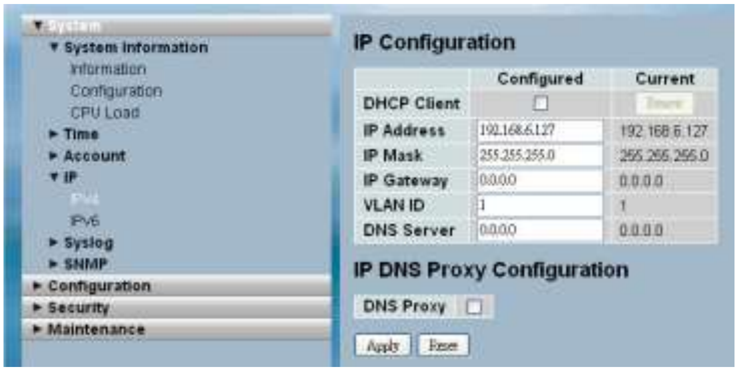
33-33-FF-73-01-29: Destination MAC for IPv6 neighbor solicitation (reference IPv6 DAD.JPG).

33-33-FF-A8-01-01: This is your switch MAC address for IPv6 global IP.

FF-FF-FF-FF-FF-FF: This is for broadcast.

3-10 VLAN

This sections provides information on assigning a specific VLAN for management purpose. The management VLAN is used to establish an IP connection to the switch from a workstation connected to a port in the VLAN. This connection supports a VSM, SNMP, and Telnet session. By default, the active management VLAN is VLAN 1, but you can designate any VLAN as the management VLAN by configuring System->IP->IPv4->VLAN ID. Only one management VLAN can be active at a time.



IP Configuration

	Configured	Current
DHCP Client	□	[illegible]
IP Address	192.168.6.127	192.168.6.127
IP Mask	255.255.255.0	255.255.255.0
IP Gateway	0.0.0.0	0.0.0.0
VLAN ID	1	1
DNS Server	0.0.0.0	0.0.0.0

IP DNS Proxy Configuration

DNS Proxy □

Figure 3-10.1.1: IP Configuration for Management VLAN

When you specify a new management VLAN, the HTTP connection to the old management VLAN is lost. For this reason, you should have a connection between your management station and a port in the new management VLAN or connect to the new management VLAN through a multi-VLAN route.

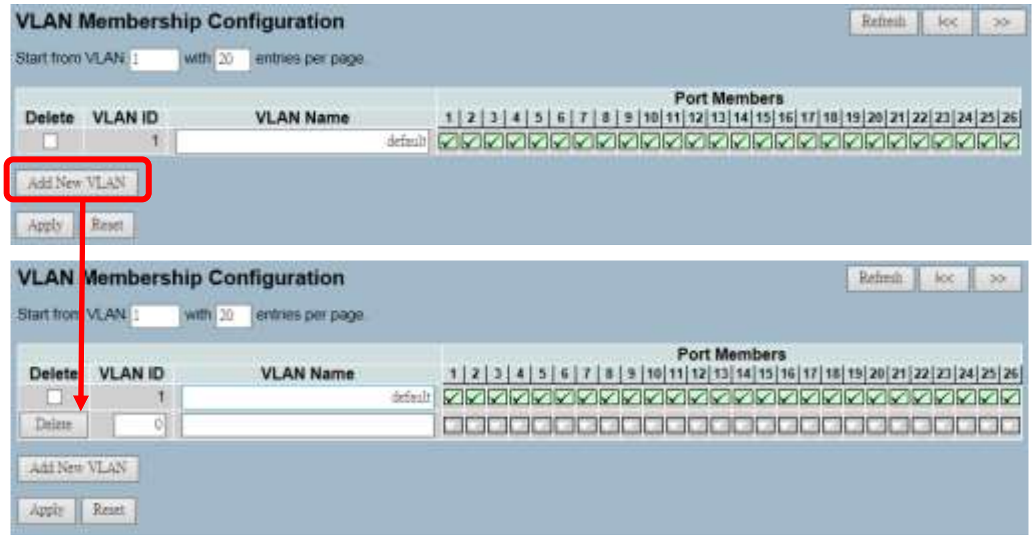
3-10.1 VLAN Membership

This section provides information on modifying and monitoring the VLAN membership configuration. This supports up to 4094 VLANs. You will also learn how to add and delete VLANs and port members of each VLAN.

Web Interface

To configure VLAN membership configuration in the web interface:

1. Click VLAN membership configuration.
2. Specify the management VLAN ID from 1 to 4094.
3. Click save.



VLAN Membership Configuration

Start from VLAN 1 with 20 entries per page

Delete	VLAN ID	VLAN Name	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
☐	1	default	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

VLAN Membership Configuration

Start from VLAN 1 with 20 entries per page

Delete	VLAN ID	VLAN Name	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
☐	1	default	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Delete	0		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Figure 3-10.1.2: The VLAN Membership Configuration

Parameter Description

Delete: Click to delete a VLAN entry for the selected switch.

Warning: You are able to delete the default VLAN 1. However, if the default VLAN 1 is deleted, the connection to the switch will be lost and some errors will occur.

VLAN ID: This indicates the ID of every single VLAN. The legal values for a VLAN ID are 1 to 4094.

VLAN Name: This indiciates the name of VLAN. The VLAN name contains a mix of alphabets, numbers and blanks, but excludes special characters. The length of VLAN name supports up to 32 characters. It can be edited for existing VLAN entries.

Port Members: A row of check boxes for each port display port members of each VLAN. Click the checkbox to include a port in the VLAN. Uncheck the box to remove or exclude a port from the VLAN.

Adding a New VLAN: Click to add a new VLAN group. **Note**: A VLAN without any port members cannot be set up.

Buttons:

- **Apply** – Click to save changes.
- **Reset-** Click to restore default settings.

Upper right icon (Refresh, |<<, >>): Click to manually refresh the VLAN entries, or to go to the next or previous page.

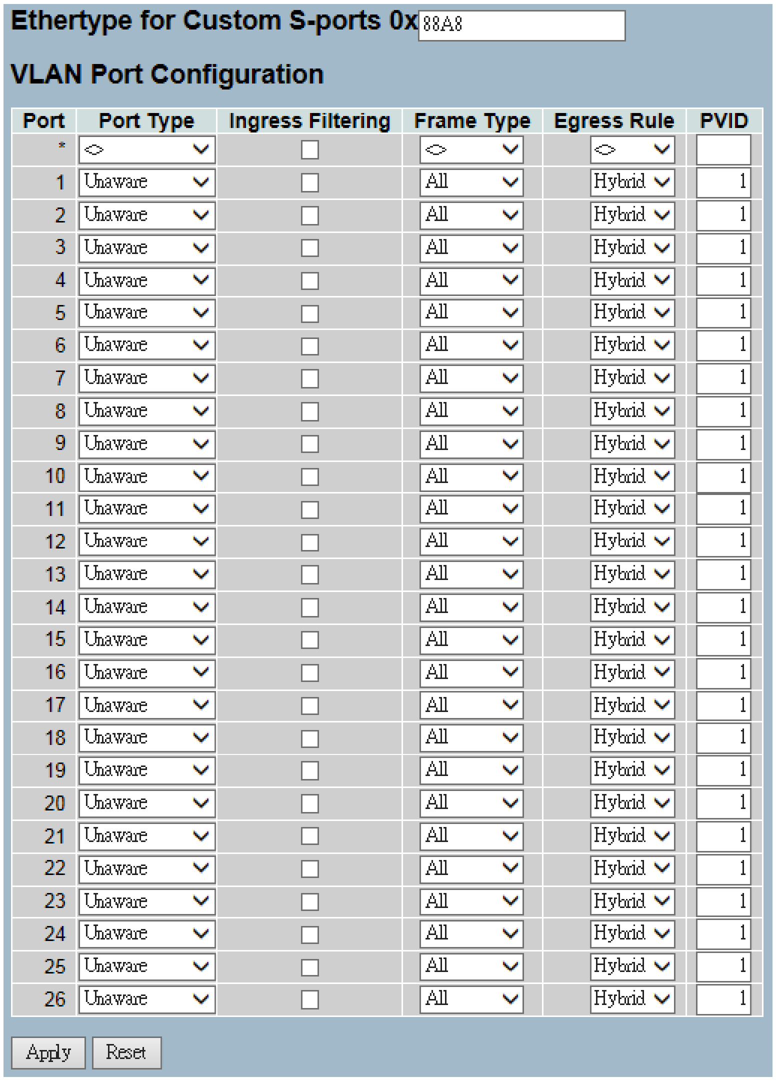
3-10.2 Ports

This sections provides information on how to configure all parameters for each port in the VLAN port setting. These parameters involved two parts: ingress rule and egress rule. Ingress process is affected by functions such as port type, ingress filtering, frame type, and PVID. Egress process is affected by functions such as port type, egress rule, and PVID.

Web Interface

To configure VLAN port configuration in the web interface:

1. Click the VLAN Port Configuration.
2. Specify the VLAN port configuration parameters.
3. Click save.



Ethertype for Custom S-ports 0x 88A8

VLAN Port Configuration

Port	Port Type	Ingress Filtering	Frame Type	Egress Rule	PVID
*	<>	□	<>	<>	
1	Unaware	□	All	Hybrid	1
2	Unaware	□	All	Hybrid	1
3	Unaware	□	All	Hybrid	1
4	Unaware	□	All	Hybrid	1
5	Unaware	□	All	Hybrid	1
6	Unaware	□	All	Hybrid	1
7	Unaware	□	All	Hybrid	1
8	Unaware	□	All	Hybrid	1
9	Unaware	□	All	Hybrid	1
10	Unaware	□	All	Hybrid	1
11	Unaware	□	All	Hybrid	1
12	Unaware	□	All	Hybrid	1
13	Unaware	□	All	Hybrid	1
14	Unaware	□	All	Hybrid	1
15	Unaware	□	All	Hybrid	1
16	Unaware	□	All	Hybrid	1
17	Unaware	□	All	Hybrid	1
18	Unaware	□	All	Hybrid	1
19	Unaware	□	All	Hybrid	1
20	Unaware	□	All	Hybrid	1
21	Unaware	□	All	Hybrid	1
22	Unaware	□	All	Hybrid	1
23	Unaware	□	All	Hybrid	1
24	Unaware	□	All	Hybrid	1
25	Unaware	□	All	Hybrid	1
26	Unaware	□	All	Hybrid	1

Figure 3-10.2: The VLAN Port Configuration

Parameter Description

Ethertype for Custom S-ports: This field specifies the ethertype used for custom S-ports while the custom s-ports are enabled. This is a global setting for all the custom S-ports. Custom Ethertype enables the user to change the Ethertype value on a port to any value, in order to support network devices which do not use the standard 0x8100 Ethertype field value on 802.1Q-tagged or 802.1p-tagged frames.

Port: This indicates the port number of each port.

Port Type: A port can be one of the following types: Unaware, C-port, S-port, and S-custom-port.

	Ingress action	**Egress action**
Unaware **The function of Unaware can be used for 802.1QinQ (double tag).**	When the port received untagged frames, an untagged frame obtain a tag (based on PVID) and is forwarded. When the port received tagged frames, 1. If the tagged frame is TPID=0x8100, it become a double-tag frame and is forwarded. 2. If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	The TPID, of frame transmitted by unaware port, will be set to 0x8100.
C-port	When the port received untagged frames, an untagged frame obtain a tag (based on PVID) and is forwarded. When the port received tagged frames, 1. If an tagged frame is TPID=0x8100, it is forwarded. 2. If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	The TPID, of frame transmitted by C-port, will be set to 0x8100.
S-port	When the port received untagged frames, an untagged frame obtain a tag (based on PVID) and is forwarded. When the port received tagged frames, 1. If an tagged frame is TPID=0x88A8, it is forwarded. 2. If the TPID of tagged frame is not 0x88A8 (ex. 0x8100), it will be discarded.	The TPID, of frame transmitted by S-port, will be set to 0x88A8.
S-custom-port	When the port received untagged frames, an untagged frame obtain a tag (based on PVID) and is forwarded. When the port received tagged frames, 1. If an tagged frame is TPID=0x88A8, it is forwarded. 2. If the TPID of tagged frame is not 0x88A8 (ex. 0x8100), it will be discarded.	The TPID, of frame transmitted by S-custom-port, will be set to an self-customized value and can be set by the user using the column of **Ethertype for Custom S-ports.**

Ingress Filtering: This enables ingress filtering on a port. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN group of the frame, the frame is discarded (does not forward).

If ingress filtering is disabled and the ingress port is not a member of the classified VLAN group of the frame, the frame is still forwarded.

By default, ingress filtering is disabled.

Frame Type: This determines whether the port accepts all frames or only tagged/untagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. By default, the field is set to all.

Egress Rule: This determines what device the port connects to. If the port connects to VLAN-unaware devices (terminal/work station), access link should be used. If the port connect to VLAN-aware devices (switch connect to switch), trunk link should be used. Hybrid link is used for more flexible application.

- **Hybrid:** If the tag of tagged frame is as the same as PVID, the tag of the frame will be removed. The frame become an untagged frame and transmitted.
- Any other tagged frame whose tag value is different from PVID are transmitted directly.
- **Trunk:** All tagged frames with any tag value are transmitted.
- **Access:** The tag of any tagged frame will be removed to become an untagged frame. These untagged frames will be transmitted.

PVID: This configures the port VLAN identifier. The allowed values are 1 through 4094. The default value is 1.

When the port received an untagged frame, the port will give a tag to the frame based on the value of PVID and the frame become tagged frame.

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

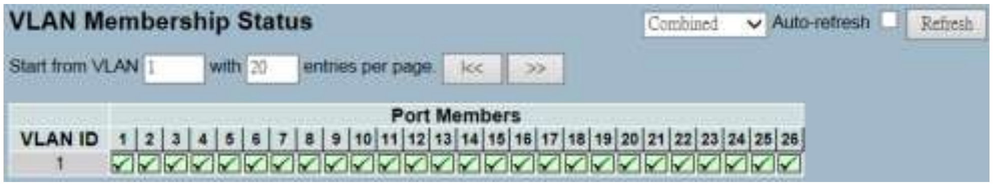
3-10.3 Switch Status

The switch status gathers information of all VLAN status and reports it by the order of Static, NAS, MVRP, MVP, Voice VLAN, MSTP, and GVRP Combined.

Web Interface

To display VLAN membership status in the web interface:

1. Click VLAN membership.
2. Specify the Static, NAS, MVRP, MVP, Voice VLAN, MSTP, and GVRP Combined.
3. Display membership information.



VLAN Membership Status

Combined ▾ Auto-refresh □ Refresh

Start from VLAN 1 with 20 entries per page. |<< >>

VLAN ID	Port Members																									
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Figure 3-10.3: The VLAN Membership Status

Parameter Description

VLAN User (scroll to select one kind VLAN user):
The VLAN user module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configurations such as PVID and UVID. Currently, we support the following VLAN user types:

- **CLI/Web/SNMP:** These are referred to as static.
- **NAS:** The NAS provides port-based authentication, which involves communications between a supplicant, authenticator, and an authentication server.
- **Voice VLAN:** Voice VLAN is a VLAN configured specifically for voice traffic, typically originating from IP phones.
- **MVR:** MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.
- **MSTP:** The 802.1s multiple spanning tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

VLAN ID: This indicates the ID of this particular VLAN.

Port Members: A row of check boxes for each port is displayed for each VLAN ID.

- If a port is included in a VLAN, an image ✓ will be displayed.
- If a port is included in a forbidden port list, an image ✗ will be displayed.
- If a port is included in a forbidden port list and dynamic VLAN user register VLAN on same forbidden port, then the conflict port will be displayed as ✗.

VLAN Membership: The VLAN membership status page shall show the current VLAN port members for all VLANs configured by a selected VLAN user (selection shall be allowed by a combo box). When **all** VLAN users are selected, it shall show this information for all the VLAN users. This is the default setting. VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.

Auto-Refresh: Click to automatically refresh the information.

Upper Right Icon (Refresh): Click to manually refresh the information.

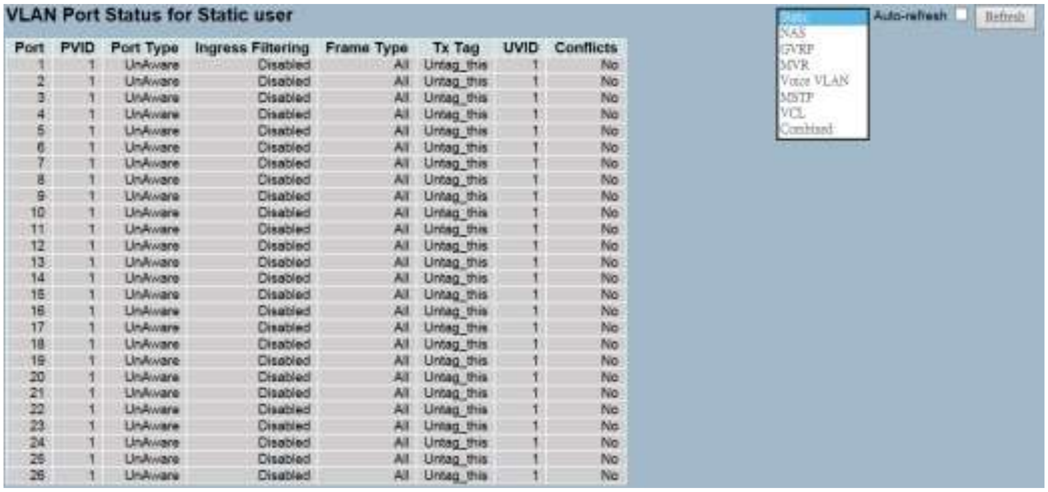
3-10.4 Port Status

The port status gathers information of all VLAN status and reports it by the order of Static, NAS, MVRP, MVP, Voice VLAN, MSTP, and GVRP Combined.

Web Interface

To display VLAN port status in the web interface:

1. Click VLAN Port Status.
2. Specify the Static, NAS, MVRP, MVP, Voice VLAN, MSTP, and GVRP Combined.
3. Display port status information.



VLAN Port Status for Static user

Port	PVID	Port Type	Ingress Filtering	Frame Type	Tx Tag	UVID	Conflicts
1	1	UnAware	Disabled	All	Untag_this	1	No
2	1	UnAware	Disabled	All	Untag_this	1	No
3	1	UnAware	Disabled	All	Untag_this	1	No
4	1	UnAware	Disabled	All	Untag_this	1	No
5	1	UnAware	Disabled	All	Untag_this	1	No
6	1	UnAware	Disabled	All	Untag_this	1	No
7	1	UnAware	Disabled	All	Untag_this	1	No
8	1	UnAware	Disabled	All	Untag_this	1	No
9	1	UnAware	Disabled	All	Untag_this	1	No
10	1	UnAware	Disabled	All	Untag_this	1	No
11	1	UnAware	Disabled	All	Untag_this	1	No
12	1	UnAware	Disabled	All	Untag_this	1	No
13	1	UnAware	Disabled	All	Untag_this	1	No
14	1	UnAware	Disabled	All	Untag_this	1	No
15	1	UnAware	Disabled	All	Untag_this	1	No
16	1	UnAware	Disabled	All	Untag_this	1	No
17	1	UnAware	Disabled	All	Untag_this	1	No
18	1	UnAware	Disabled	All	Untag_this	1	No
19	1	UnAware	Disabled	All	Untag_this	1	No
20	1	UnAware	Disabled	All	Untag_this	1	No
21	1	UnAware	Disabled	All	Untag_this	1	No
22	1	UnAware	Disabled	All	Untag_this	1	No
23	1	UnAware	Disabled	All	Untag_this	1	No
24	1	UnAware	Disabled	All	Untag_this	1	No
25	1	UnAware	Disabled	All	Untag_this	1	No
26	1	UnAware	Disabled	All	Untag_this	1	No

Figure 3-10.4: The VLAN Port Status for Static User

Parameter Description

Port: This is the logical port for the settings contained in the same row.

PVID: This shows the VLAN identifier for that port. The allowed values are 1 through 4095. The default value is 1.

Port Type: This shows the port type. Port type can be any of unaware, C-port, S-port, and custom S-port.

If port type is unaware, all frames are classified to the port VLAN ID and tags are not removed. C-port is customer port. S-port is service port. Custom S-port is S-port with custom TPID.

Ingress Filtering: This shows the ingress filtering on a port. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN, the frame is discarded.

Frame Type: This shows whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on that port are discarded.

Tx Tag: This shows egress filtering frame status, whether it’s tagged or untagged.

UVID: This shows the UVID (untagged VLAN ID). Port's UVID determines the packet's behaviour at the egress side.

Conflicts: This shows status of conflicts whether exists or not. When a volatile VLAN user requests to set the VLAN membership or VLAN port configuration, the following conflicts can occur:

- Functional conflicts between features.
- Conflicts due to hardware limitation.
- Direct conflict between user modules.

Auto-Refresh: Click to automatically refresh the information.

Upper Right Icon (Refresh): Click to manually refresh the information.

3-10.5 Private VLANs

In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.

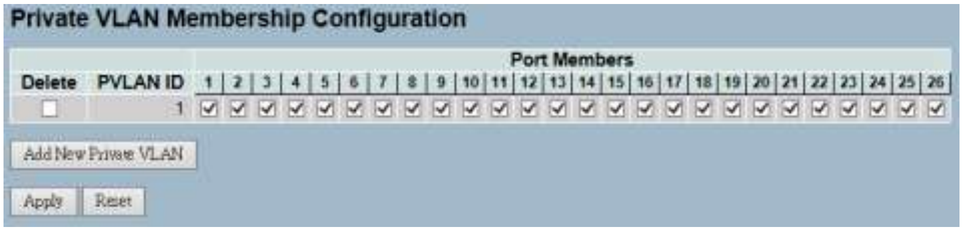
3-10.5.1 Private VLANs Membership

This section provides information on adding, deleting, monitoring, and modifying the private VLAN membership configurations. Port members of each private VLAN can also be added or removed. Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and private VLAN IDs can be identical. A port must be a member of both a VLAN and a private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and private VLAN 1. A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple private VLANs.

Web Interface

To configure private VLAN configuration in the web interface:

1. Click add new Private VLAN configuration.
2. Specify the private VLAN ID and port members.
3. Click save.



Private VLAN Membership Configuration

		Port Members																									
Delete	PVLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
☐	1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Figure 3-10.5.1: The Private VLAN Membership Configuration

Parameter Description	**Delete:** Click to delete a private VLAN entry. **Private VLAN ID:** This indicates the ID of this particular private VLAN. **Port Members :** A row of check boxes for each port is displayed for each private VLAN ID. Click to include a port in a private VLAN. Uncheck the box to remove or exclude the port from the private VLAN. By default, no ports are members and all boxes are unchecked. **Adding a New Private VLAN:** Click to add a new private VLAN ID. An empty row is added to the table and the private VLAN can be configured as needed. **Buttons:** • **Save** – Click to save changes. • **Reset-** Click to restore default settings.

3-10.5.2 Port Isolation

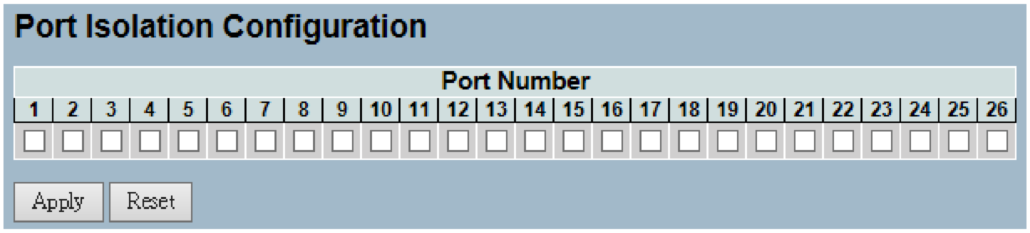
Port isolation provides for an apparatus and method to isolate ports on layer 2 switches on the same VLAN to restrict traffic flow. The apparatus comprises a switch having said plurality of ports, each port configured as a protected port or a non-protected port. An address table memory stores an address table having a destination address and port number pair. A forwarding map generator creates a forwarding map, which is responsive to a destination address of a data packet. The method for isolating ports on a layer 2 switch comprises configuring each of the ports on the layer 2 switch as a protected port or a non-protected port. A destination address on an data packet is matched with a physical address on said layer 2 switch and a forwarding map is generated for the data packet based upon the destination address on the data packet. The data packet is then sent to the plurality of ports pursuant to the forwarding map generated based upon whether the ingress port was configured as a protected or non-protected port.

This section is used for enabling or disabling port isolation on ports in a Private VLAN.A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.

Web Interface

To configure port isolation configuration in the web interface:

1. Click VLAN and Port Isolation.
2. Choose which port to enable port isolation on.
3. Click save.



Port Isolation Configuration

Port Number																									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Figure 3-10.5.2: The Port Isolation Configuration

Parameter Description

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

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

3-10.6 Mac-based VLAN

MAC address-based VLAN decides the VLAN for forwarding an untagged frame, based on the source MAC address of the frame.

A most common way of grouping VLAN members is by port, hence the name port-based VLAN. Typically, the device adds the same VLAN tag to untagged packets that are received through the same port. Later on, these packets can be forwarded in the same VLAN. Port-based VLAN is easy to configure and applies to networks where the locations of terminal devices are relatively fixed. As mobile office and wireless network access gain more popularity, the ports that terminal devices use to access the networks are very often non-fixed. A device may access a network through port A this time, but through port B the next time. If port A and port B belong to different VLANs, the device will be assigned to a different VLAN the next time it accesses the network. As a result, it will not be able to use the resources in the old VLAN. If port A and port B belong to the same VLAN, after terminal devices access the network through port B, they will have access to the same resources as those accessing the network through port A do. This brings security issues. To provide user access and ensure data security in the mean time, the MAC-based VLAN technology is developed.

MAC-based VLANs group VLAN members by MAC address. With MAC-based VLAN configured, the device adds a VLAN tag to an untagged frame according to its source MAC address. MAC-based VLANs are mostly used in conjunction with security technologies such as 802.1X to provide secure and flexible network access for terminal devices.

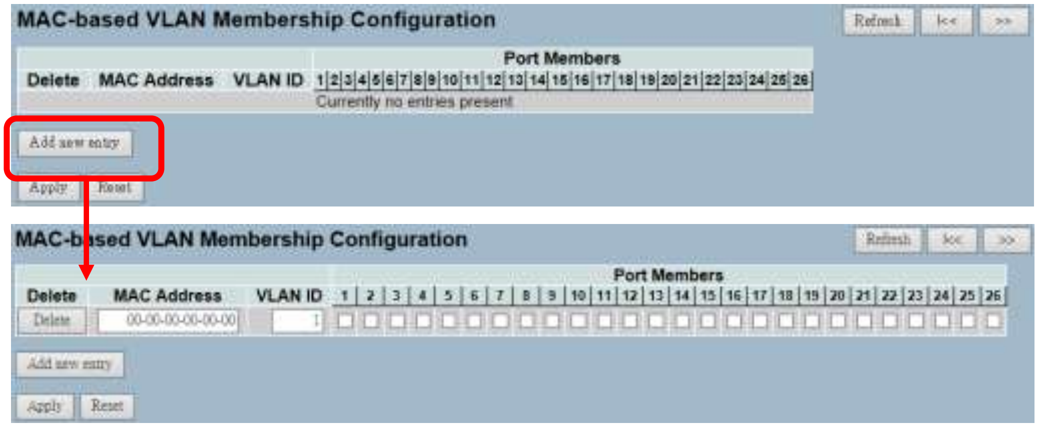
3-10.6.1 Configuration

This section provides information on adding, deleting, and configuring static MAC-based VLAN entries. You can also assign the entries to different ports.

Web Interface

To configure MAC address-based VLAN configuration in the web interface:

1. Click MAC address-based VLAN configuration and add new entry.
2. Specify the MAC address and VLAN ID.
3. Click save.



MAC-based VLAN Membership Configuration

Delete	MAC Address	VLAN ID	Port Members																									
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
			Currently no entries present																									

MAC-based VLAN Membership Configuration

Delete	MAC Address	VLAN ID	Port Members																									
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Delete	00-00-00-00-00-00	1	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Figure 3-10.6.1: The MAC-based VLAN Membership Configuration

Parameter Description

Delete: Click to delete a MAC-based VLAN entry.

MAC Address: This indicates the MAC address.

VLAN ID: This indicates the VLAN ID.

Port Members: A row of check boxes for each port is displayed for each MAC-based VLAN entry. Check the box to include a port in a MAC-based VLAN. Uncheck the box to remove or exclude the port from the MAC-based VLAN. By default, no ports are members and all boxes are unchecked.

Adding a New MAC-based VLAN

Click to add a new MAC-based VLAN entry. An empty row is added to the table and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. The legal values for a VLAN ID are 1 through 4095.

The MAC-based VLAN entry is enabled on the selected switch unit when you click on "Save". A MAC-based VLAN without any port members on any unit will be deleted when you click "Apply". The “Delete” button can be used to undo the addition of new MAC-based VLANs.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

3-10.6.2 Status

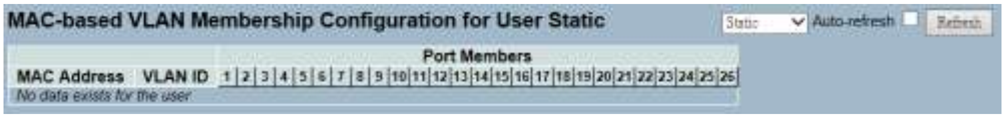
This section provides information on MAC-based VLAN entries configured by various MAC-based VLAN users. Currently, the following VLAN user types are supported:

NAS: NAS provides port-based authentication, which involves communications between a supplicant, authenticator, and an authentication server.

Web Interface

To display MAC-based VLAN configured in the web interface:

1. Click MAC-based VLAN Status.
2. Specify the static NAS combined.
3. Display MAC-based information.



MAC-based VLAN Membership Configuration for User Static

		Port Members																									
MAC Address	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
No data exists for the user																											

Figure 3-10.6.2: The MAC-based VLAN Membership Status for User Static

Parameter Description

MAC Address: This indicates the MAC address.

VLAN ID: This indicates the VLAN ID.

Port Members: These are port members of the MAC-based VLAN entry.

Auto-Refresh: Click to automatically refresh the information.

Upper Right Icon (Refresh): Click to manually refresh the information.

3-10.7 Protocol-based VLAN

This section provides information on the protocol-based VLAN. The switch supports LLC and SNAP.

LLC: The logical link control (LLC) data communication protocol layer is the upper sub-layer of the data link layer (which is itself layer 2, just above the physical layer) in the seven-layer OSI reference model. It provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX, Decnet, and Appletalk) to coexist within a multipoint network and to be transported over the same network media. It can also provide flow control and automatic repeat request (ARQ) error management mechanisms.

SNAP: The subnetwork access protocol (SNAP) is a mechanism for multiplexing on networks using IEEE 802.2 LLC. More protocols 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 spaces. It is used with IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.11, other IEEE 802 physical network layers, and non-IEEE 802 physical network layers such as FDDI that uses 802.2 LLC.

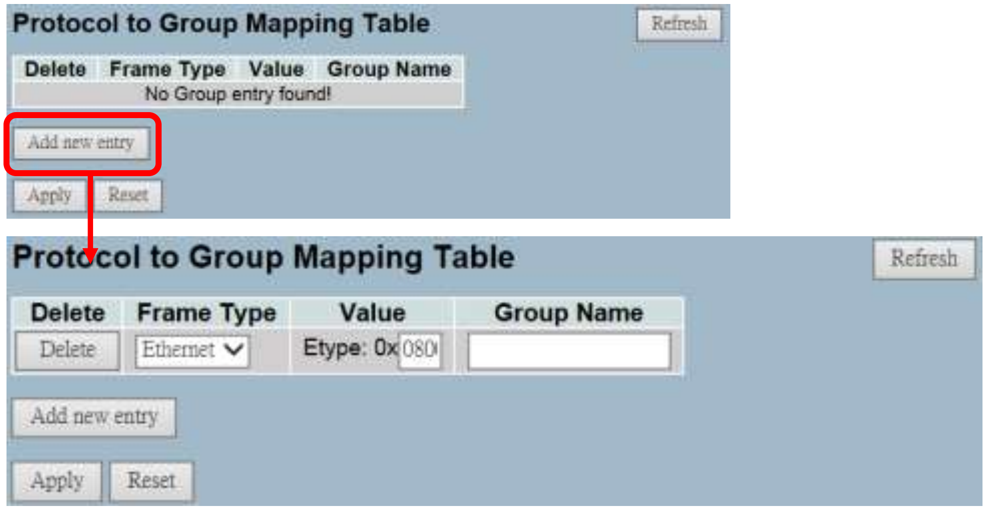
3-10.7.1 Protocol to Group

This sections provides information on adding new protocols to group name (unique for each group), and mapping, viewing, and deleting mapped entries.

Web Interface

To configure protocol-based VLAN configuration in the web interface:

1. Click Protocol-based VLAN configuration and add new entry.
2. Specify the Ethernet LLC SNAP protocol and group name.
3. Click save.



Protocol to Group Mapping Table

Delete	Frame Type	Value	Group Name
No Group entry found!			

Protocol to Group Mapping Table

Delete	Frame Type	Value	Group Name
Delete	Ethernet	Etype: 0x 0800	

Figure 3-10.7.1: The Protocol to Group Mapping Table

Parameter Description

Delete: Click to delete a protocol to group name map entry.

Frame Type: Frame type can have one of the following values:

1. Ethernet
2. LLC
3. SNAP

> **NOTE:** In regards to changing the frame type field, valid value of the following text field will vary depending on the new frame type you selected.

Value: Valid value that can be entered in this text field depends on the option selected from the the preceding frame type selection menu.

Below is the criteria for three different frame types:

1. **For Ethernet:** Values in the text field when Ethernet is selected as a frame type is called etype. Valid values for etype ranges from 0x0600 to 0xffff.
2. **For LLC:** Valid value in this case is comprised of two different sub-values.
   a. **DSAP:** 1-byte Long String (0x00-0xff)
   b. **SSAP:** 1-byte Long String (0x00-0xff)

3. **For SNAP:** Valid value for SNAP is also comprised of two different sub-values.
    a. **OUI:** OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00 to 0xff.
    b. **PID:** If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP. If the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP.
       In other words, if value of OUI field is 00-00-00, then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00, then valid value of PID will be any value from 0x0000 to 0xffff.

Group Name: A valid group name is a unique 16-character long string for every entry that consists a combination of alphabets (a-z or A-Z) and integers (0-9).

NOTE: Special character and underscore(_) are not allowed.

Adding a New Group to VLAN Mapping Entry: Click to add a new entry in mapping table. An empty row is added to the table. Frame type, value, and group name can be configured as needed. The button can be used to undo the addition of new entry.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

Upper Right Icon (Refresh): Click to manually refresh the protocol group mapping information.

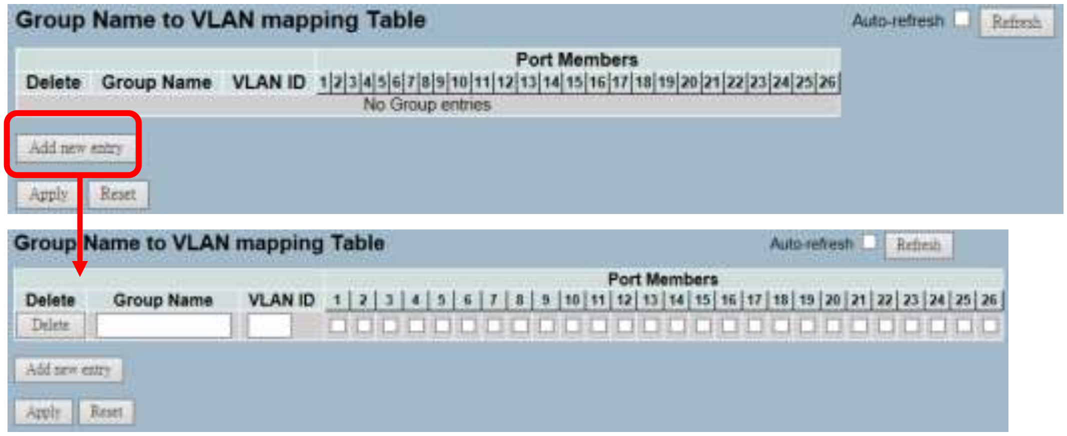
3-10.7.2 Group to VLAN

This section provides information on mapping a configured group name to a VLAN.

Web Interface

To display group name to VLAN mapping table configured in the web interface:

1. Click Group Name VLAN configuration and add new entry.
2. Specify the group name and VLAN ID.
3. Click save.



Group Name to VLAN mapping Table

Auto-refresh □ Refresh

Delete	Group Name	VLAN ID	Port Members																									
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
No Group entries																												

Add new entry

Apply Reset

Group Name to VLAN mapping Table

Auto-refresh □ Refresh

Delete	Group Name	VLAN ID	Port Members																									
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Delete			□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Add new entry

Apply Reset

Figure 3-12.7.2: The Group Name of VLAN Mapping Table

Parameter Description

Delete: Click to delete a group name to VLAN map entry.

Group Name: A valid group name is a string of atmost 16 characters that consists a combination of alphabets (a-z or A-Z) and integers (0-9). No special character is allowed. Whichever group name you’re trying to map to, a VLAN must be present in protocol and must not be preused by other existing mapping entries.

VLAN ID: This indicates the ID to which group name will be mapped to. A valid VLAN ID ranges from 1 to 4095.

Port Members: A row of check boxes for each port is displayed for each group name to VLAN ID mapping. Check the box to include a port in a mapping. Uncheck the box to remove or exclude the port from the mapping. By default, no ports are members and all boxes are unchecked.

Adding a New Group to VLAN Mapping Entry: Click to add a new entry in mapping table. An empty row is added to the table. The group name, VLAN ID, and port members can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The “Delete” button can be used to undo the addition of new entry.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

Auto-Refresh: Click to automatically refresh the information.

Upper Right Icon (Refresh): Click to manually refresh the information.

3-10.8 IEEE 802.1 QinQ (double-tag) Configuration

Service providers can use Q-in-Q to transparently pass Layer 2 VLAN traffic from a customer site, through the service provider network, to another customer site without removing or changing the customer VLAN tags.

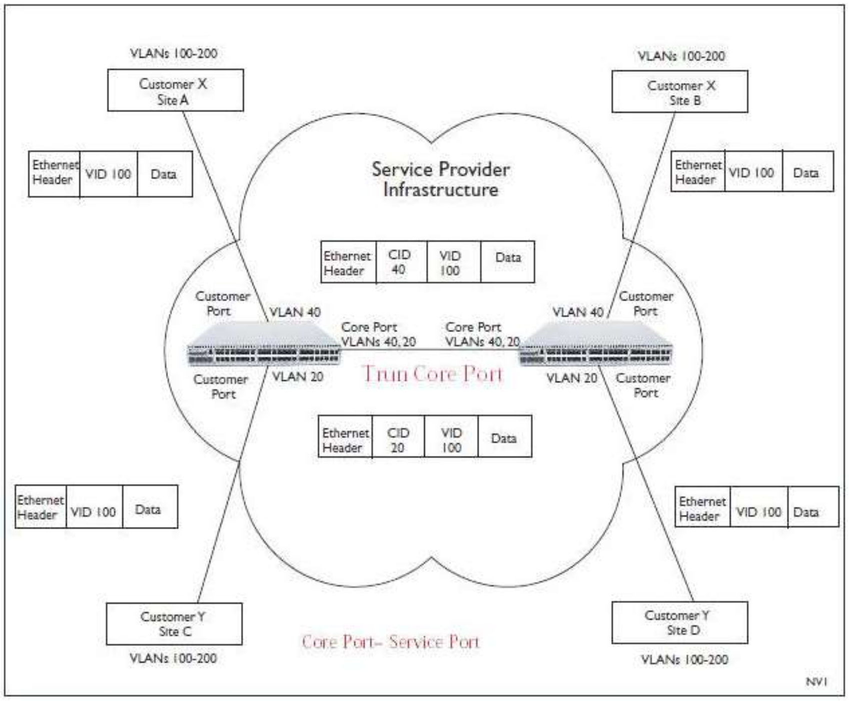
The double Q-in-Q tags can indicate different information. The inner tag indicates the user and the outer tag indicates carrier provider. The Q-in-Q packet with two tags can traverse the carrier's network and the inner tag is transmitted transparently.

Scenario :

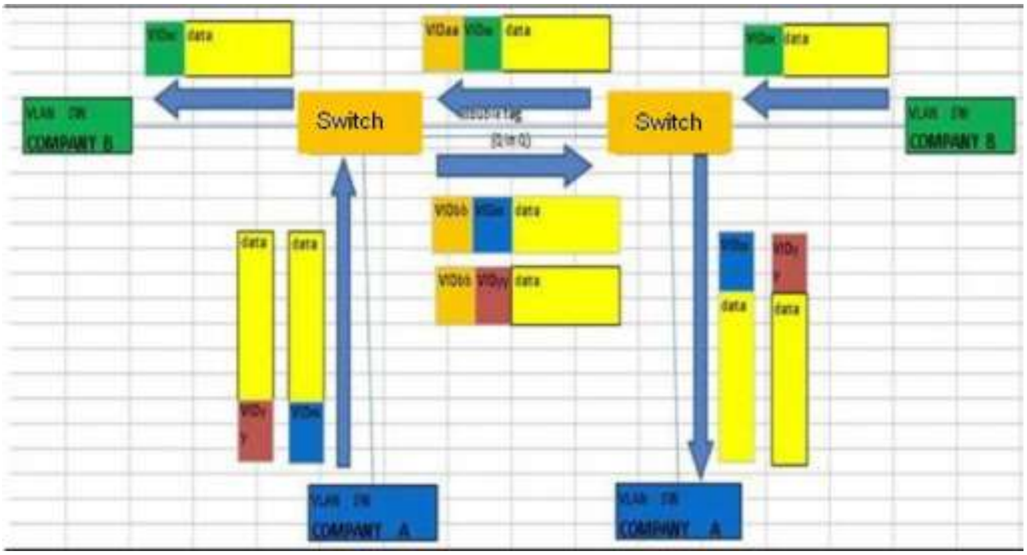
The switch will be used for leased line service.

They are already using tag VLAN (802.1q), so they would like to add another tag without changing existing VLAN.

Typical Application :



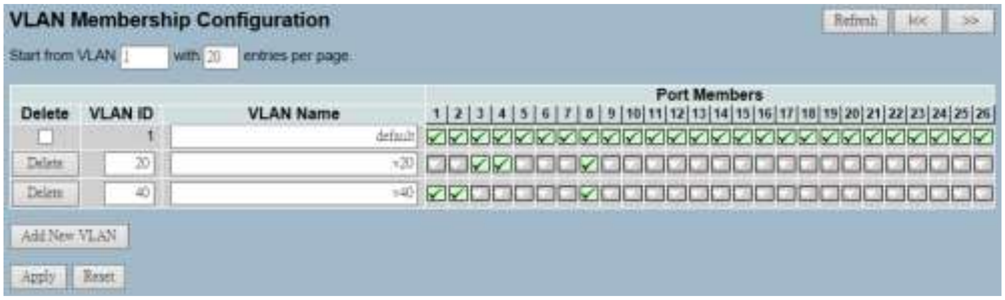
An Abstract Illustration To Above Application:



Configure Steps:

Step 1: Create VLAN 20 and VLAN 40

- Configure Port 3. Port 4 and Port 8 are belong to VLAN 20.
- Configure Port 1. Port 2 and Port 8 are belong to VLAN 40.
- Port 8 is uplink port.
- The above setting is configured at SW1 (left side) and SW2 (right side).



VLAN Membership Configuration

Start from VLAN 1 with 20 entries per page.

			Port Members																									
Delete	VLAN ID	VLAN Name	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
□	1	default	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Delete	20	v20	□	□	☑	☑	□	□	□	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Delete	40	v40	☑	☑	□	□	□	□	□	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Step 2 : Configure PVID

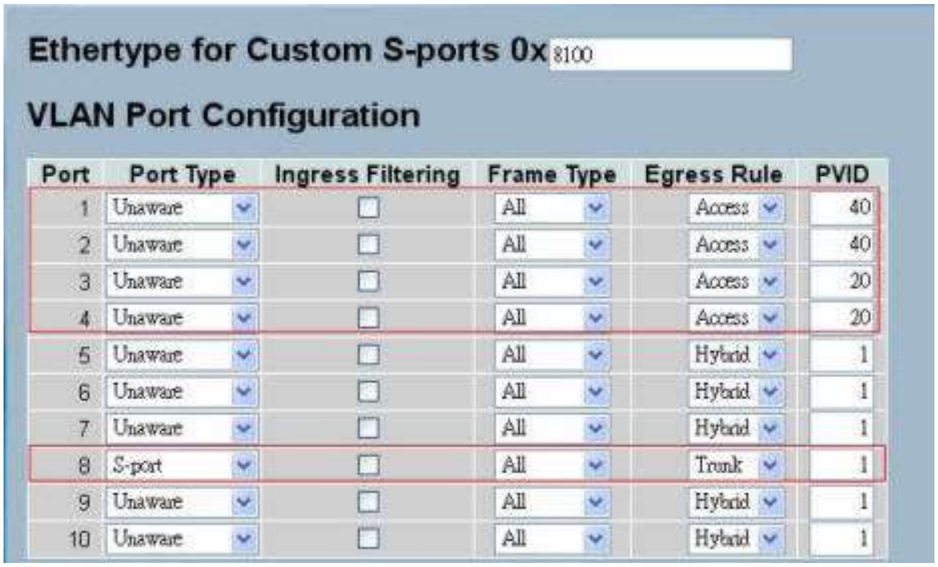
- Port 1 and Port 2 are PVID=40 and their port role are VLAN access mode.
- Port 3 and Port 4 are PVID=20 and their port role are VLAN access mode.
- The port role of Port 8 is VLAN trunk mode.

Step 3 : Configure Port Type to "Unaware" at Port 1 to Port 4.

Step 4 : Configure Port Type to “S-Port“ at Port 8.

The uplink port [port 8] can be set as C-Port or S-Port. The uplink port on the both switches must be set the same type. We set S-Port to S-Port as an example.

Q-in-Q belong to the tag-based mode. However, it would treat all frames as the untagged ones. This means that tag with PVID will be added into all packets. Then, these packets will be forwarded as tag-based VLAN. So, the incoming packets with tag will become the double-tag ones.



Ethertype for Custom S-ports 0x 8100

VLAN Port Configuration

Port	Port Type	Ingress Filtering	Frame Type	Egress Rule	PVID
1	Unaware	□	All	Access	40
2	Unaware	□	All	Access	40
3	Unaware	□	All	Access	20
4	Unaware	□	All	Access	20
5	Unaware	□	All	Hybrid	1
6	Unaware	□	All	Hybrid	1
7	Unaware	□	All	Hybrid	1
8	S-port	□	All	Trunk	1
9	Unaware	□	All	Hybrid	1
10	Unaware	□	All	Hybrid	1

3-11 Voice VLAN

Voice VLAN is VLAN configured specifically for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data to ensure the transmission priority of voice traffic and voice quality.

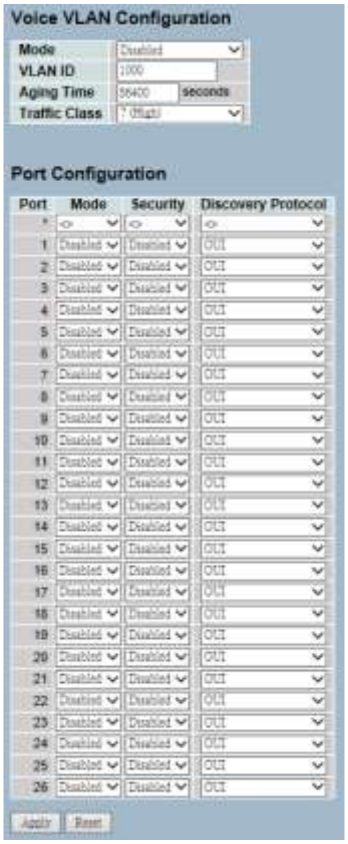
3-11.1 Configuration

The voice VLAN feature enables voice traffic forwarding on the voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice and one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI.

Web Interface

To configure Voice VLAN in the web interface:

1. Select “Enabled” in the Voice VLAN Configuration.
2. Specify VLAN ID aging time traffic class.
3. Specify (port mode, security, discovery protocol) in the port configuration.
2. Click save.



Voice VLAN Configuration

Mode	Disabled	
VLAN ID	1000	
Aging Time	86400	seconds
Traffic Class	7 (High)	

Port Configuration

Port	Mode	Security	Discovery Protocol
*	<>	<>	<>
1	Disabled	Disabled	OUI
2	Disabled	Disabled	OUI
3	Disabled	Disabled	OUI
4	Disabled	Disabled	OUI
5	Disabled	Disabled	OUI
6	Disabled	Disabled	OUI
7	Disabled	Disabled	OUI
8	Disabled	Disabled	OUI
9	Disabled	Disabled	OUI
10	Disabled	Disabled	OUI
11	Disabled	Disabled	OUI
12	Disabled	Disabled	OUI
13	Disabled	Disabled	OUI
14	Disabled	Disabled	OUI
15	Disabled	Disabled	OUI
16	Disabled	Disabled	OUI
17	Disabled	Disabled	OUI
18	Disabled	Disabled	OUI
19	Disabled	Disabled	OUI
20	Disabled	Disabled	OUI
21	Disabled	Disabled	OUI
22	Disabled	Disabled	OUI
23	Disabled	Disabled	OUI
24	Disabled	Disabled	OUI
25	Disabled	Disabled	OUI
26	Disabled	Disabled	OUI

Figure 3-11.1: The Voice VLAN Configuration

Parameter Description

Mode: This indicates the voice VLAN mode operation. You must disable the MSTP feature before you enable voice VLAN to avoid ingress filtering conflicts. Possible modes are:

- **Enabled:** This enables voice VLAN mode operation.
- **Disabled:** This disables voice VLAN mode operation.

VLAN ID: This indicates the voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID, etc. The allowed range is 1 to 4095.

Aging Time: This indicates the voice VLAN secure learning aging time. The allowed range is 10 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time; 2 * age_time] interval.

Traffic Class: This indicates the voice VLAN traffic class. All traffic on the voice VLAN will apply this class.

Port Mode: This indicates the voice VLAN port mode.

When the port mode isn't equal disabled, you must disable theMSTP feature before you enable voice VLAN to avoid ingress filtering conflicts.

Possible port modes are:

- **Disabled:** This disjoins from the voice VLAN.
- **Auto:** This enables auto detect mode. It detects whether there is a VoIP phone attached to the specific port and configures the voice VLAN members automatically.
- **Forced:** This forces join to voice VLAN.

Port Security: This indicates the voice VLAN port security mode. When the function is enabled, all non-telephonic MAC addresses in the voice VLAN will be blocked for 10 seconds. Possible port modes are:

- **Enabled:** This enables voice VLAN security mode operation.
- **Disabled:** This disables voice VLAN security mode operation.

Port Discovery Protocol: This indicates the voice VLAN port discovery protocol. It will only work when auto-detect mode is enabled. You should enable the LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart auto detect process. Possible discovery protocols are:

- **OUI:** This detects the telephony device by OUI address.
- **LLDP:** This detects the telephony device by LLDP.
- **Both:** This is both OUI and LLDP.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

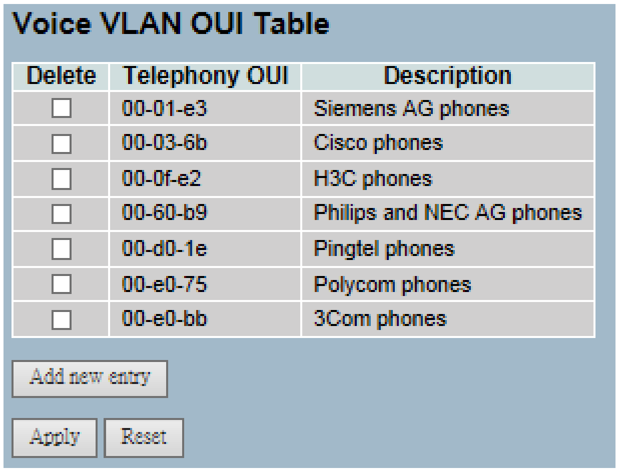
3-11.2 OUI

The section provides information on the voice VLAN OUI table. The maximum entry number for the table is 16. Modifying the OUI table will restart auto detection of OUI process.

Web Interface

To configure voice VLAN OUI table in the web interface:

1. Select "Add new entry" and "Delete"in the voice VLAN OUI table.
2. Specify telephony OUI, description, and other information.
3. Click save.



Voice VLAN OUI Table

Delete	Telephony OUI	Description
□	00-01-e3	Siemens AG phones
□	00-03-6b	Cisco phones
□	00-0f-e2	H3C phones
□	00-60-b9	Philips and NEC AG phones
□	00-d0-1e	Pingtel phones
□	00-e0-75	Polycom phones
□	00-e0-bb	3Com phones

Figure 3-11.2: The Voice VLAN OUI Table

Parameter Description

Delete: Click to remove the entry.

Telephony OUI: A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).

Description: This is the description of OUI address. It describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.

Add New Entry: Click to add a new entry in voice VLAN OUI table.
Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

NOTE: All non-telephonic MAC addresses in the voice VLAN will be blocked for 10 seconds.

For example: When the packets enter the port to add a new OUI entry, it can help this OUI match current packets. Once it's found, the packet will be forwarded.

3-12 GARP

The generic attribute registration protocol (GARP) provides a generic framework whereby devices in a bridged LAN (end stations and switches) can register and de-register attribute values with each other (VLAN identifiers). In doing so, the attributes are propagated to devices in the bridged LAN and these devices form a reachability tree that is a subset of an active topology. GARP defines the architecture, rules of operation, state machines, and variables for the registration and de-registration of attribute values.

A GARP participation in a switch or an end station consists of a GARP application component and a GARP information declaration (GID) component associated with each port or the switch. The propagation of information between GARP participants for the same application in a bridge is carried out by the GARP information propagation (GIP) component. Protocol exchanges take place between GARP participants by means of LLC type 1 services, using the group MAC address and PDU format defined for the GARP application concerned.

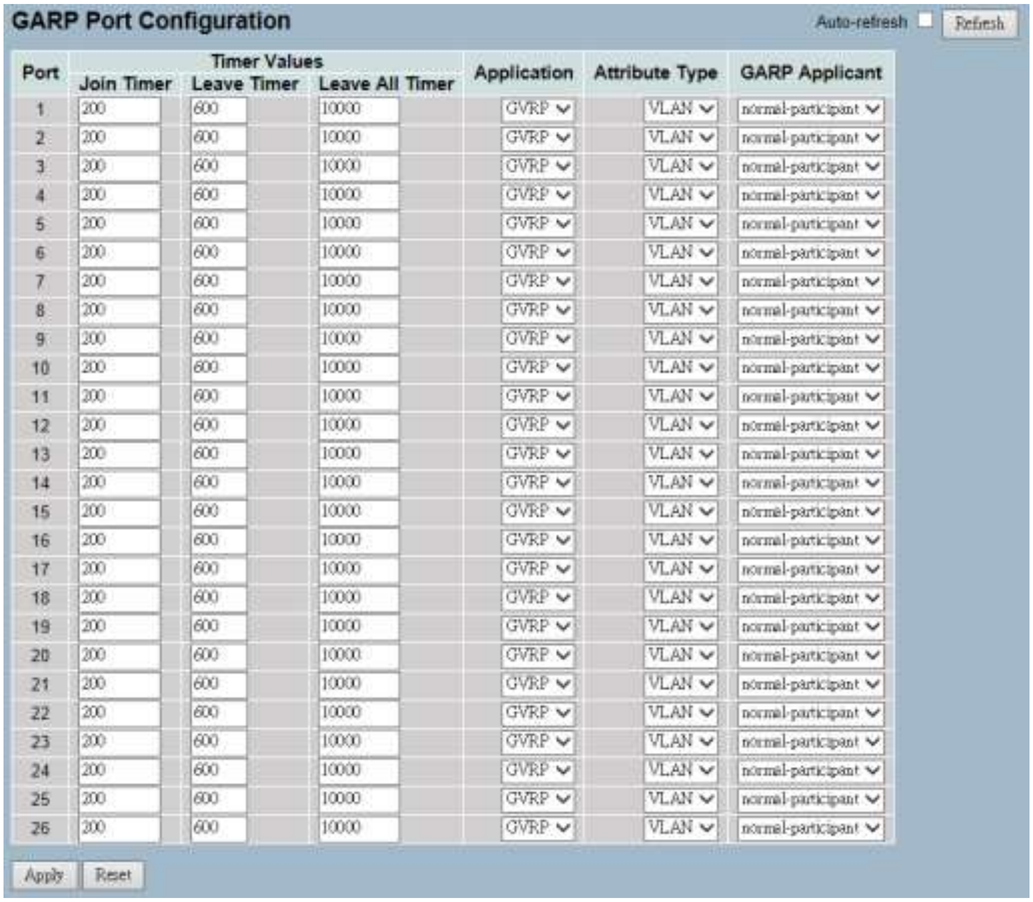
3-12.1 Configuration

This section provides information on basic GARP configuration settings for all ports.

Web Interface

To configure GARP port configuration in the web interface:

1. Click GARP configure.
2. Specify GARP configuration parameters.
3. Click save.



GARP Port Configuration

Port	Timer Values			Application	Attribute Type	GARP Applicant
	Join Timer	Leave Timer	Leave All Timer			
1	200	600	10000	GVRP	VLAN	normal-participant
2	200	600	10000	GVRP	VLAN	normal-participant
3	200	600	10000	GVRP	VLAN	normal-participant
4	200	600	10000	GVRP	VLAN	normal-participant
5	200	600	10000	GVRP	VLAN	normal-participant
6	200	600	10000	GVRP	VLAN	normal-participant
7	200	600	10000	GVRP	VLAN	normal-participant
8	200	600	10000	GVRP	VLAN	normal-participant
9	200	600	10000	GVRP	VLAN	normal-participant
10	200	600	10000	GVRP	VLAN	normal-participant
11	200	600	10000	GVRP	VLAN	normal-participant
12	200	600	10000	GVRP	VLAN	normal-participant
13	200	600	10000	GVRP	VLAN	normal-participant
14	200	600	10000	GVRP	VLAN	normal-participant
15	200	600	10000	GVRP	VLAN	normal-participant
16	200	600	10000	GVRP	VLAN	normal-participant
17	200	600	10000	GVRP	VLAN	normal-participant
18	200	600	10000	GVRP	VLAN	normal-participant
19	200	600	10000	GVRP	VLAN	normal-participant
20	200	600	10000	GVRP	VLAN	normal-participant
21	200	600	10000	GVRP	VLAN	normal-participant
22	200	600	10000	GVRP	VLAN	normal-participant
23	200	600	10000	GVRP	VLAN	normal-participant
24	200	600	10000	GVRP	VLAN	normal-participant
25	200	600	10000	GVRP	VLAN	normal-participant
26	200	600	10000	GVRP	VLAN	normal-participant

Figure 3-12.1: The GARP Port Configuration

Parameter Description

Port: The port column shows the list of ports that you can configure the GARP settings for. There are 2 types configuration settings, which can be configured on per port bases.

- Timer Values
- Applicantion
- Attribute Type
- GARP Applicant

Timer Values: The timer values that can be configured are the GARP join timer, leave timer, and leave all timers. Units are in micro-second.

Three different timers can be configured on this page:

- **Join Timer:** The default value for join timer is 200ms.
- **Leave Timer:** The range of values for leave Time is 600 to 1000ms. The default value for leave timer is 600ms.
- **Leave All Timer:** The default value for leave all timer is 10000ms.

Application: Currently, the only supported application is GVRP.

Attribute Type: Currently, the only supported attribute type is VLAN.

GARP Applicant: This is used to configure the applicant state machine behaviour for GARP on a particular local port.

- **Normal-Participant:** In this mode, the applicant state machine will operate normally in GARP protocol exchanges.
- **Non-Participant:** In this mode, the applicant state machine will not participate in the protocol operation.

The default configuration is normal participant.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

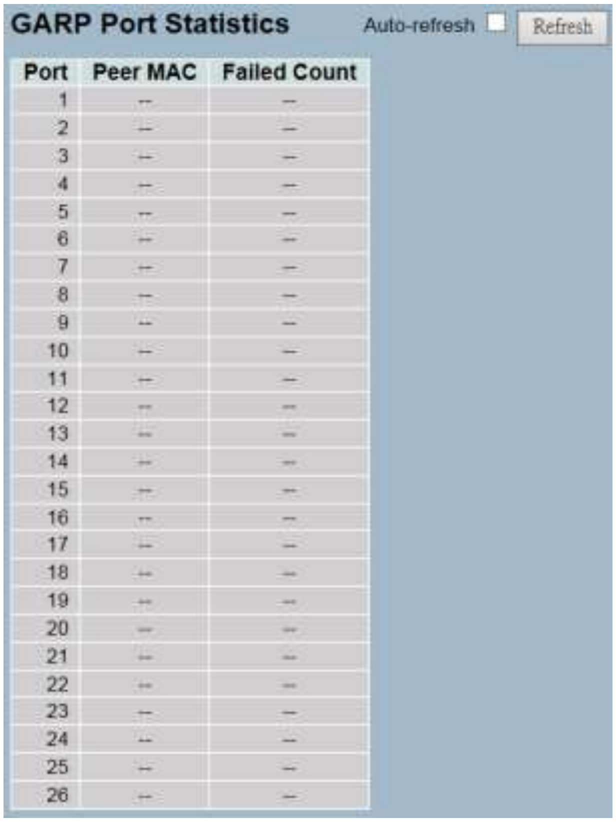
3-12.2 Statistics

The section provides information on the GARP port statistics of the switch.

Web Interface

To display GARP port statistics in the web interface:

1. Click GARP statistics.
2. Choose the port you would like to display the GARP counter information for.
3. Click refresh to manually refresh the GARP statistics.



GARP Port Statistics

Auto-refresh □ Refresh

Port	Peer MAC	Failed Count
1	--	--
2	--	--
3	--	--
4	--	--
5	--	--
6	--	--
7	--	--
8	--	--
9	--	--
10	--	--
11	--	--
12	--	--
13	--	--
14	--	--
15	--	--
16	--	--
17	--	--
18	--	--
19	--	--
20	--	--
21	--	--
22	--	--
23	--	--
24	--	--
25	--	--
26	--	--

Figure 3-12.2: The GARP Port Statistics

Parameter Description

Port : The port column shows the list of ports for which per port GARP statistics are shown for.

Peer MAC: Peer MAC is the MAC address of the neighbour switch from with GARP frame is received.

Failed Count: This explains the failed count.

Auto-Refresh: Click to automatically refresh the information.

Upper Right Icon (Refresh): Click to manually refresh the information.

3-13 GVRP

GVRP is an application-based on generic attribute registration protocol (GARP). It is mainly used to automatically and dynamically maintain the group membership information of the VLANs. The GVRP offers the VLAN registration service through a GARP application. It makes use of GARP information declaration (GID) to maintain the ports associated with their attribute database and GARP information propagation (GIP) to communicate among switches and end stations. With GID information and GIP, the GVRP state machine maintain the contents of dynamic VLAN registration entries for each VLAN and propagate these information to other GVRP-aware devices to setup and update their knowledge database, the set of VLANs associated with currently active members, and through which ports these members can be reached.

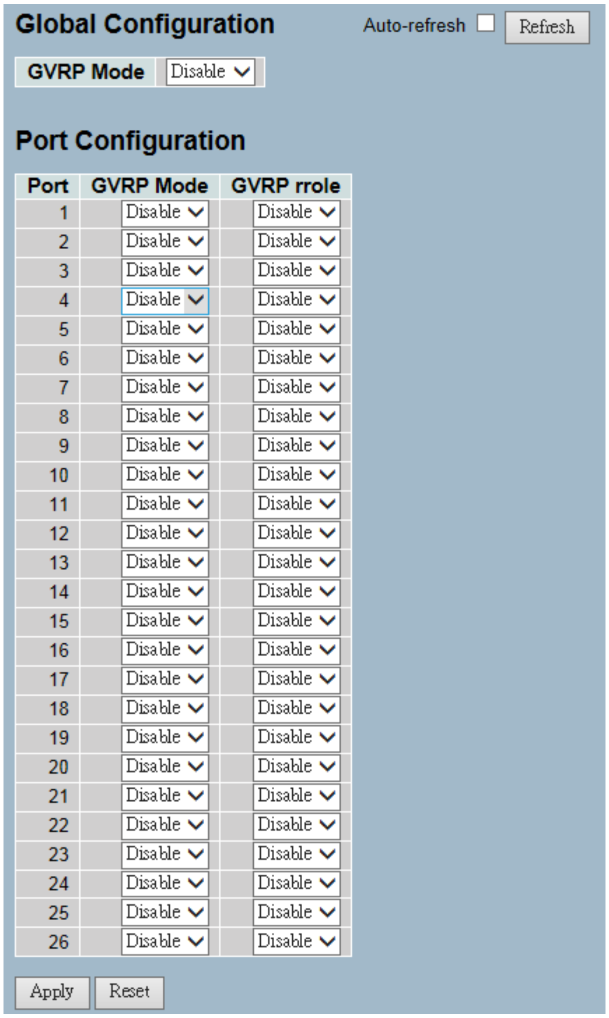
3-13.1 Configuration

This sections provides information on basic configurations for the GVRP settings for all ports.

Web Interface

To configure GVRP port configuration in the web interface:

1. Click GVRP configure.
2. Specify GVRP configuration parameters.
3. Click save.



Global Configuration

Auto-refresh □ Refresh

GVRP Mode: Disable

Port Configuration

Port	GVRP Mode	GVRP rrole
1	Disable	Disable
2	Disable	Disable
3	Disable	Disable
4	Disable	Disable
5	Disable	Disable
6	Disable	Disable
7	Disable	Disable
8	Disable	Disable
9	Disable	Disable
10	Disable	Disable
11	Disable	Disable
12	Disable	Disable
13	Disable	Disable
14	Disable	Disable
15	Disable	Disable
16	Disable	Disable
17	Disable	Disable
18	Disable	Disable
19	Disable	Disable
20	Disable	Disable
21	Disable	Disable
22	Disable	Disable
23	Disable	Disable
24	Disable	Disable
25	Disable	Disable
26	Disable	Disable

Figure 3-13.1: The GVRP Global Configuration

Parameter Description

GVRP Mode: GVRP Mode is a global setting. To enable the GVRP globally, select “Enable” from menu and to disable theGVRP globally, select “Disable”.

Port: The port column shows the list of ports that you can configure the per port GVRP settings for. There are three configuration settings:

1. **GVRP Mode:** This configuration is to enable/disable the GVRP mode on a particular local port.
   - **Disable:** Select to disable GVRP mode on this port.
   - **Enable:** Select to enable GVRP mode on this port.
   - The default value of configuration is disable.

2. **GVRP rrole:** This configuration is used to configure restricted role on an interface.
    - **Disable:** Select to disable GVRP rrole on this port.
    - **Enable:** Select to enable GVRP rrole on this port.
    - The default configuration is disable.

Auto-Refresh: Click to automatically refresh the information.

Upper Right Icon (Refresh): Click to manually refresh the information.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

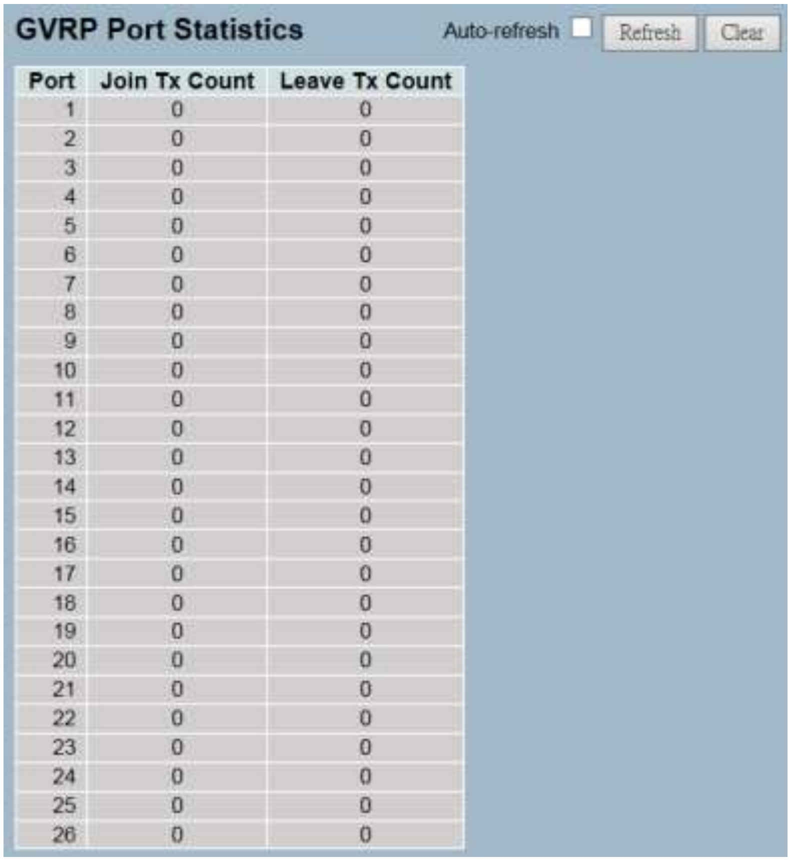
3-13.2 Statistics

The section provides information on the basic GVRP port statistics.

Web Interface

To display GVRP port statistics in the web interface:

1. Click GVRP statistics.
2. Choose which port you want to display the GVRP counter information for.
3. Click refresh to modify the GVRP statistics information.



GVRP Port Statistics

Auto-refresh □ Refresh Clear

Port	Join Tx Count	Leave Tx Count
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0
13	0	0
14	0	0
15	0	0
16	0	0
17	0	0
18	0	0
19	0	0
20	0	0
21	0	0
22	0	0
23	0	0
24	0	0
25	0	0
26	0	0

Figure 3-13.2: The GVRP Port Statistics

Parameter Description

Port: The port column shows the list of ports that you can view the port counters and statistics for.

Join Tx Count: This explains Join Tx count.

Leave Tx Count: This explains Leave Tx count.

Auto-Refresh: Click to automatically refresh the information.

Upper Right Icon (Refresh): Click to manually refresh the information.

3-14 QoS

The switch support four QoS queues per port with strict or weighted fair queuing scheduling. It supports QoS control lists (QCL) for advance programmable QoS classification, based on IEEE 802.1p, Ethertype, VID, IPv4/IPv6 DSCP, and UDP/TCP ports and ranges.

High flexibility in the classification of incoming frames to a QoS class. The QoS classification looks for information up to Layer 4, including IPv4 and IPv6 DSCP, IPv4 TCP/UDP port numbers, and user priority of tagged frames. This QoS classification mechanism is implemented in a QoS control list (QCL). The QoS class assigned to a frame 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.

The switch support advanced memory control mechanisms providing excellent performance of all QoS classes under any traffic scenario, including jumbo frame. A super priority queue with dedicated memory and strict highest priority in the arbitration. The ingress super priority queue allows traffic recognized as CPU traffic to be received and queued for transmission to the CPU even when all the QoS class queues are congested.

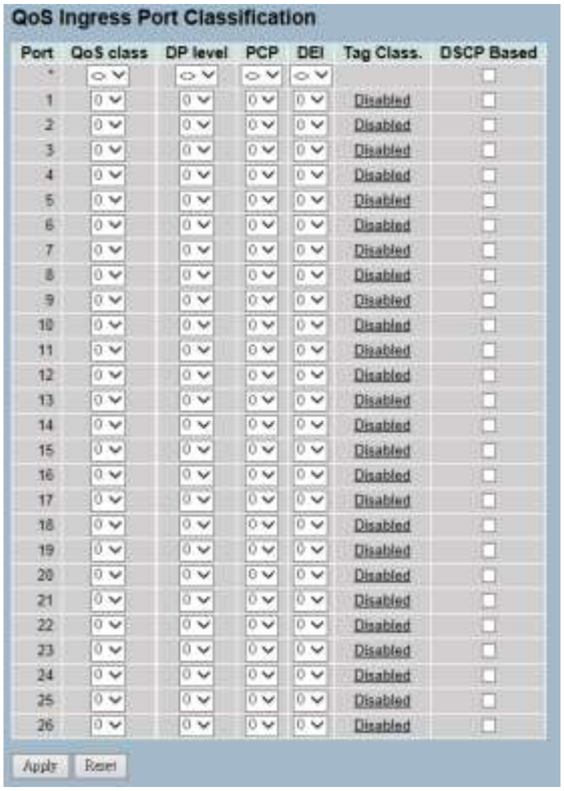
3-14.1 Port Classification

The section provides configurations for the basic QoS ingress classification settings.

Web Interface

To configure the QoS port classification parameters in the web interface:

1. Click Configuration, QoS, and Port Classification.
2. Select the QoS class, DP Level, PCP, and DEI parameters.
3. Click save.
4. Click reset to restore default settings.



QoS Ingress Port Classification

Port	QoS class	DP level	PCP	DEI	Tag Class.	DSCP Based
*	<>	<>	<>	<>		□
1	0	0	0	0	Disabled	□
2	0	0	0	0	Disabled	□
3	0	0	0	0	Disabled	□
4	0	0	0	0	Disabled	□
5	0	0	0	0	Disabled	□
6	0	0	0	0	Disabled	□
7	0	0	0	0	Disabled	□
8	0	0	0	0	Disabled	□
9	0	0	0	0	Disabled	□
10	0	0	0	0	Disabled	□
11	0	0	0	0	Disabled	□
12	0	0	0	0	Disabled	□
13	0	0	0	0	Disabled	□
14	0	0	0	0	Disabled	□
15	0	0	0	0	Disabled	□
16	0	0	0	0	Disabled	□
17	0	0	0	0	Disabled	□
18	0	0	0	0	Disabled	□
19	0	0	0	0	Disabled	□
20	0	0	0	0	Disabled	□
21	0	0	0	0	Disabled	□
22	0	0	0	0	Disabled	□
23	0	0	0	0	Disabled	□
24	0	0	0	0	Disabled	□
25	0	0	0	0	Disabled	□
26	0	0	0	0	Disabled	□

Figure 3-14.1: The QoS Configuration

Parameter Description

Port: This is the port number which the configuration applies to.

QoS Class: This controls the default QoS class (e.g. the QoS class for frames not classified in any other way). There is a one-to-one mapping between QoS class, queue, and priority. A QoS class of zero (0) has the lowest priority.

DP Level: This controls the default DP level (e.g. the DP level for frames not classified in any other way).

PCP: This controls the default PCP for untagged frames.

DEI: This controls the default DEI for untagged frames.

Tag Class: This shows the classification mode for tagged frames on this port.

- **Disabled:** Use default QoS class and DP level for tagged frames.
- **Enabled:** Use mapped versions of PCP and DEI for tagged frames.
- Click on the mode in order to configure the mode and/or mapping.

DSCP Based: Click to enable DSCP-based QoS ingress port classification.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

NOTE:

DP Level: Every incoming frame is classified to a drop precedence level (DP level), which is used throughout the device to provide congestion control guarantees to the frame according to what was configured for that specific DP level.

- **PCP:** PCP is an acronym for priority code point. It is a 3-bit field storing the priority level for the 802.1Q frame.
- **DEI:** DEI is an acronym for drop eligible indicator. It is a 1-bit field in the VLAN tag.

Actual PCP is the PRI column in VLAN tag packet and DEI is the CFI column.

- PCP value can be used for priority definition from 0 to 7.
- DEI value is settable and used to map the DP value from 0 or 1. When the ingress QoS class value is the same, the DP level value is used to define the priority. Larger DP value will be dropped first.

Example: From port 1 input 1G Pkts, Egress port 7 rate be set with 500M. Port 1 Pkts will includes two kinds packet:

a. **PCP & DEI** = 0 0, via configured map to QoS class & DP level = 1, 0.
b. **PCP & DEI** = 0 1, via configured map to QoS class & DP level = 1, 1.

Result will find (a) all past packets, and (b) all dropped packets.

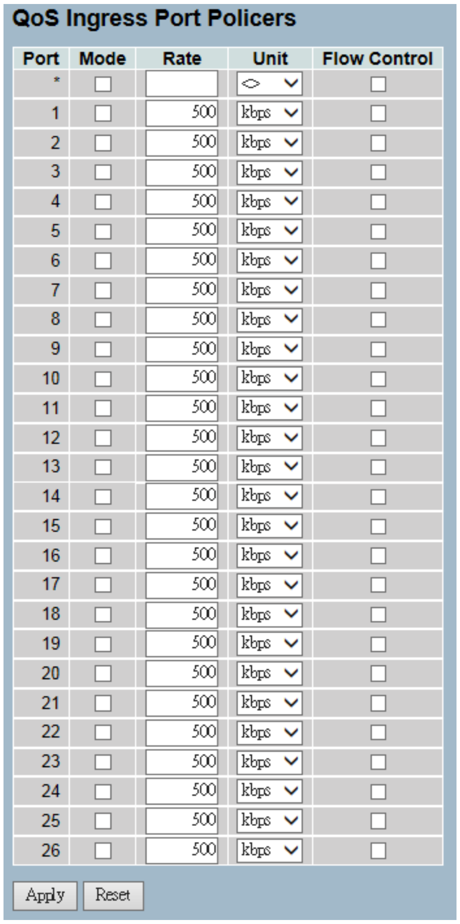
3-14.2 Port Policing

This section provides an overview of the QoS ingress port policers. The port policing is useful in constraining traffic flows and marking frames above specific rates. Policing is primarily useful for data, voice, and video flows because voice and video usually maintains a steady rate of traffic.

Web Interface

To display the QoS port schedulers in the web interface:

1. Click Configuration, QoS, and then Port Policing.
2. Select which port to enable the QoS ingress port policers on and the rate limit condition type.
3. Select the rate limit unit with Kbps, Mbps, Fps, or Kfps.
4. Click save.



QoS Ingress Port Policers

Port	Mode	Rate	Unit	Flow Control
*	□		<>	□
1	□	500	kbps	□
2	□	500	kbps	□
3	□	500	kbps	□
4	□	500	kbps	□
5	□	500	kbps	□
6	□	500	kbps	□
7	□	500	kbps	□
8	□	500	kbps	□
9	□	500	kbps	□
10	□	500	kbps	□
11	□	500	kbps	□
12	□	500	kbps	□
13	□	500	kbps	□
14	□	500	kbps	□
15	□	500	kbps	□
16	□	500	kbps	□
17	□	500	kbps	□
18	□	500	kbps	□
19	□	500	kbps	□
20	□	500	kbps	□
21	□	500	kbps	□
22	□	500	kbps	□
23	□	500	kbps	□
24	□	500	kbps	□
25	□	500	kbps	□
26	□	500	kbps	□

Figure 3-14.2: The QoS Ingress Port Policers Configuration

Parameter Description

Port: This is the logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.

Mode: Select which port you need to enable the QoS ingress port policers function on. This controls whether the policer is enabled on the switch port.

Rate: This controls the rate for the policer. The default value is 500. This value is restricted from 100 to 1000000 when the unit is Kbps or Fps. It is restricted from 1 to 1000 when the unit is Mbps or Kfps.

Unit: Select the rate unit from the following: Kbps, Mbps, Fps, or Kfps. The default is Kbps.

Flow Control: Click to enable or disable the flow control on a port.

Buttons:

- **Save** – Click to save changes.
- **Reset** – Click to restore default settings.

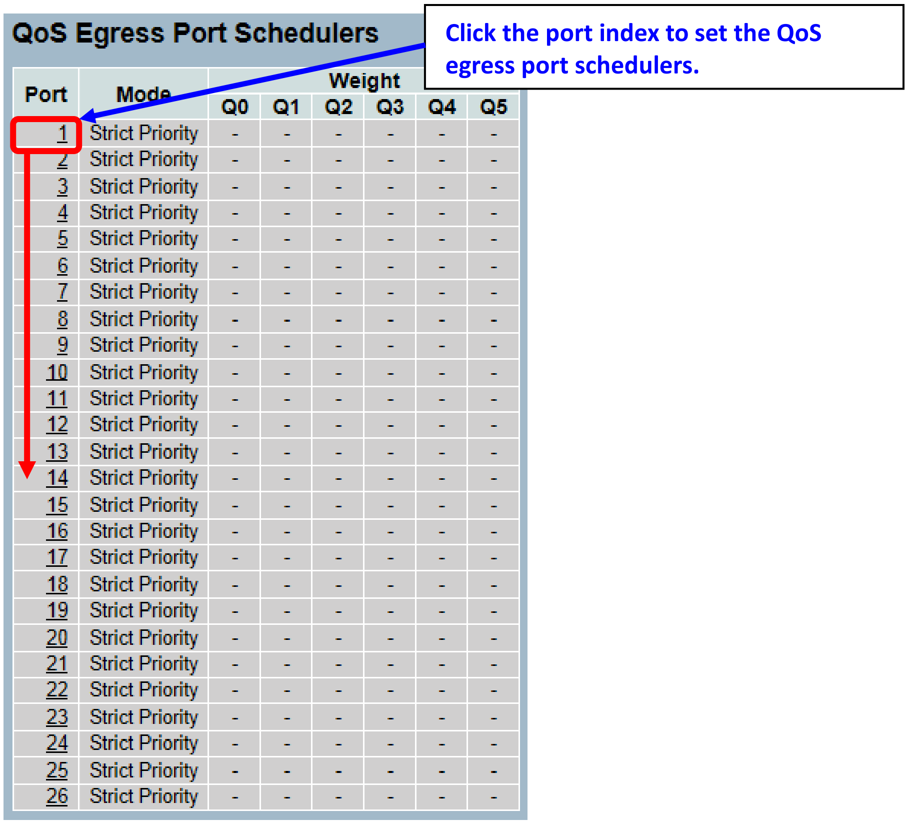
3-14.3 Port Scheduler

This section provides an overview of QoS egress port schedulers.

Web Interface

To display the QoS port schedulers in the web interface:

1. Click Configuration, QoS, and then Port Schedulers.
2. Display the QoS egress port schedulers.

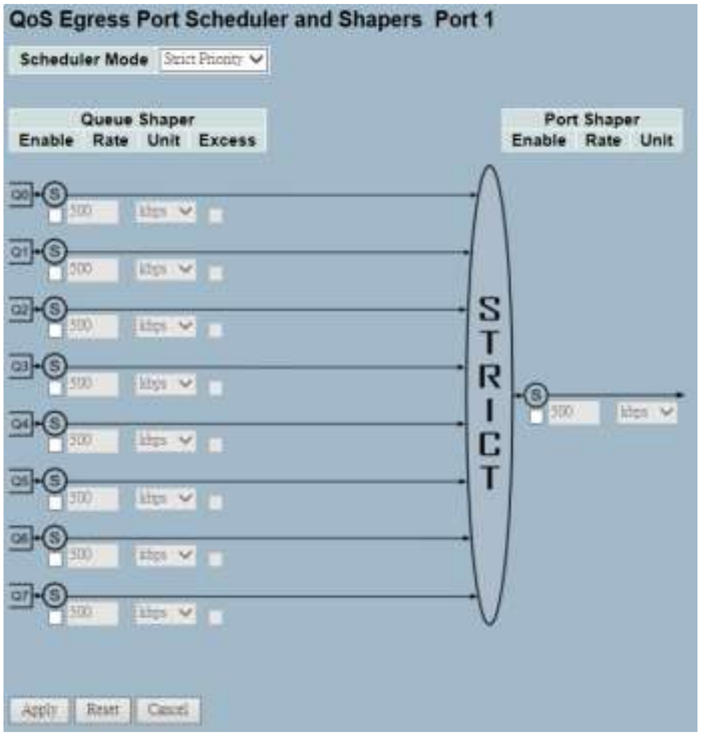


Click the port index to set the QoS egress port schedulers.

QoS Egress Port Schedulers

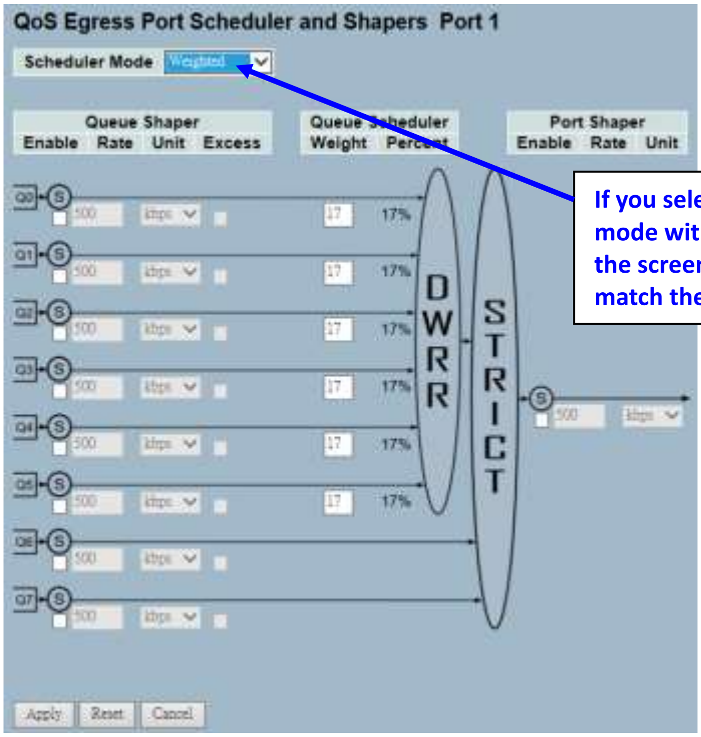
Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-
11	Strict Priority	-	-	-	-	-	-
12	Strict Priority	-	-	-	-	-	-
13	Strict Priority	-	-	-	-	-	-
14	Strict Priority	-	-	-	-	-	-
15	Strict Priority	-	-	-	-	-	-
16	Strict Priority	-	-	-	-	-	-
17	Strict Priority	-	-	-	-	-	-
18	Strict Priority	-	-	-	-	-	-
19	Strict Priority	-	-	-	-	-	-
20	Strict Priority	-	-	-	-	-	-
21	Strict Priority	-	-	-	-	-	-
22	Strict Priority	-	-	-	-	-	-
23	Strict Priority	-	-	-	-	-	-
24	Strict Priority	-	-	-	-	-	-
25	Strict Priority	-	-	-	-	-	-
26	Strict Priority	-	-	-	-	-	-

Figure 3-14.3: The QoS Egress Port Schedules



QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: Strict Priority



QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: Weighted

If you select the scheduler mode with weighted, then the screen will change to match the figure.

Parameter Description

Port: This is the logical port for the settings contained in the same row. Click on the port number to configure the schedulers.

Mode: This shows the scheduling mode for this port.

Weight (Qn): This shows the weight for this queue and port.

Scheduler Mode: This controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.

Queue Shaper Enable: This controls whether the queue shaper is enabled for this queue on this switch port.

Queue Shaper Rate: This controls the rate for the queue shaper. The default value is ?. This value is restricted to ? to 1000000 when the unit is Kbps. It is restricted to 1 to ? when the unit is Mbps.

Queue Shaper Unit: This controls the unit of measure for the queue shaper rate as Kbps or Mbps. The default value is Kbps.

Queue Shaper Excess: This controls whether the queue is allowed to use excess bandwidth.

Queue Scheduler Weight: This controls the weight for this queue. The default value is 17. This value is restricted to 1 to 100. This parameter is only shown if scheduler mode is set to "Weighted".

Queue Scheduler Percent: This shows the weight in percent for this queue. This parameter is only shown if scheduler mode is set to "Weighted".

Port Shaper Enable: This controls whether the port shaper is enabled for this switch port.

Port Shaper Rate: This controls the rate for the port shaper. The default value is ?. This value is restricted to ? to 1000000 when the unit is Kbps. It is restricted to 1 to ? when the unit is Mbps.

Port Shaper Unit: This controls the unit of measure for the port shaper rate as Kbps or Mbps. The default value is Kbps.

Buttons:

- **Save** – Click to save changes.
- **Reset -** Click to restore default settings.

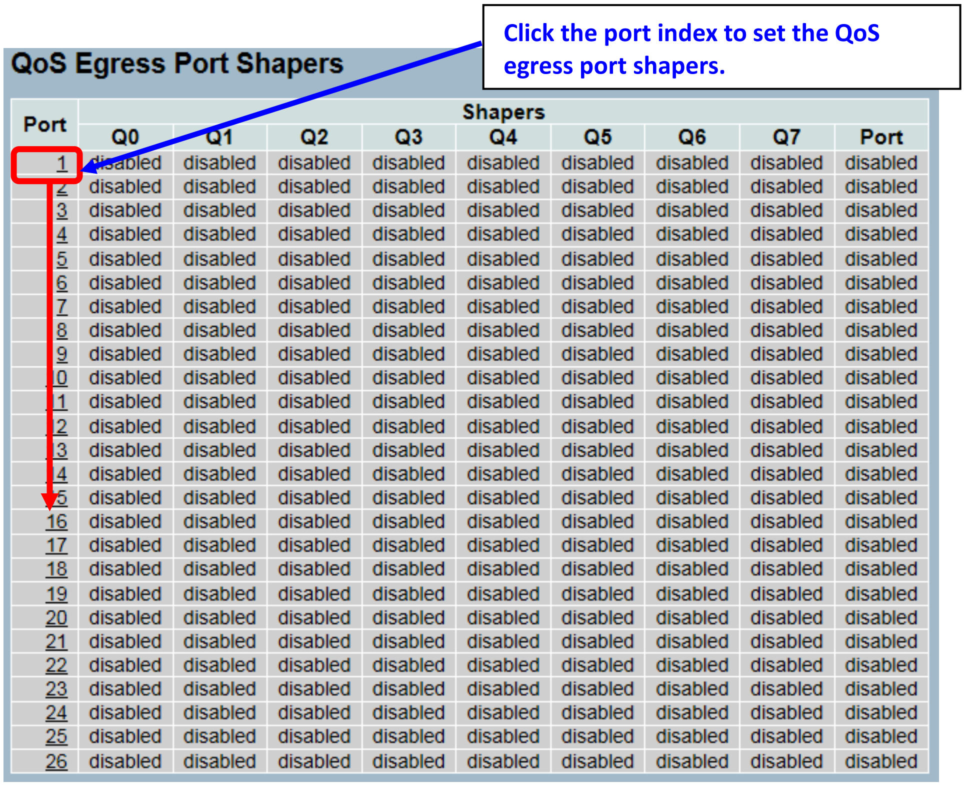
3-14.4 Port Shaping

This section provides an overview of QoS egress port shaping for all switch ports.

Web Interface

To display the QoS port shapers in the web interface:

1. Click Configuration, QoS, and then Port Shapers.
2. Display the QoS egress port shapers.

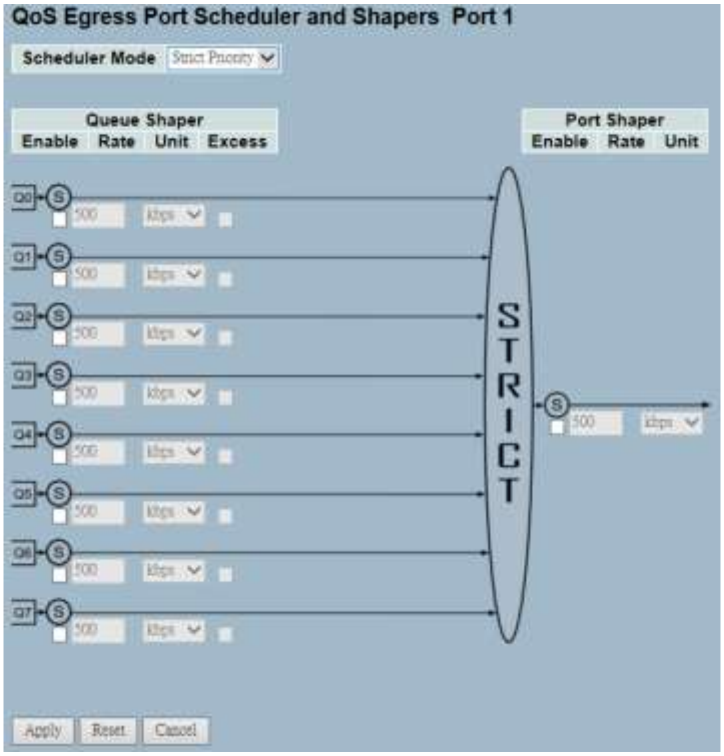


Click the port index to set the QoS egress port shapers.

QoS Egress Port Shapers

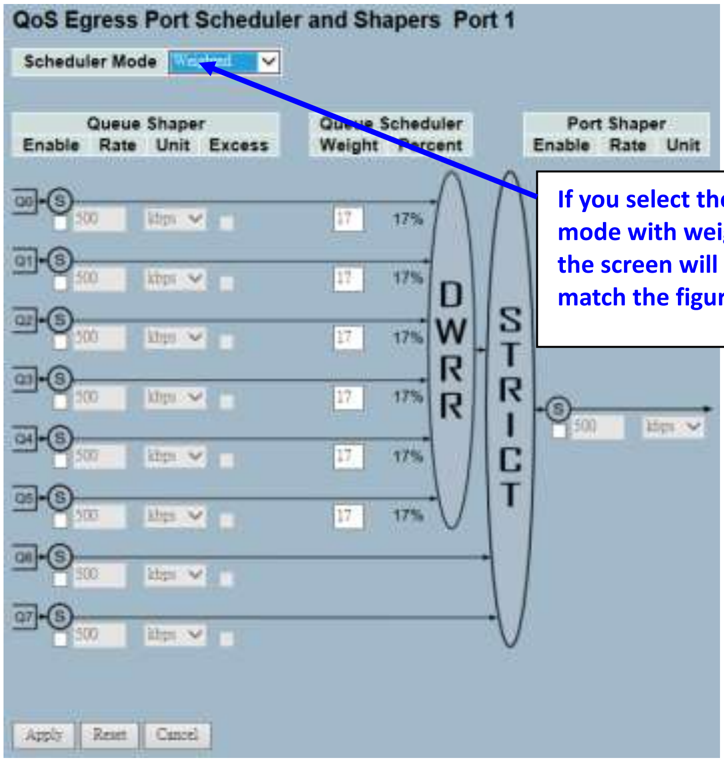
Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
9	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
10	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
11	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
12	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
13	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
14	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
15	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
16	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
17	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
18	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
19	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
20	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
21	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
22	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
23	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
24	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
25	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
26	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

Figure 3-14.4: The QoS Egress Port Shapers



QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: Strict Priority



QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: Weighted

If you select the scheduler mode with weighted, then the screen will change to match the figure.

Parameter Description

Port: This is the logical port for the settings contained in the same row. Click on the port number in order to configure the shapers.

Shapers (Qn): This shows "disabled" or actual queue shaper rate. Example - "800 Mbps".

Shapers (Port): This shows "disabled" or actual port shaper rate. Example - "800 Mbps".

Scheduler Mode: This controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.

Queue Shaper Enable: This controls whether the queue shaper is enabled for this queue on this switch port.

Queue Shaper Rate: This controls the rate for the queue shaper. The default value is ?. This value is restricted to ? to 1000000 when the unit is Kbps. It is restricted to 1 to ? when the unit is Mbps.

Queue Shaper Unit: This controls the unit of measure for the queue shaper rate Kbps or Mbps. The default value is Kbps.

Queue Shaper Excess: This controls whether the queue is allowed to use excess bandwidth.

Queue Scheduler Weight: This controls the weight for this queue. The default value is 17. This value is restricted to 1 to 100. This parameter is only shown if scheduler mode is set to "Weighted".

Queue Scheduler Percent: This shows the weight in percent for this queue. This parameter is only shown if scheduler mode is set to "Weighted".

Port Shaper Enable: This controls whether the port shaper is enabled for this switch port.

Port Shaper Rate: This controls the rate for the port shaper. The default value is ?. This value is restricted to ? to 1000000 when the unit is Kbps. It is restricted to 1 to ? when the unit is Mbps.

Port Shaper Unit: This controls the unit of measure for the port shaper rate as Kbps or Mbps. The default value is Kbps.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

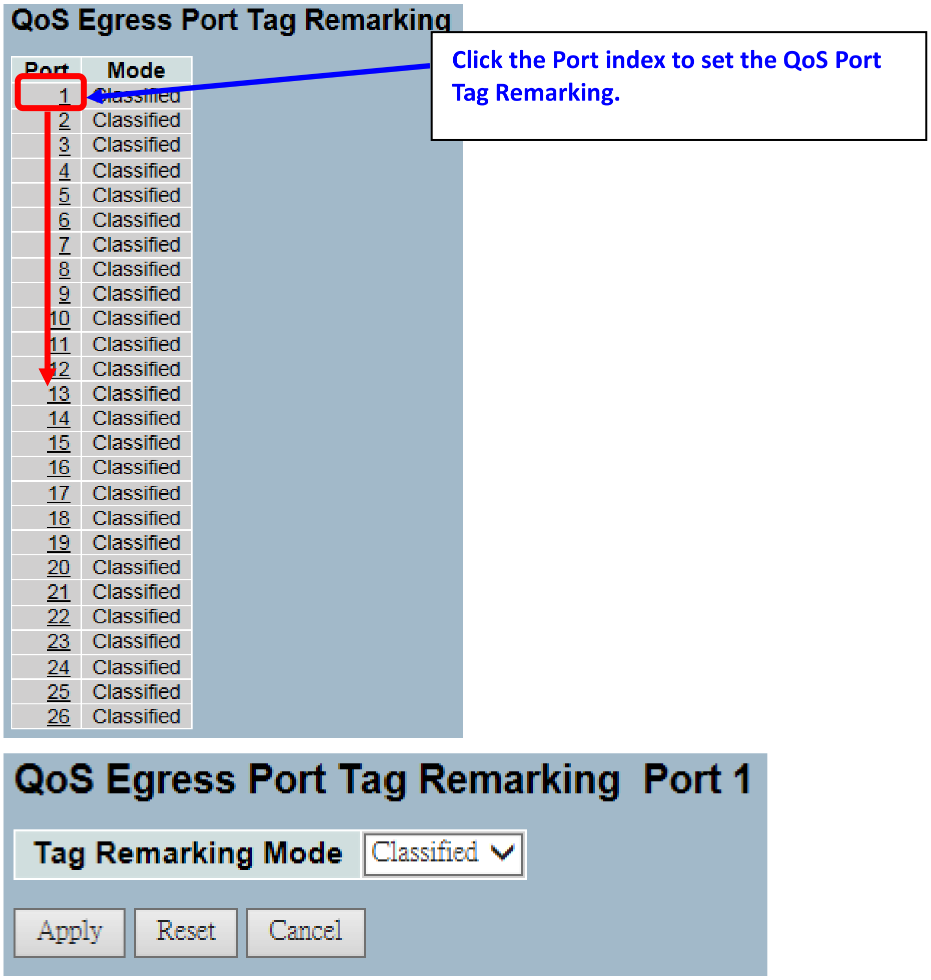
3-14.5 Port Tag Remarking

The section provides an overview of QoS egress port tag remarking.

Web Interface

To display the QoS port tag remarking in the web interface:

1. Click Configuration, QoS, and then Port Tag Remarking.



QoS Egress Port Tag Remarking

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified
11	Classified
12	Classified
13	Classified
14	Classified
15	Classified
16	Classified
17	Classified
18	Classified
19	Classified
20	Classified
21	Classified
22	Classified
23	Classified
24	Classified
25	Classified
26	Classified

Click the Port index to set the QoS Port Tag Remarking.

QoS Egress Port Tag Remarking Port 1

Tag Remarking Mode: Classified

Figure 3-14.5: The Port Tag Remarking

Parameter Description

Port: This is the logical port for the settings contained in the same row. Click on the port number in order to configure tag remarking.

Mode: This shows the tag remarking mode for this port.

- **Classified:** This uses classified PCP/DEI values.
- **Default:** This uses default PCP/DEI values.
- **Mapped:** This uses mapped versions of QoS class and DP level.

Tag Remarking Mode: This selects the tag remarking mode for this port.

- **Classified:** This uses classified PCP/DEI values.
- **Default:** This uses default PCP/DEI values.
- **Mapped:** This uses mapped versions of QoS class and DP level.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.
- **Cancel** – Click to cancel the changes.

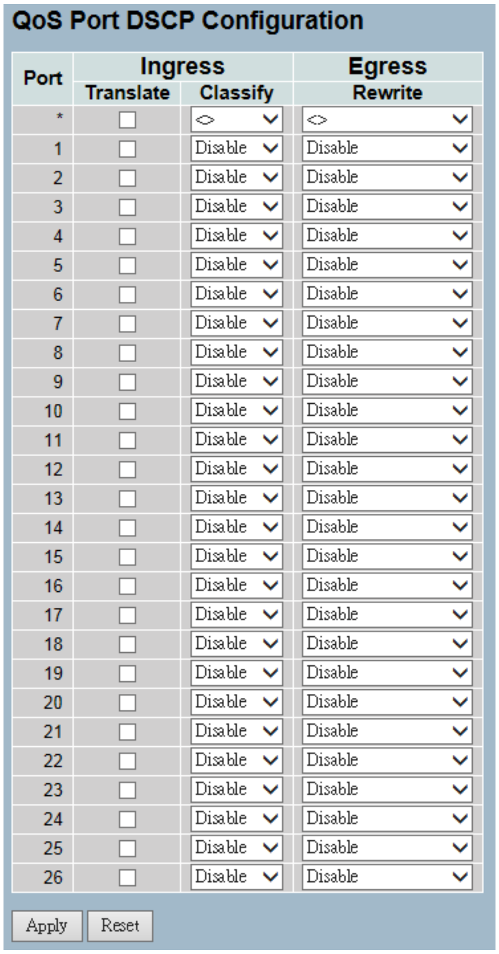
3-14.6 Port DSCP

The section provides information on setting up the QoS Port DSCP configuration.

Web Interface

To configure the QoS port DSCP parameters in the web interface:

1. Click Configuration, QoS, and then Port DSCP.
2. Click to enable or disable the ingress translate and select the classify parameter configuration.
3. Select the egress rewrite parameters.
4. Click save.
5. Click reset to restore default settings.



QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	□	<>	<>
1	□	Disable	Disable
2	□	Disable	Disable
3	□	Disable	Disable
4	□	Disable	Disable
5	□	Disable	Disable
6	□	Disable	Disable
7	□	Disable	Disable
8	□	Disable	Disable
9	□	Disable	Disable
10	□	Disable	Disable
11	□	Disable	Disable
12	□	Disable	Disable
13	□	Disable	Disable
14	□	Disable	Disable
15	□	Disable	Disable
16	□	Disable	Disable
17	□	Disable	Disable
18	□	Disable	Disable
19	□	Disable	Disable
20	□	Disable	Disable
21	□	Disable	Disable
22	□	Disable	Disable
23	□	Disable	Disable
24	□	Disable	Disable
25	□	Disable	Disable
26	□	Disable	Disable

Figure 3-14.6: The QoS Port DSCP Configuration

Parameter Description

Port: The port column shows the list of ports that you can configure DSCP ingress and egress settings for.

Ingress: Click to change the ingress translation and classification settings for individual ports.

There are two configuration parameters available for ingress:

1. **Translate:** Click to enable the ingress translation.
2. **Classify:** Classification for a port have 4 different values -

    - **Disable**: No ingress DSCP classification.
    - **DSCP=0**: Classify if incoming (or translated, if enabled) DSCP is 0.
    - **Selected**: Classification is enabled, as specified in DSCP translation window for the specific DSCP.
    - **All**: Classify all DSCP.

Egress: Port Egress Rewriting can be one of below parameters

- **Disable**: No Egress rewrite.
- **Enable**: Rewrite enable without remapped.
- **Remap DP Unaware**: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation->Egress Remap DP0' table.
- **Remap DP Aware**: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the 'DSCP Translation->Egress Remap DP0' table or from the 'DSCP Translation->Egress Remap DP1' table.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

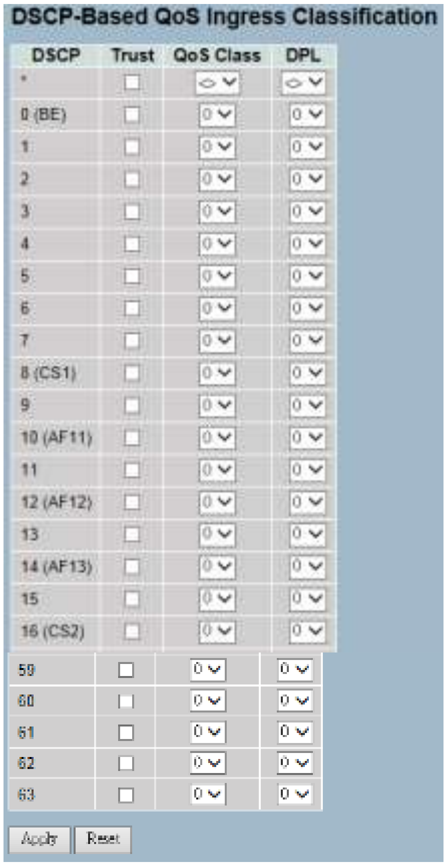
3-14.7 DSCP-based QoS

The section provides configurations on the DSCP-based QoS mode.

Web Interface

To configure the DSCP –based QoS ingress classification parameters in the web interface:

1. Click Configuration, QoS, and DSCP-Based QoS.
2. Click to enable or disable the DSCP for trust.
3. Select the QoS class and DPL parameters.
4. Click save.
5. Click reset to restore default settings.



DSCP-Based QoS Ingress Classification

DSCP	Trust	QoS Class	DPL
*	□	<>	<>
0 (BE)	□	0	0
1	□	0	0
2	□	0	0
3	□	0	0
4	□	0	0
5	□	0	0
6	□	0	0
7	□	0	0
8 (CS1)	□	0	0
9	□	0	0
10 (AF11)	□	0	0
11	□	0	0
12 (AF12)	□	0	0
13	□	0	0
14 (AF13)	□	0	0
15	□	0	0
16 (CS2)	□	0	0
59	□	0	0
60	□	0	0
61	□	0	0
62	□	0	0
63	□	0	0

Figure 3-14.7: The DSCP-Based QoS Ingress Classification Configuration

Parameter Description

DSCP: The maximum number of supported DSCP values are 64.

Trust: Click if the DSCP value is trusted.

QoS Class: The QoS class value can be 0 to 7.

DPL: The drop precedence level 0 to 3.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

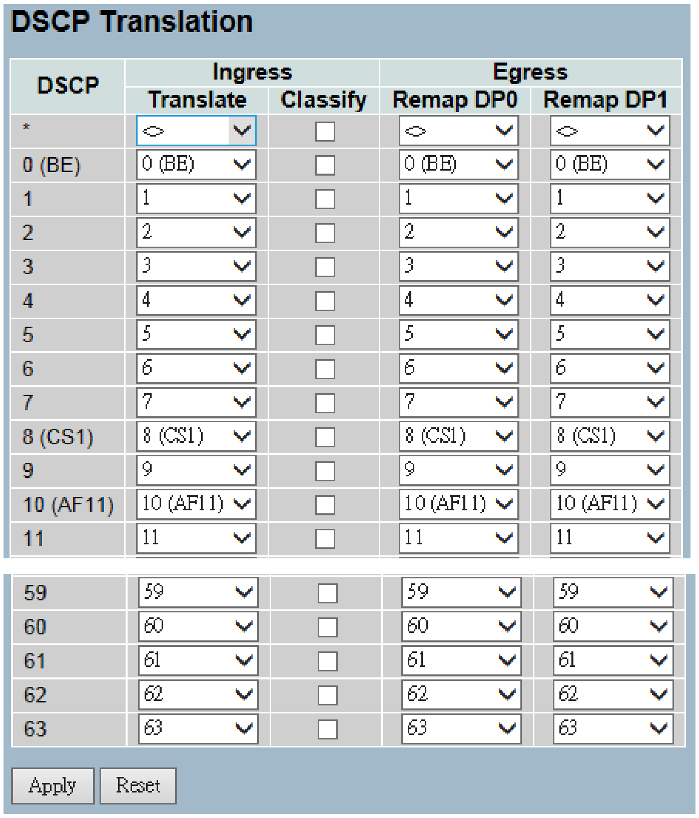
3-14.9 DSCP Translation

The section provides configurations for the basic QoS DSCP translation settings. DSCP translation can be done in ingress or egress.

Web Interface

To configure the DSCP translation parameters in the web interface:

1. Click Configuration, QoS, and then DSCP Translation.
2. Scroll to set the ingress translate, egress remap DP0, and remap DP1 parameters.
3. Click to enable or disable classify.
4. Click save.
5. Click reset to restore default settings.



DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>	□	<>	<>
0 (BE)	0 (BE)	□	0 (BE)	0 (BE)
1	1	□	1	1
2	2	□	2	2
3	3	□	3	3
4	4	□	4	4
5	5	□	5	5
6	6	□	6	6
7	7	□	7	7
8 (CS1)	8 (CS1)	□	8 (CS1)	8 (CS1)
9	9	□	9	9
10 (AF11)	10 (AF11)	□	10 (AF11)	10 (AF11)
11	11	□	11	11
59	59	□	59	59
60	60	□	60	60
61	61	□	61	61
62	62	□	62	62
63	63	□	63	63

Figure 3-14.8: The DSCP Translation Configuration

Parameter Description

DSCP: The maximum number of supported DSCP values are 64. The valid DSCP value ranges from 0 to 63.

Ingress: Ingress DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map.

There are two configuration parameters for DSCP translation:

1. **Translate:** DSCP at the ingress side can be translated from 0 to 63 DSCP values.
2. **Classify:** Click to enable classification at the ingress side.

Egress: There are following configurable parameters for Egress side:

1. **Remap DP0:** Select the DSCP value that you want to remap. The DSCP value ranges from 0 to 63.
2. **Remap DP1:** Select the DSCP value that you want to remap. The DSCP value ranges from 0 to 63.

There is following configurable parameter for Egress side -

- **Remap:** Select the DSCP value that you want to remap. The DSCP value ranges from 0 to 63.

Buttons:

- **Save** – Click to save changes.
- **Reset** - Click to restore default settings.

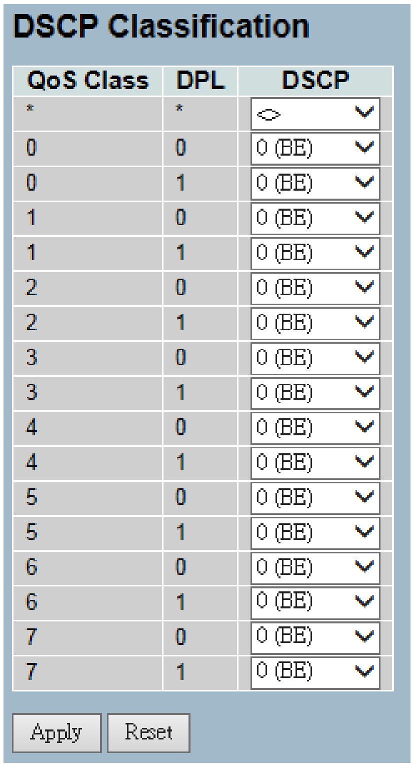
3-14.10 DSCP Classification

The section provides configurations and information on how to map map a DSCP value to a QoS Class and DPL value.

Web Interface

To configure the DSCP Classification parameters in the web interface:

1. Click Configuration, QoS, and then DSCP Translation.
2. Set the DSCP parameters.
3. Click save.
4. Click reset to restore default settings.



DSCP Classification

QoS Class	DPL	DSCP
*	*	<>
0	0	0 (BE)
0	1	0 (BE)
1	0	0 (BE)
1	1	0 (BE)
2	0	0 (BE)
2	1	0 (BE)
3	0	0 (BE)
3	1	0 (BE)
4	0	0 (BE)
4	1	0 (BE)
5	0	0 (BE)
5	1	0 (BE)
6	0	0 (BE)
6	1	0 (BE)
7	0	0 (BE)
7	1	0 (BE)

Figure 3-14.9: The DSCP Classification Configuration

Parameter Description

QoS Class: The available QoS class value ranges from 0 to 7. The QoS class (0-7) can be mapped to followed parameters.

DPL: The drop precedence level (0-1) can be configured for all available QoS classes.

DSCP: Select the DSCP value (0-63) from DSCP menu to map DSCP to corresponding QoS Class and DPL value.

Buttons:

- **Save** – Click to save changes.
- **Reset** - Click to restore default settings.

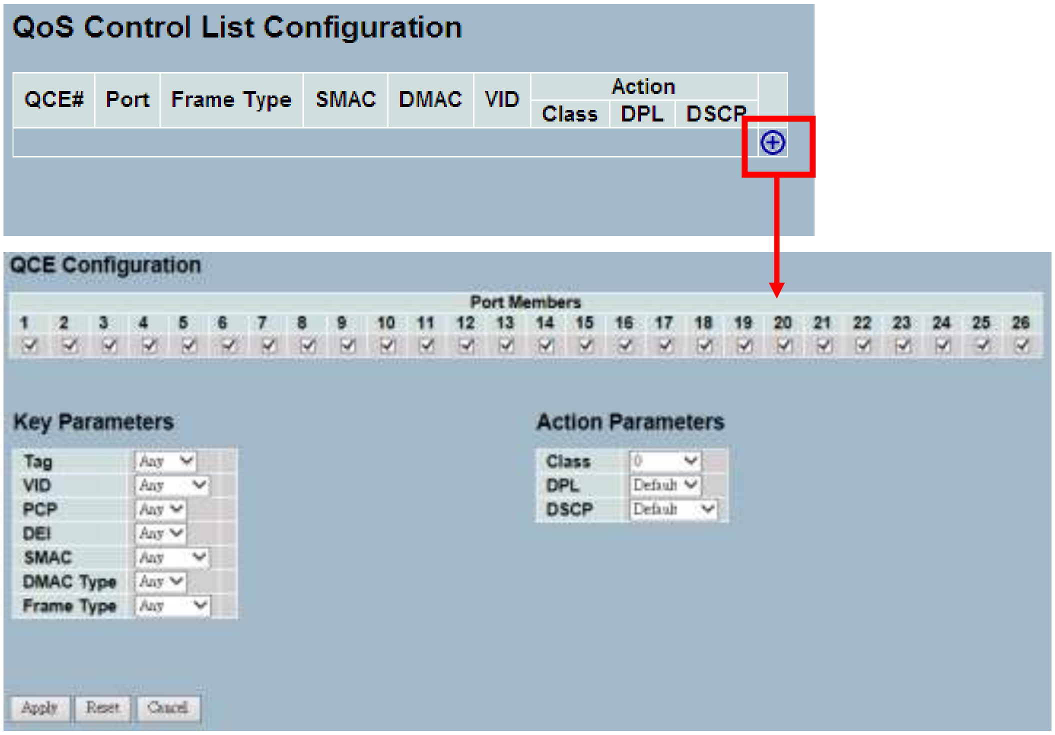
3-14.11 QoS Control List Configuration

The section provides information about the QoS control list (QCL). QCL is made up of QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch. Click on the lowest plus sign to add a new QCE to the list.

Web Interface

To configure the QoS Control List parameters in the web interface:

1. Click Configuration, QoS, and QoS contol list.
2. Click the ⊕ to add a new QoS control list.
3. Select all parameters and choose the port member to join the QCE rules.
4. Click save.
5. Click reset to restore default settings.



QoS Control List Configuration

QCE#	Port	Frame Type	SMAC	DMAC	VID	Action		
						Class	DPL	DSCP
								⊕

QCE Configuration

Port Members

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Key Parameters

Tag	Any
VID	Any
PCP	Any
DEI	Any
SMAC	Any
DMAC Type	Any
Frame Type	Any

Action Parameters

Class	0
DPL	Default
DSCP	Default

Figure 3-14.10: The QoS Control List Configuration

Parameter Description

QCE#: This indicates the index of QCE.

Port: This indicates the list of ports configured with the QCE.

Frame Type: This indicates the type of incoming frame to look for. Possible frame types are:

- **Any:** The QCE will match all frame type.
- **Ethernet:** Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.
- **LLC:** Only (LLC) frames are allowed.
- **SNAP:** Only (SNAP) frames are allowed
- **IPv4:** The QCE will match only IPV4 frames.
- **IPv6:** The QCE will match only IPV6 frames.

SMAC: This displays the OUI field of source MAC address. Example – The first three octet (byte) of MAC address.

DMAC: This specifies the type of destination MAC addresses for incoming frame. Possible values are:

- **Any:** All types of destination MAC addresses are allowed.
- **Unicast:** Only unicast MAC addresses are allowed.
- **Multicast:** Only multicast MAC addresses are allowed.
- **Broadcast:** Only broadcast MAC addresses are allowed.
- The default value is 'Any'.

VID: This indicates the VLAN ID - either a specific VID or range of VIDs. The VID can be in the range 1-4094 or “Any”.

PCP (Priority Code Point): The valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7), or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or “Any”.

DEI (Drop Eligible Indicator): The valid value of DEI can be any of values between 0 to 1 or “Any”.

Action: This indicates the classification action taken on ingress frame if the configured parameters matched the frame's content.

There are three action fields: Class, DPL, and DSCP.

- **Class (Classified QoS Class):** If a frame matches the QCE, it will be put in the queue.
- **DPL (Classified Drop Precedence Level):** If a frame matches the QCE, then the DP level will set to the value displayed under DPL column.
- **DSCP (Classified DSCP Value):** If a frame matches the QCE, then the DSCP will be classified with the value displayed under DSCP column.

Modification Buttons: You can modify each QCE (QoS Control Entry) in the table using the following buttons:

⊕ Inserts a new QCE before the current row.

ⓔ Edits the QCE.

↑ Moves the QCE up the list.

↓ Moves the QCE down the list.

⊗ Deletes the QCE.

⊕ (Lower plus sign) Adds a new entry to the bottom of the list.

Port Members: Click the box to make any port member part of the QCL entry. All ports are checked by default.

Key Parameters: Key configuration are described as below:

- **Tag:** The value of tag field can be "Any", "Untag", or "Tag".
- **VID:** The valid value of the VLAN ID can be in the range of 1-4095 or "Any". You can enter a specific value or a range of VIDs.
- **PCP (Priority Code Point):** The valid value of PCP can be specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or "Any".
- **DEI (Drop Eligible Indicator):** The valid value of DEI can be any of values between 0, 1. or "Any".
- **SMAC (Source MAC Address):** The value can be 24 MS bits (OUI) or "Any".
- **DMAC Type (Destination MAC Type):** The possible values are unicast(UC), multicast(MC), broadcast(BC), or "Any".
- **Frame Type:** The frame type can have any of the following values:
    1. Any
    2. Ethernet
    3. LLC
    4. SNAP
    5. IPv4
    6. IPv6

NOTE: All frame types are explained below.
1. Any: Allows all types of frames.

2. Ethernet: Ethernet type valid ethernet type can have values within 0x600 to 0xFFFF or “Any”. The default value is “Any”.

3. LLC: **SSAP Address:** Valid SSAP (Source Service Access Point) can vary from 0x00 to 0xFF or “Any”. The default value is “Any”.
DSAP Address: Valid DSAP (Destination Service Access Point) can vary from 0x00 to 0xFF or “Any”. The default value is “Any”.
Control: Valid control address can vary from 0x00 to 0xFF or “Any”. The default value is “Any”.

4. SNAP: **PID:** Valid PID (a.k.a ethernet type) can have value within 0x00 to 0xFFFF or “Any”. The default value is “Any”.

5. IPv4: **Protocol:** IP protocol number can be (0-255, TCP or UDP) or “Any”.
Source IP: Specific source IP address in value/mask format or “Any”. IP and mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero.
DSCP (Diffserv Code Point Value): It can be specific value, range of value, or “Any”. DSCP values are in the range 0-63 including BE, CS1-CS7, EF, or AF11-AF43.
IP Fragment: IPv4 frame fragmented option: yes|no|any
Sport (Source TCP/UDP Port): (0-65535) or “Any”, specific or port range applicable for IP protocol UDP/TCP.
Dport (Destination TCP/UDP Port): (0-65535) or “Any”, specific or port range applicable for IP protocol UDP/TCP.

6. IPv6 : **Protocol:** IP protocol number can be (0-255, TCP or UDP) or “Any”.
Source IP: IPv6 source address can be (a.b.c.d) or “Any”, 32 LS bits.
DSCP (Diffserv Code Point Value): It can be specific value, range of value, or “Any”. DSCP values are in the range 0-63 including BE, CS1-CS7, EF, or AF11-AF43.
Sport (Source TCP/UDP Port): (0-65535) or “Any”, specific or port range for IP protocol UDP/TCP.
Dport (Destination TCP/UDP Port): 0-65535) or “Any”, specific or port range for IP protocol UDP/TCP.

Action Parameters:

- **Class:** QoS Class can be class 0 to 7. The default is basic classification.
- **DP:** Valid DP Level can be 0 to 3. The default is basic classification.
- **DSCP:** Valid DSCP value can be 0-63, BE, CS1-CS7, EF. or AF11-AF43.

Buttons:

- **Apply**– Click to apply the configuration and move to main QCL page.
- **Reset-** Click to restore default settings.
- **Cancel**–Return to the previous page without saving the configuration change.

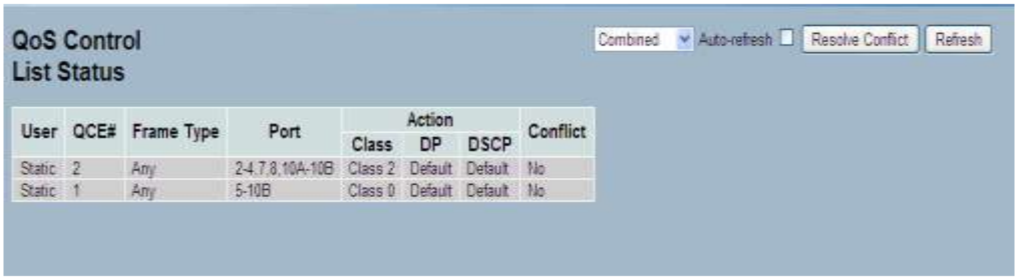
3-14.12 QCL Status

The section provides configurations of the QCL status by different QCL users. 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.

Web Interface

To display the QoS control list status in the web interface:

1. Click Configuration, QoS, and then QCL Status.
2. Click auto-refresh to automatically refresh the information.
3. Select the combined, static, voice VLAN, and conflict.
4. Click refresh to manually refresh the information.



QoS Control List Status

User	QCE#	Frame Type	Port	Action			Conflict
				Class	DP	DSCP	
Static	2	Any	2-4,7,8,10A-10B	Class 2	Default	Default	No
Static	1	Any	5-10B	Class 0	Default	Default	No

Figure 3-14.11: The QoS Control List Status

Parameter Description

User: This indicates the QCL user.

QCE#: This indicates the index of QCE.

Frame Type: This indicates the type of incoming frame to look for. Possible frame types are:

- **Any:** The QCE will match all frame type.
- **Ethernet:** Only Ethernet frames (with Ether Type 0x600 to 0xFFFF) are allowed.
- **LLC:** Only LLC frames are allowed.
- **SNAP:** Only SNAP frames are allowed.
- **IPv4:** The QCE will match only IPV4 frames.
- **IPv6:** The QCE will match only IPV6 frames.

Port: This indicates the list of ports configured with the QCE.

Action: This 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.

- **Class (Classified QoS Class):** If a frame matches the QCE, it will be put in the queue.
- **DPL (Drop Precedence Level):** If a frame matches the QCE, then DP level will set to value displayed under the DPL column.
- **DSCP:** If a frame matches the QCE, then DSCP will be classified with the value displayed under the DSCP column.

Conflict: This displays conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available. In that case, it shows the 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 by pressing the “Resolve Conflict” button.

Buttons:

- – Select the QCL status from this drop down list.

- **Auto-refresh-** Click to automatically refresh the information.
- **Resolve Conflict**– Click to release the resources required to add QCL entry, in case conflict status for any QCL entry is 'yes'.
- **Refresh**– Click to manually refresh the information.

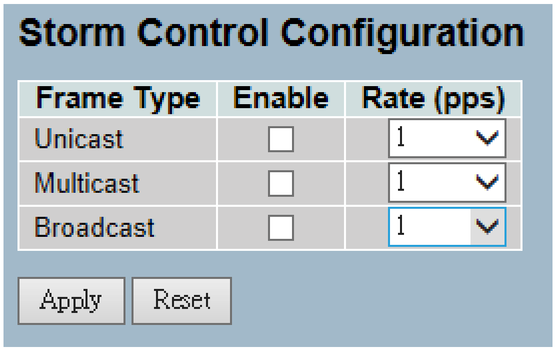
3-14.13 Storm Control

The section provides configurations for the storm control. There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames (e.g. frames with a [VLAN ID, DMAC] pair not present on the MAC Address table). The configuration indicates the permitted packet rate for unicast, multicast, or broadcast traffic across the switch.

Web Interface

To configure the storm control configuration parameters in the web interface:

1. Click Configuration, QoS, and then Storm Control Configuration.
2. Select the frame type to enable storm control.
3. Set the rate parameters.
5. Click save.
6. Click reset to restore default settings.



Storm Control Configuration

Frame Type	Enable	Rate (pps)
Unicast	□	1
Multicast	□	1
Broadcast	□	1

Figure 3-14.12: The Storm Control Configuration

Parameter Description

Frame Type: The settings in a particular row apply to the frame type listed here: Unicast, Multicast, or Broadcast.

Enable: This enables or disables the storm control status for the given frame type.

Rate: The rate unit is packets per second (pps). Valid values are: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K or 1024K, 1024K, 2048K, 4096K, 8192K, 16384K or 32768K, or 1024K. The 1 kpps is actually 1002.1 pps.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

3-15 s-Flow Agent

This section provides information on monitoring, modifying and configuring the sFlow collector IP type, Sflow collector IP address, and port number. Up to 1 collector is supported.

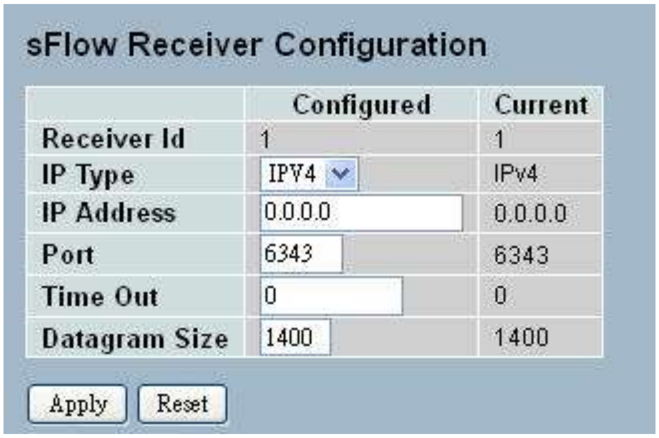
3-15.1 Collector

The “Current” field displays the currently configured sFlow collector. The “Configured” field displays the new collector configuration.

Web Interface

To configure the sFlow agent in the web interface:

1. Click Configuration, sFlow Agent, and then Collector.
2. Set the parameters.
3. Select IPv4 or IPv6 for IP type.
4. Click save.
5. Click reset to restore default settings.



sFlow Receiver Configuration

	Configured	Current
Receiver Id	1	1
IP Type	IPV4	IPv4
IP Address	0.0.0.0	0.0.0.0
Port	6343	6343
Time Out	0	0
Datagram Size	1400	1400

Figure 3-15.1: The sFlow Collector Configuration

Parameter Description

Receiver ID: The "Receiver ID" input fields allow the user to select the receiver ID. This indicates the ID of this particular sFlow receiver. Currently, one ID is supported because only one collector is supported.

IP Type: A drop down list to select the type of IP of the collector is displayed. By default, the type of collector IP is IPv4. You can choose between IPv4 or IPv6.

IP Address: This is the address of a reachable IP is to be entered into the text box. This IP is used to monitor the sFlow samples sent by sFlow Agent (switch). By default, the IP is set to 0.0.0.0, and a new entry has to be added to it.

Port: A port to listen to the sFlow Agent has to be configured for the collector. The value of the port number has to be typed into the text box. The value accepted is within the range of 1 to 65535. However, an appropriate port number not used by other protocols need to be configured. By default, the port's number is 6343.

Time Out: It is the duration during which the collector receives samples. Once it is expired, the sampler stops sending the samples. It is through the management that the value is set before it expires. The value accepted is within the range of 0 to 2,147,483,647. By default, it is set to 0.

Datagram Size: It is the maximum UDP datagram size to send out the sFlow samples to the receiver. The value accepted is within the range of 200 to 1500 bytes. The default is 1400 bytes.

Buttons:

- **Apply** – Click to save changes.
- **Reset-** Click to restore default settings.

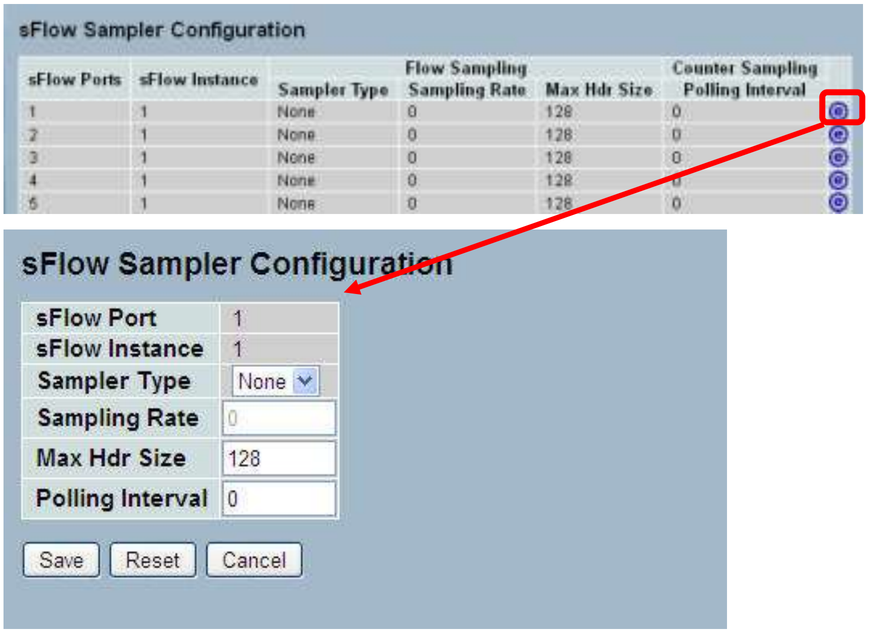
3-15.2 Sampler

The section provides configurations to set or edit the sFlow sampler. what you set or you can edit it for your requirement. An average of 1 out of N packets/operations is randomly sampled. This type of sampling does not provide a 100% accurate result, but it does provide a result with quantifiable accuracy.

Web Interface

To configure the sFlow agent in the web interface:

1. Click Configuration, sFlow Agent, and then sampler.
2. click the ⓔ to edit the sFlow sampler parameters.
3. Choose the sample type with None, Tx, Rx, or All.
4. Click save.
6. Click reset to restore default settings.



sFlow Sampler Configuration

sFlow Ports	sFlow Instance	Sampler Type	Flow Sampling Sampling Rate	Max Hdr Size	Counter Sampling Polling Interval	
1	1	None	0	128	0	ⓔ
2	1	None	0	128	0	ⓔ
3	1	None	0	128	0	ⓔ
4	1	None	0	128	0	ⓔ
5	1	None	0	128	0	ⓔ

sFlow Sampler Configuration

sFlow Port	1
sFlow Instance	1
Sampler Type	None
Sampling Rate	0
Max Hdr Size	128
Polling Interval	0

Figure 3-15.2: The sFlow Sampler Configuration

Parameter Description

sFlow Ports : List of the port numbers on which sFlow is configured.

sFlow Instance : Configured sFlow instance for the port number. Multiple instances of sFlow can be supported on the port.Currently we support one sFlow instance on each port due to hardware limitation.

Flow Sampling : Packet flow sampling refers to arbitrarily choosing some packets out of a specified number, reading the first "Max Hdr Size" bytes and exporting the sampled datagram for analysis. The attributes associated with the flow sampling are: sampler type, sampling rate.

Sampler Type : Configured sampler type on the port and could be any of the types: None, Rx, Tx or All. You can scroll to choice one for your sampler type.By default, The value is “None”.

Sampling Rate : Determines the rate at which samples must be taken on the ports. If sampling rate is configured as 'N',1/N frames is sampled. The sampling rate ranges from 0 to 4095.

- Default value is "0" meaning sampling is disabled on the port.
- If receiver time_out is 0sec, this sFlow configuration is disabled operationally.
- To make it operational the receiver time_out has to remain alive.
- When operational, the sample rate 'N' is rounded off to the nearest possible value.

Max Hdr Size : Configures the size of the header of the sampled frame to be copied to the Queue for further processing. The Max header size ranges from 14 to 200 bytes.Default is 128 bytes.

Counter Sampling : Counter sampling performs periodic,time-based sampling or polling of counters associated with an interface enabled for sFlow.Attribute associated with counter sampling is polling interval.

Polling Interval : Configures the polling interval for the counter sampling. It decides at what regular intervals the counter should be polled for statistics. The accepted value for Counter Polling Interval ranges from 0 to 3600 seconds.Default is 0 seconds which means polling is disabled.

Buttons:

- ⓔ - Edits the port sampler configuration.
- **Apply** – Click to save changes.
- **Reset-** Click to restore default settings.
- **Cancel-** Click to cancel to clear up what your setting.

Auto-Refresh: Click to automatically refresh the information.

Upper right icon (Refresh): Click to manually refresh the information.

3-16 Loop Protection

The loop protection is used to detect the presence of traffic. When the switch receives same packet’s (looping protection frame) MAC address as the one from the port, loop protection will occur. The port will be locked when it received the looping protection frames. If you want to resume the locked port, find the looping path and take off the looping path. Then, select “Resume” to turn on the locked ports.

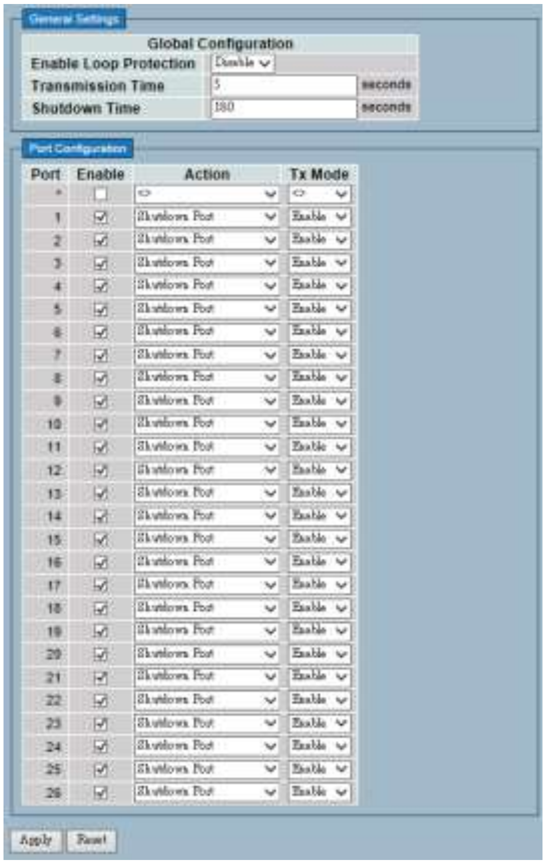
3-16.1 Configuration

The section provides information on how to set loop protection.

Web Interface

To configure the loop protection parameters in the web interface:

1. Click Configuration, Loop Protection, and then Configuration.
2. Select to enable or disable the port loop protection.
3. Click save.
4. Click reset to restore default settings.



General Settings

Global Configuration		
Enable Loop Protection	Disable	
Transmission Time	5	seconds
Shutdown Time	180	seconds

Port Configuration

Port	Enable	Action	Tx Mode
*	□	<>	<>
1	☑	Shutdown Port	Enable
2	☑	Shutdown Port	Enable
3	☑	Shutdown Port	Enable
4	☑	Shutdown Port	Enable
5	☑	Shutdown Port	Enable
6	☑	Shutdown Port	Enable
7	☑	Shutdown Port	Enable
8	☑	Shutdown Port	Enable
9	☑	Shutdown Port	Enable
10	☑	Shutdown Port	Enable
11	☑	Shutdown Port	Enable
12	☑	Shutdown Port	Enable
13	☑	Shutdown Port	Enable
14	☑	Shutdown Port	Enable
15	☑	Shutdown Port	Enable
16	☑	Shutdown Port	Enable
17	☑	Shutdown Port	Enable
18	☑	Shutdown Port	Enable
19	☑	Shutdown Port	Enable
20	☑	Shutdown Port	Enable
21	☑	Shutdown Port	Enable
22	☑	Shutdown Port	Enable
23	☑	Shutdown Port	Enable
24	☑	Shutdown Port	Enable
25	☑	Shutdown Port	Enable
26	☑	Shutdown Port	Enable

Figure 3-16.1: The Loop Protection Configuration

Parameter Description

Enable Loop Protection: This 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.

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 is to shut 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).

Port No: The switch port number of the port.

Enable: This controls whether loop protection is enabled on this switch port.

Action: This 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: This controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

Buttons:

- **Apply** – Click to save changes.
- **Reset-** Click to restore default settings.

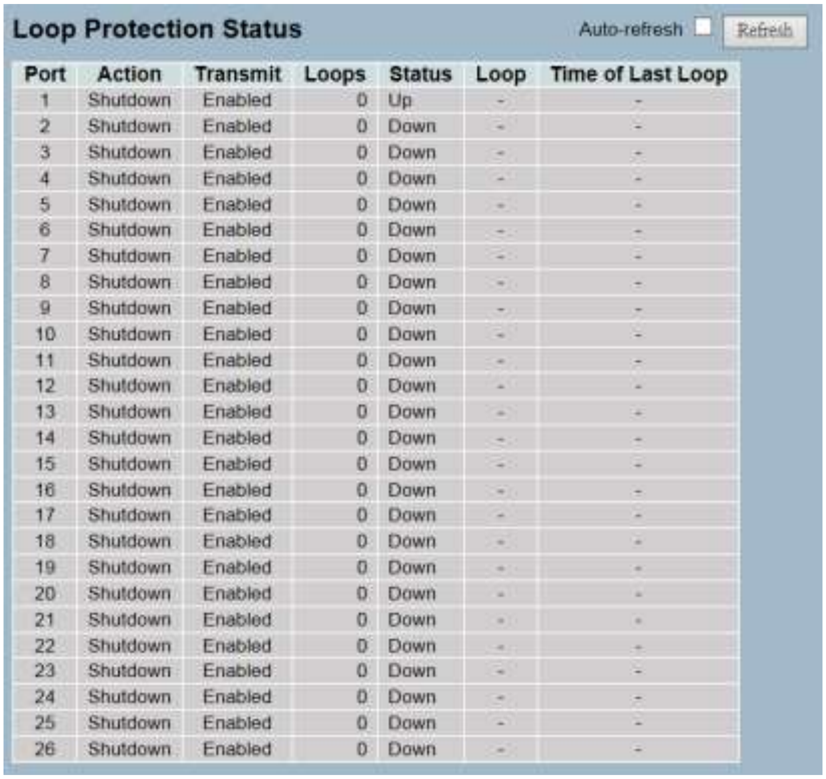
3-16.2 Status

The section provides information on displaying and viewing the loop protection status.

Web Interface

To display the loop protection parameters in the web interface:

1. Click Configuration, Loop protection, and then Status.
2. Select to enable or disable the auto-refresh.
3. Click refresh to update the loop protection record.



Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	0	Up	-	-
2	Shutdown	Enabled	0	Down	-	-
3	Shutdown	Enabled	0	Down	-	-
4	Shutdown	Enabled	0	Down	-	-
5	Shutdown	Enabled	0	Down	-	-
6	Shutdown	Enabled	0	Down	-	-
7	Shutdown	Enabled	0	Down	-	-
8	Shutdown	Enabled	0	Down	-	-
9	Shutdown	Enabled	0	Down	-	-
10	Shutdown	Enabled	0	Down	-	-
11	Shutdown	Enabled	0	Down	-	-
12	Shutdown	Enabled	0	Down	-	-
13	Shutdown	Enabled	0	Down	-	-
14	Shutdown	Enabled	0	Down	-	-
15	Shutdown	Enabled	0	Down	-	-
16	Shutdown	Enabled	0	Down	-	-
17	Shutdown	Enabled	0	Down	-	-
18	Shutdown	Enabled	0	Down	-	-
19	Shutdown	Enabled	0	Down	-	-
20	Shutdown	Enabled	0	Down	-	-
21	Shutdown	Enabled	0	Down	-	-
22	Shutdown	Enabled	0	Down	-	-
23	Shutdown	Enabled	0	Down	-	-
24	Shutdown	Enabled	0	Down	-	-
25	Shutdown	Enabled	0	Down	-	-
26	Shutdown	Enabled	0	Down	-	-

Figure 3-16.2: The Loop Protection Status

Parameter Description

Port: This is the switch port number of the logical port.

Action: This is the currently configured port action.

Transmit: This is the currently configured port transmit mode.

Loops: This is the number of loops detected on this port.

Status: This is the current loop protection status of the port.

Loop: This tells whether a loop is currently detected on the port.

Time of Last Loop: This is the time of the last loop event detected.

Buttons:

- **Refresh –** Click to manually refresh the information.
- **Auto-Refresh-** Click to automatically refresh the information.

3-17 Single IP

Single IP Management (SIM) is a simple and useful method to optimize network utilities and management. It is designed to manage a group of switches as a single entity called a SIM group. Implementing the SIM feature will have the following advantages for users:

- Simplify management of small workgroups or wiring closets while scaling networks to handle increased bandwidth demand.
- Reduces the number of IP addresses needed on the network.
- Virtual stacking structure - Eliminates any specialized cables for stacking and remove the distance barriers that typically limit topology options when using other stacking technology.

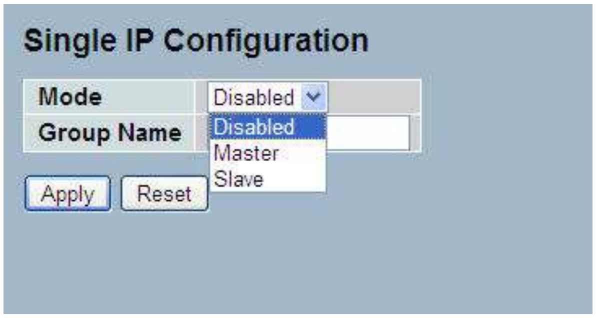
3-17.1 Configuration

The section provides information on setting up configurations for the single IP.

Web Interface

To configure the single IP in the web interface:

1. Click Configuration and then Single IP.
2. Set the parameters.
4. Scroll to choose from disable, master, or slave for the single IP mode.
5. Click save.
6. Click reset to restore default settings.



Single IP Configuration

Mode	Disabled
Group Name	

Figure 3-17.1: The Single IP Configuration

Parameter Description

Mode: The parameter lets you disable the SIP function or set the device become a master or slave. Possible modes are:

- **Disable:** This disables operation of single IP management.
- **Master:** This enables single IP management and to be a master switch. The role is root. If the user connects to the master, it can control the slaves in the same SIP group.
- **Slave:** This enables single IP management and to be a slave switch. The role is slave. The user connects to the slave switch via the master management GUI.

Group Name: The parameter lets you set the name of the single IP group. The available value up to 64 characters that describes the group name.

Buttons:

- **Apply** – Click to save changes.
- **Reset-** Click to restore default settings.

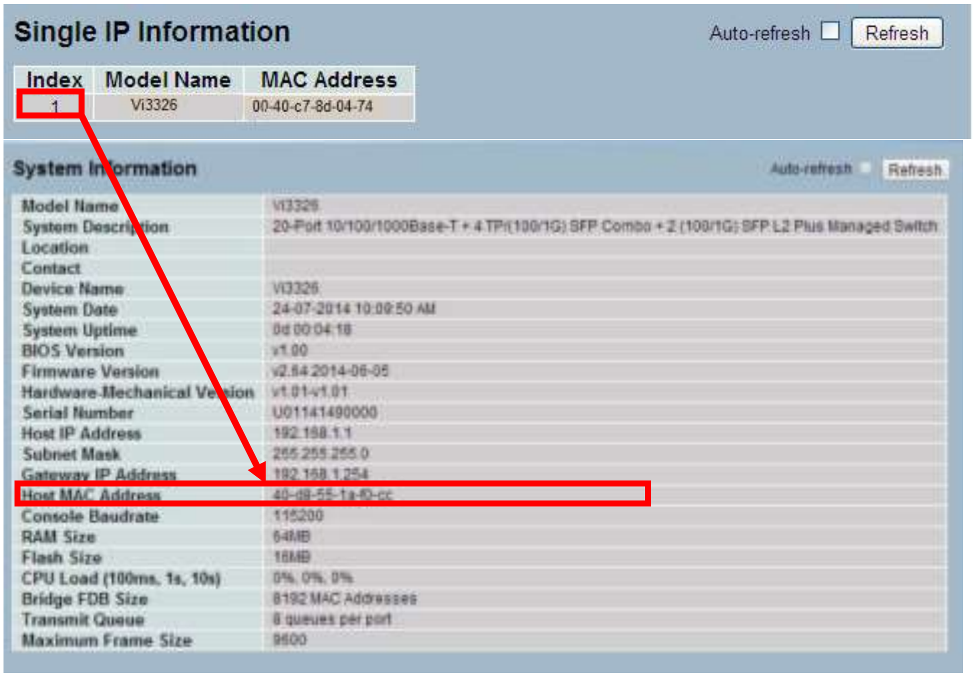
3-17.2 Information

The section provides information on displaying the single IP on the switch.

Web Interface

To show the single IP in the web interface:

1. Click Configuration, Single IP, and then information.
2. Click refresh to manually refresh the information.
3. Click auto-refresh to automaticaslly refresh the information.



Single IP Information

Index	Model Name	MAC Address
1	Vi3326	00-40-c7-8d-04-74

System Information

Model Name	Vi3326
System Description	20-Port 10/100/1000Base-T + 4 TP/(100/1G) SFP Combo + 2 (100/1G) SFP L2 Plus Managed Switch
Location	
Contact	
Device Name	Vi3326
System Date	24-07-2014 10:09:50 AM
System Uptime	0d 00:04:18
BIOS Version	v1.00
Firmware Version	v2.64 2014-06-05
Hardware-Mechanical Version	v1.01-v1.01
Serial Number	U01141490000
Host IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.254
Host MAC Address	40-d8-55-1a-f0-cc
Console Baudrate	115200
RAM Size	64MB
Flash Size	16MB
CPU Load (100ms, 1s, 10s)	0%, 0%, 0%
Bridge FDB Size	8192 MAC Addresses
Transmit Queue	8 queues per port
Maximum Frame Size	9600

Figure 3-17.2: The Single IP Information

Parameter Description

Index: This is the ID of the active slave switch. The parameter tells you how many slave devices are connected to the SIP group.

Model Name: This displays the model name of the slave switch. The parameter lets you to know what kind of devices are joined to this SIP group.

MAC Address: This displays the Ethernet MAC address of the slave switch. The parameter tells you what the device's MAC address is and what joined this SIP group.

Buttons:

- **Refresh –**Click to refresh the page immediately.
- **Auto-Refresh-** Click to automatically refresh the page.

NOTE: When you click the index, you will be redirected to the slave device and will be able to configure and display the device's management settings.

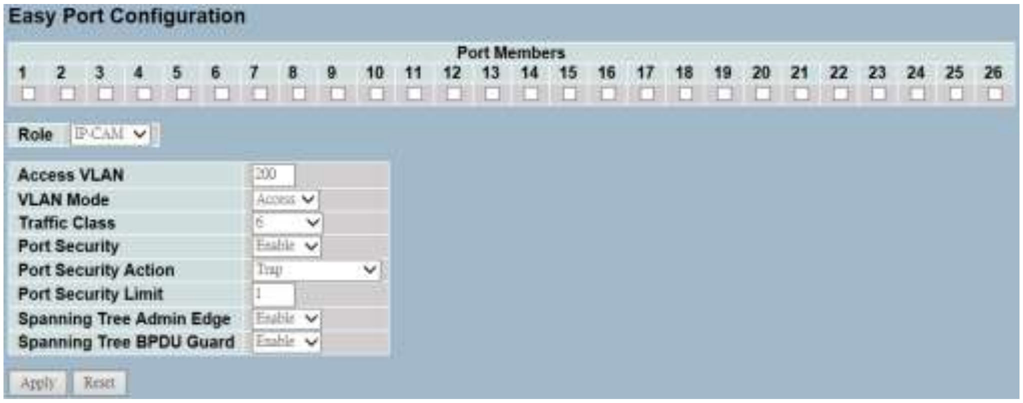
3-18 Easy Port

Easy Port provide a convenient way to save and share common configurations. You can use it to enable features and settings based on the location of a switch in the network and for mass configuration deployments across the network. It is easy to implement voice IP phone, wireless access point, IP cameras, and more. You can also leverage configuration to run a converged voice, video, and data network considering quality of service (QoS), bandwidth, latency, and high performance.

Web Interface

To configure easy port in the web interface:

1. Click Configuration and then Easy Port.
4. Set the parameters.
5. Select the role for the device you want to set easy port on and connect to.
6. Click save.
7. Click reset to restore default settings.



Easy Port Configuration

Port Members

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Role: IP-CAM

Access VLAN	200
VLAN Mode	Access
Traffic Class	6
Port Security	Enable
Port Security Action	Trap
Port Security Limit	1
Spanning Tree Admin Edge	Enable
Spanning Tree BPDU Guard	Enable

Figure 3-18.1: The Easy Port Configuration

Parameter Description

Port Members: A row of check boxes for each port is displayed for each VLAN ID.

- To include a port in an easy port, check the box as ✓.
- Remove or exclude the port from the VLAN, make sure the box is unchecked as shown □.
- By default, no ports are members.

Role: The port role are based on the type of devices to be connected to the switch ports. Select the device you want to connect to and implement the easy port setting on.

Access VLAN: To set the access VLAN ID means the switch port access VLAN ID (AVID). The allowed range is 1 to 4095.

VLAN Mode: Select the port egress rule. The allowed values are hybrid, trunk, or access. This parameter affects the VLAN egress processing. If trunk is selected, a VLAN tag with the classified VLAN ID is inserted in frames transmitted on the port. This mode is normally used for ports connected to VLAN aware switches. If hybrid (default value) is selected, the classified VLAN ID of a frame transmitted on the port is different from the port VLAN ID and a VLAN tag with the classified VLAN ID is inserted in the frame. If access is selected, all untag frames are transmitted on the port.

Voice VLAN: This indicates the voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID, etc. The allowed range is 1 to 4095. If you're connecting the IP phone, you will need to assign the voice VLAN ID.

Traffic Class: Select the traffic class for the data stream priority. The available value from 0 (Low) to 7 (High). If you want the voice to have high priority, then you can set the value with 7.

Port Security: Select to enable or disable the port security function on the port. If you turn on the function, then you need to set port security limit to allow how many devices can access the port via the MAC address.

Port Security Action: If the limit is reached, the switch can take one of the following actions:

- **None:** Does not allow more than the limited MAC addresses on the port, but take no further action.
- **Trap:** If the limit + 1 MAC addresses is seen on the port, it sends an SNMP trap. If aging is disabled, only one SNMP trap will be sent. If aging is enabled, new SNMP traps will be sent everytime the limit gets exceeded.
- **Shutdown:** If the limit + 1 MAC addresses is seen on the port, it shuts down the port. This implies that all secured MAC addresses will be removed from the port and no new address will be learned.

Port Security Limit: This is the maximum number of MAC addresses that can be secured. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken. The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a port security-enabled port. Since all ports draw from the same pool, it may be that a configured maximum cannot be granted if the remaining ports have already used all available MAC addresses.

Spanning Tree Admin Edge: This controls whether the operEdge flag should start as set or cleared. This is the initial operEdge state when a port is initialized.

Spanning Tree BPDU Guard: If it's enabled, it causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port edge status does not effect this setting. A port entering error-disabled state due to this setting is subject to the bridge port error recovery setting as well.

Buttons:

- **Apply** – Click to save changes.
- **Reset-** Click to restore default settings.

3-19 Mirroring

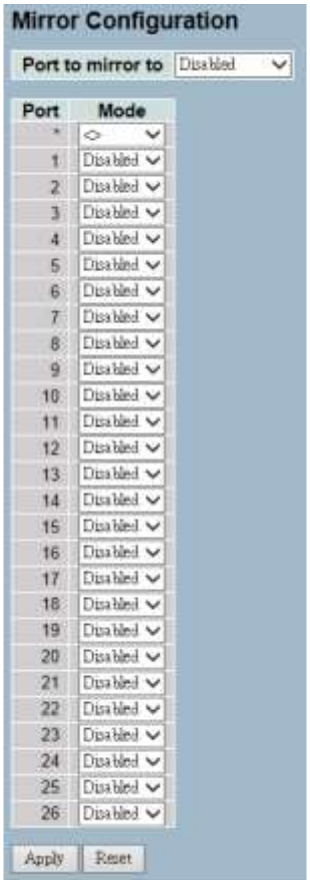
You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

Mirror configuration monitors the traffic of the network. For example, we assume that port A and port B are the monitoring port and the monitored port respectively. Thus, the traffic received by port B will be copied to port A for monitoring.

Web Interface

To configure the mirror in the web interface:

1. Click Configuration and then Mirroring.
2. Select which port to mirror.
3. Select from disabled, enable, TX only, or RX only for the port mirror mode.
4. Click save.
5. Click reset to restore default settings.



Mirror Configuration

Port to mirror to: Disabled

Port	Mode
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled
17	Disabled
18	Disabled
19	Disabled
20	Disabled
21	Disabled
22	Disabled
23	Disabled
24	Disabled
25	Disabled
26	Disabled

Figure 3-19.1: The Mirror Configuration

Parameter Description

Port to Mirror On: Port to mirror is also known as the mirror port. Frames from ports, that have either source (RX) or destination (TX) mirroring enabled, are mirrored on this port. Disabled will turn off mirroring.

Mirror Port Configuration

The following table is used for Rx and Tx enabling.

Port: This is the logical port for the settings contained in the same row.

Mode: Selects mirror mode.

- **Rx Only:** Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored.
- **Tx Only:** Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored.
- **Disabled:** Neither frames transmitted or received are mirrored.
- Enabled Frames received and frames transmitted are mirrored on the mirror port.

NOTE: For a given port, a frame is only transmitted once. Therefore, it is not possible to mirror Tx frames on the mirror port. Because of this, the mode for the selected mirror port is limited to disabled or Rx only.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

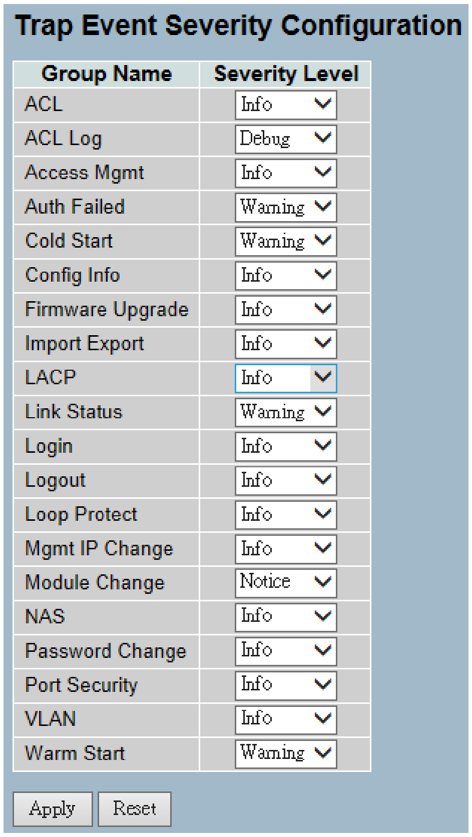
3-20 Trap Event Severity

The trap event severity is used to set an alarm trap and to get the event log. It is used to enable the switch in order to send out the trap information while pre-defined trap events occur.

Web Interface

To configure the trap event severity configuration in the web interface:

1. Click Configuration and then Trap Event Severity Configuration.
2. Select the group name and severity level.
3. Click save.
4. Click reset to restore default settings.



Trap Event Severity Configuration

Group Name	Severity Level
ACL	Info
ACL Log	Debug
Access Mgmt	Info
Auth Failed	Warning
Cold Start	Warning
Config Info	Info
Firmware Upgrade	Info
Import Export	Info
LACP	Info
Link Status	Warning
Login	Info
Logout	Info
Loop Protect	Info
Mgmt IP Change	Info
Module Change	Notice
NAS	Info
Password Change	Info
Port Security	Info
VLAN	Info
Warm Start	Warning

Figure 3-20.1: The Trap Event Severity Configuration

Parameter Description

Group Name: This is the name identifying the severity group.

Severity Level: Select a severity level for each group. The following level types are supported:

- **<0> Emergency:** System is unusable.
- **<1> Alert:** Action must be taken immediately.
- **<2> Critical:** Critical conditions.
- **<3> Error:** Error conditions.
- **<4> Warning:** Warning conditions.
- **<5> Notice:** Normal but significant conditions.
- **<6> Information:** Information messages.
- <**7> Debug:** Debug-level messages.

Buttons:

- **Apply** – Click to save changes.
- **Reset-** Click to restore default settings.

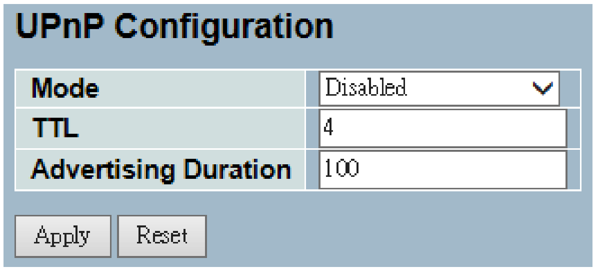
3-21 UpnP

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.

Web Interface

To configure the UPnP configuration in the web interface:

1. Click Configuration and then UpnP.
2. Select to enable or disable UPnP.
3. Specify the parameters.
4. Click save.
5. Click reset to restore default settings.



UPnP Configuration

Mode	Disabled
TTL	4
Advertising Duration	100

Figure 3-21.1: The UPnP Configuration

Parameter Description

These parameters are displayed on the UPnP configuration page.

Mode: This indicates the UPnP operation mode. Possible modes are:

- **Enabled:** This enables the UPnP mode operation.
- **Disable:** This disables the UPnP mode operation.
- When the mode is enabled, two ACEs are added automatically to trap UPNP related packets to CPU. The ACEs are automatically removed when the mode is disabled.

TTL: The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range 1 to 255.

Advertising Duration: The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive an SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it will think that the switch no longer exists. Due to the unreliable nature of UDP, standardly, it is recommended that such refreshing of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. The valid values are in the range 100 to 86400.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

Chapter 4: Security

Chapter 4 provides detailed information on the switch's security configuration tasks to enhance security for local network, which includes IP source guard, ARP inspection, DHCP snooping, AAA, and more.

4-1 IP Source Guard

The section provides configurations for the IP source guard parameters. You can enable or disable the IP source guard on the switch.

4-1.1 Configuration

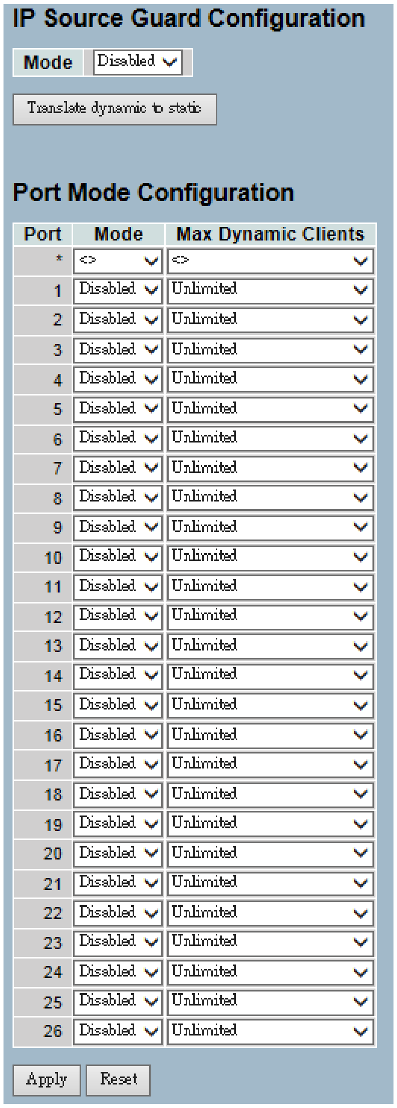
This section provides configuration information for IP source guard.

- Mode (Enabled or Disabled)
- Maximum Dynamic Clients (0, 1, 2, or Unlimited)

Web Interface

To configure an IP source guard in the web interface:

1. Select "Enabled" in the mode of IP source guard configuration.
2. Select "Enabled" of the specific port in the mode of port mode configuration.
3. Select the maximum dynamic clients (0, 1, 2, or Unlimited) of the specific port.
4. Click save.



IP Source Guard Configuration

Mode: Disabled

Port Mode Configuration

Port	Mode	Max Dynamic Clients
*	<>	<>
1	Disabled	Unlimited
2	Disabled	Unlimited
3	Disabled	Unlimited
4	Disabled	Unlimited
5	Disabled	Unlimited
6	Disabled	Unlimited
7	Disabled	Unlimited
8	Disabled	Unlimited
9	Disabled	Unlimited
10	Disabled	Unlimited
11	Disabled	Unlimited
12	Disabled	Unlimited
13	Disabled	Unlimited
14	Disabled	Unlimited
15	Disabled	Unlimited
16	Disabled	Unlimited
17	Disabled	Unlimited
18	Disabled	Unlimited
19	Disabled	Unlimited
20	Disabled	Unlimited
21	Disabled	Unlimited
22	Disabled	Unlimited
23	Disabled	Unlimited
24	Disabled	Unlimited
25	Disabled	Unlimited
26	Disabled	Unlimited

Figure 4-1.1: The IP Source Guard Configuration

Parameter Description

Mode of IP Source Guard Configuration: This enables or disables the global IP source guard. All configured ACEs will be lost when the mode is enabled.

Port Mode Configuration: This specifies which port the IP source guard is enabled on. Only when both global mode and port mode on a given port are enabled, IP source guard is enabled on this port.

Max Dynamic Clients: This specifies 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:

- **Apply** – Click to save changes.
- **Reset -** Click to restore default settings.
- **Translate dynamic to static -** Click to translate all dynamic entries to static entries.

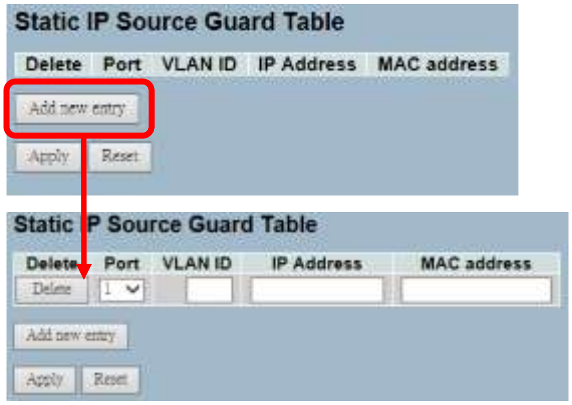
4-1.2 Static Table

The section provides configurations for the static IP source guard table and information on how to manage the entries.

Web Interface

To configure a static IP source guard table configuration in the web interface:

1. Click “Add New Entry”.
2. Specify the port, VLAN ID, IP address, and MAC address in the entry.
3. Click save.



Static IP Source Guard Table

Delete	Port	VLAN ID	IP Address	MAC address

Static IP Source Guard Table

Delete	Port	VLAN ID	IP Address	MAC address
Delete	1			

Figure 4-1.2: The Static IP Source Guard Table

Parameter Description

Delete: Click delete to remove the entry.

Port: This is the logical port for the settings.

VLAN ID: This is the VLAN ID for the settings.

IP Address: This is the allowed source IP address.

IP Mask: This can be used to calculate the allowed network with the IP address.

Adding New Entry: Click to add a new entry to the static IP source guard table. Specify the port, VLAN ID, IP address, and IP mask for the new entry.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

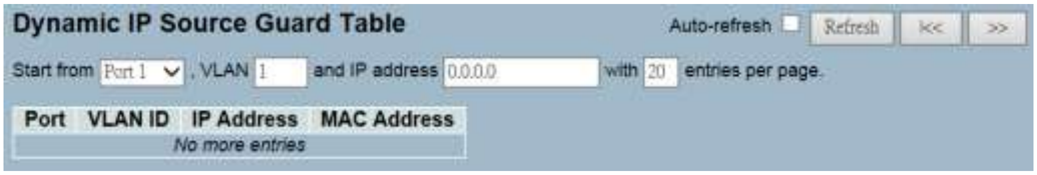
4-1.3 Dynamic Table

The section provides configurations for the dyamic IP source guard table and information on how to manage the entries.

Web Interface

To configure a dynamic IP source guard table configuration in the web interface:

1. Specify the port, VLAN ID, IP address, and entries per page.
2. Check "Auto-refresh".



Dynamic IP Source Guard Table

Auto-refresh □ Refresh |<< >>

Start from Port 1 , VLAN 1 and IP address 0.0.0.0 with 20 entries per page.

Port	VLAN ID	IP Address	MAC Address
No more entries			

Figure 4-1.3: The Dynamic Table

Parameter Description

Port: This is the switch port number for the displayed entries.

VLAN ID: This is VLAN ID that the IP traffic is permitted for.

IP Address: This is the user IP address of the entry.

MAC Address: This is the source MAC address.

Auto-refresh: Click to automatically refresh the information.

Upper right icon (Refresh, <<, >>): Click to manually refresh the table, or to move to the previous or next page.

4-2 ARP Inspection

The section provides configurations for the ARP inspection parameters and information on how to manage the ARP table.

4-2.1 Configuration

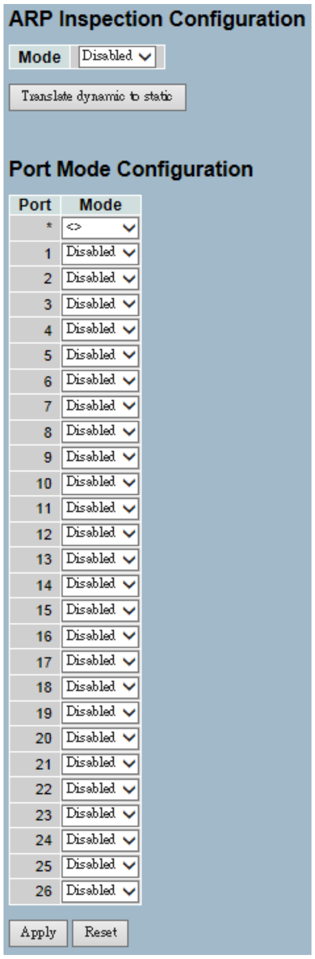
This section provides configuration information for ARP inspection setting, which includes:

- Mode (Enabled or Disabled)
- Port (Enabled or Disabled)

Web Interface

To configure an ARP inspection configuration in the web interface:

1. Select "Enabled" in the mode of ARP inspection configuration.
2. Select "Enabled" for the specific port in the port mode configuration.
3. Click save.



ARP Inspection Configuration

Mode: Disabled

Port Mode Configuration

Port	Mode
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled
17	Disabled
18	Disabled
19	Disabled
20	Disabled
21	Disabled
22	Disabled
23	Disabled
24	Disabled
25	Disabled
26	Disabled

Figure 4-2.1: The ARP Inspection Configuration

Parameter Description

ARP Inspection 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.

Mode of ARP Inspection Configuration: This enables or disables the global ARP inspection.

Port Mode Configuration: This specifies which port ARP inspection is enabled on. Only when both global mode and port mode on a given port are enabled, ARP inspection is enabled on this given port.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.
- **Translate dynamic to static -** Click to translate all dynamic entries to static entries.

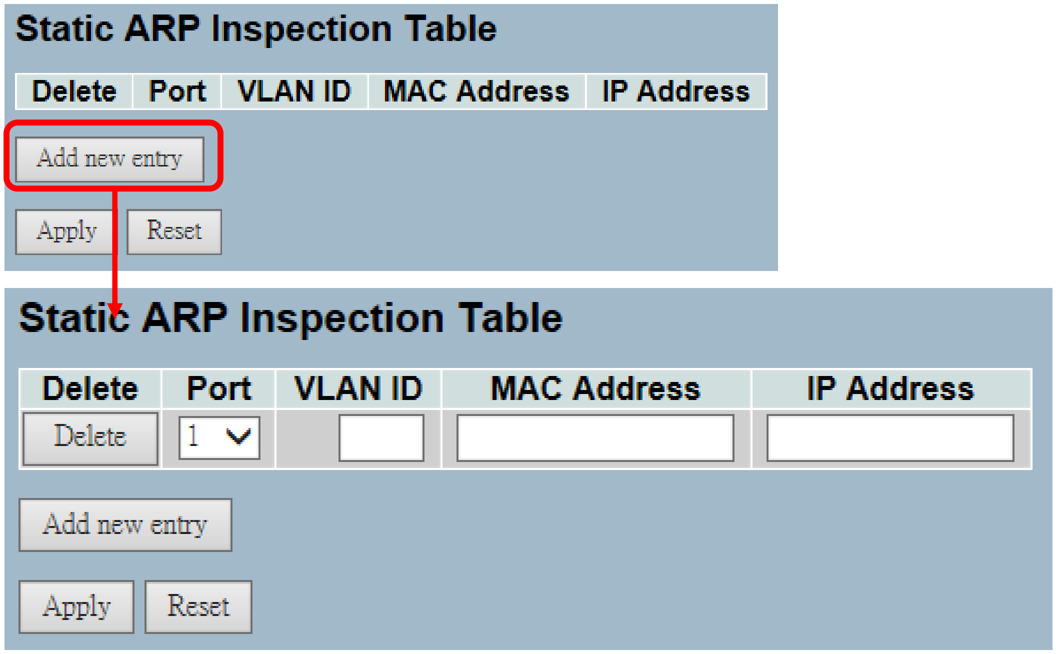
4-2.2 Static Table

The section provides configurations for the static ARP inspection table parameters and information on how to manage the ARP entries.

Web Interface

To configure a static ARP inspection table configuration in the web interface:

1. Click “Add New Entry”.
2. Specify the port, VLAN ID, IP address, and MAC address in the entry.
3. Click save.



Static ARP Inspection Table

Delete	Port	VLAN ID	MAC Address	IP Address

Static ARP Inspection Table

Delete	Port	VLAN ID	MAC Address	IP Address
Delete	1			

Figure 4-2.2: The Static ARP Inspection Table

Parameter Descripton

Delete: Click delete to remove the entry.

Port: This is the logical port for the settings.

VLAN ID: This is the VLAN ID for the settings.

MAC Address: This is the allowed source MAC address in ARP request packets.

IP Address: This is the allowed source IP address in ARP request packets.

Adding new entry: Click to add a new entry to the static ARP inspection table. Specify the port, VLAN ID, MAC address, and IP address for the new entry.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

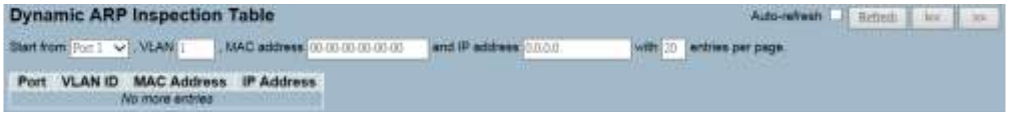
4-2.3 Dynamic Table

The section provides configurations for the dynamic ARP inspection table parameters. It contains up to 1024 entries. It is sorted by port, VLAN ID, Mac address and then by IP address.

Web Interface

To configure a dynamic ARP inspection table configuration in the web interface:

1. Specify the port, VLAN ID, MAC address, IP address, and entries per page.
2. Check “Auto-refresh”.



Dynamic ARP Inspection Table

Auto-refresh □

Start from Port 1 , VLAN 1 , MAC address 00-00-00-00-00-00 and IP address 0.0.0.0 with 20 entries per page.

Port	VLAN ID	MAC Address	IP Address
No more entries			

Figure 4-2.3: The Dynamic ARP Inspection Table

Parameter Description

Port: This is the switch port number.

VLAN ID: This is the VLAN ID that the ARP traffic is permitted for.

MAC Address: This is the user MAC address of the entry.

IP Address: This is the user IP address of the entry.

Auto-refresh: Click to automatically refresh the information.

Upper right icon (Refresh, <<, >>): Click to manually refresh the table, or to move to the previous or next page.

4-3 DHCP Snooping

The section provides configurations for the DHCP snooping parameters. The DHCP snooping can prevent attackers from adding their own DHCP servers to the network.

4-3.1 Configuration

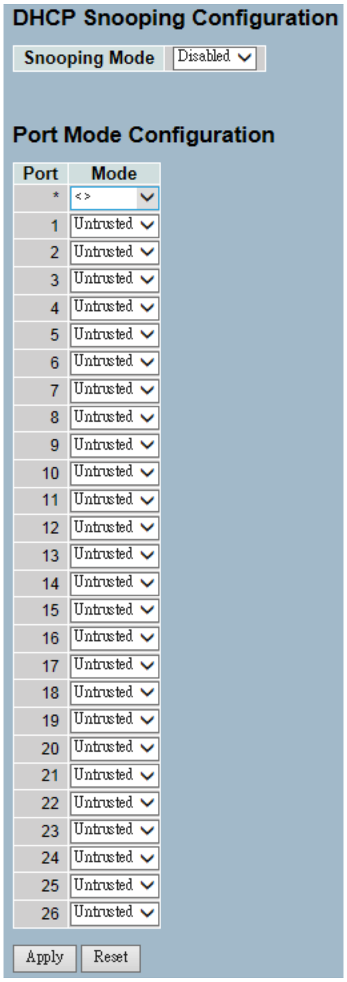
This section provides configuration information for the DHCP snooping settings, which includes:

- Snooping Mode (Enabled or Disabled)
- Port Mode Configuration (Trusted or Untrusted)

Web Interface

To configure a DHCP snooping in the web interface:

1. Select “Enabled” in the mode of DHCP snooping configuration.
2. Select “Trusted” of the specific port in the port mode configuration.
3. Click save.



DHCP Snooping Configuration

Snooping Mode: Disabled

Port Mode Configuration

Port	Mode
*	<>
1	Untrusted
2	Untrusted
3	Untrusted
4	Untrusted
5	Untrusted
6	Untrusted
7	Untrusted
8	Untrusted
9	Untrusted
10	Untrusted
11	Untrusted
12	Untrusted
13	Untrusted
14	Untrusted
15	Untrusted
16	Untrusted
17	Untrusted
18	Untrusted
19	Untrusted
20	Untrusted
21	Untrusted
22	Untrusted
23	Untrusted
24	Untrusted
25	Untrusted
26	Untrusted

Figure 4-3.1: The DHCP Snooping Configuration

Parameter Description

Snooping Mode: This indicates the DHCP snooping mode operation. Possible modes are:

- **Enabled:** This enables the 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:** This disables the DHCP snooping mode operation.

Port Mode: This indicates the DHCP snooping port mode. Possible port modes are:

- **Trusted:** This configures the port as trusted source of the DHCP messages.
- **Untrusted:** This configures the port as untrusted source of the DHCP messages.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

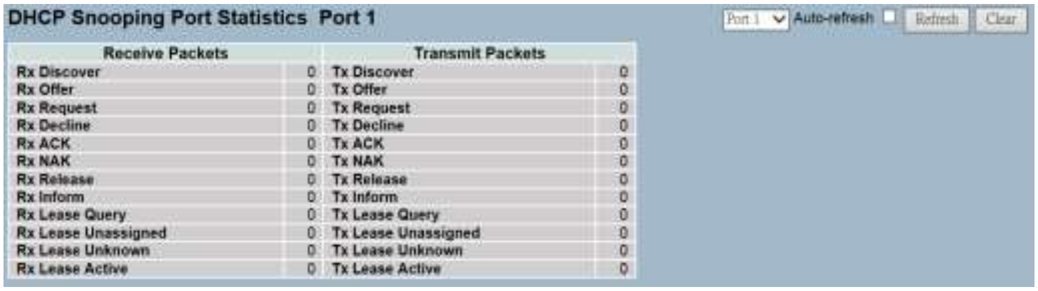
4-3.2 Statistics

The section provides information regarding the DHCP snooping statistic information. The statistics show only packet counters when DHCP snooping is enabled and the relay mode is disabled. It does not count the DHCP packets for the DHCP client.

Web Interface

To configure a DHCP snooping statistics configuration in the web interface:

1. Specify the port that you want to monitor.
2. Check “Auto-refresh”.



DHCP Snooping Port Statistics Port 1

Receive Packets		Transmit Packets	
Rx Discover	0	Tx Discover	0
Rx Offer	0	Tx Offer	0
Rx Request	0	Tx Request	0
Rx Decline	0	Tx Decline	0
Rx ACK	0	Tx ACK	0
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	0	Tx Inform	0
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
Rx Lease Unknown	0	Tx Lease Unknown	0
Rx Lease Active	0	Tx Lease Active	0

Figure 4-3.2: The DHCP Snooping Port Statistics

Parameter Description

Rx and Tx Discover: This is the number of discover (option 53 with value 1) packets received and transmitted.

Rx and Tx Offer: This is the number of offer (option 53 with value 2) packets received and transmitted.

Rx and Tx Request: This is the number of request (option 53 with value 3) packets received and transmitted.

Rx and Tx Decline: This is the number of decline (option 53 with value 4) packets received and transmitted.

Rx and Tx ACK: This is the number of ACK (option 53 with value 5) packets received and transmitted.

Rx and Tx NAK: This is the number of NAK (option 53 with value 6) packets received and transmitted.

Rx and Tx Release: This is the number of release (option 53 with value 7) packets received and transmitted.

Rx and Tx Inform: This is the number of inform (option 53 with value 8) packets received and transmitted.

Rx and Tx Lease Query: This is the number of lease query (option 53 with value 10) packets received and transmitted.

Rx and Tx Lease Unassigned: This is the number of lease unassigned (option 53 with value 11) packets received and transmitted.

Rx and Tx Lease Unknown: This is the number of lease unknown (option 53 with value 12) packets received and transmitted.

Rx and Tx Lease Active: This is the number of lease active (option 53 with value 13) packets received and transmitted.

Auto-Refresh: Click to automatically refresh the information.

Upper Right Icon (Refresh, Clear): Click to manually refresh or clear the information.

4-4 DHCP Relay

The section provides information on how to forward the DHCP requests to another specific DHCP servers via DHCP relay. The DHCP servers may be on another network.

4-4.1 Configuration

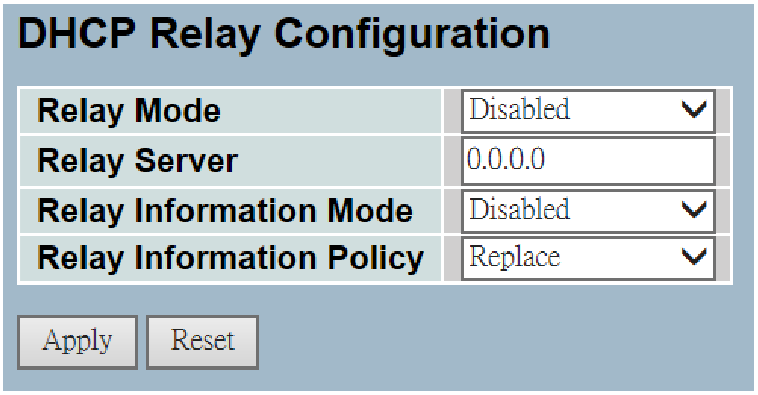
This section provides configurations for the DHCP relay setting:

- Relay Mode (Enabled or Disabled)
- Relay Server IP Setting
- Relay Information Mode (Enabled or Disabled)
- Relay Information Mode Policy (Replace, Keep, or Drop)

Web Interface

To configure a DHCP relay in the web interface:

1. Select “Enabled” in the DHCP relay mode.
2. Specify relay server IP address.
3. Select “Enabled” in the relay information mode.
4. Specify Relay (Replace, Keep, or Drop) in the relay information mode.
5. Click save.



DHCP Relay Configuration

Relay Mode	Disabled
Relay Server	0.0.0.0
Relay Information Mode	Disabled
Relay Information Policy	Replace

Figure 4-4.1: The DHCP Relay Statistics

Parameter Description

Relay Mode: This indicates the DHCP relay mode operation. Possible modes are:

- **Enabled:** This enables the DHCP relay mode operation. When the 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. The DHCP broadcast message won't be flooded for security considerations.
- **Disabled:** This disables the DHCP relay mode operation.

Relay Server: This indicates the DHCP relay server IP address. 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.

Relay Information Mode: This indicates the DHCP relay information mode option operation. Possible modes are:

- **Enabled:** This enables the 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:** This disables the DHCP relay information mode operation.

Relay Information Policy: This indicates the DHCP relay information option policy. When the DHCP relay information mode operation is enabled, if the agent receives a DHCP message that already contains relay agent information, it will enforce the policy. It only works under DHCP if relay information operation mode is enabled. Possible policies are:

- **Replace:** This replaces the original relay information when a DHCP message that already contains it is received.
- **Keep:** This keeps the original relay information when a DHCP message that already contains it is received.
- **Drop:** This drops the package when a DHCP message that already contains relay information is received.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

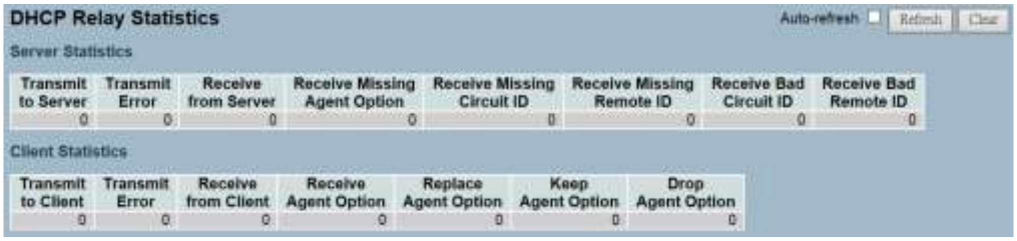
4-4.2 Statistics

The section provides information regarding the DHCP relay statistics information. The statistics show both server and client packet counters when the DHCP relay mode is enabled.

Web Interface

To configure a DHCP snooping statistics configuration in the web interface:

1. Check “Auto-refresh”.



DHCP Relay Statistics

Server Statistics

Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID	Receive Bad Circuit ID	Receive Bad Remote ID
0	0	0	0	0	0	0	0

Client Statistics

Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option
0	0	0	0	0	0	0

Figure 4-4.2: The DHCP Relay Statistics

Parameter Description

Transmit to Server: This is the number of packets that are relayed from client to server.

Transmit Error: This is the number of packets that resulted in errors while being sent to clients.

Receive from Server: This is the number of packets received from server.

Receive Missing Agent Option: This is the number of packets received without agent information options.

Receive Missing Circuit ID: This is the number of packets received with the Circuit ID option missing.

Receive Missing Remote ID: This is the number of packets received with the Remote ID option missing.

Receive Bad Circuit ID: This is the number of packets whose Circuit ID option did not match known circuit ID.

Receive Bad Remote ID: This is the number of packets whose Remote ID option did not match known Remote ID.

Client Statistics

Transmit to Client: This is the number of relayed packets from server to client.

Transmit Error: This is the number of packets that resulted in error while being sent to servers.

Receive from Client: This is the number of received packets from server.

Receive Agent Option: This is the number of received packets with relay agent information option.

Replace Agent Option: This is the number of packets which were replaced with relay agent information option.

Keep Agent Option: This is the number of packets whose relay agent information was retained.

Drop Agent Option: This is the number of packets that were dropped which were received with relay agent information.

Auto-Refresh: Click to automatically refresh the information.

Upper Right Icon (Refresh, Clear): Click to manually refresh or clear the information.

4-5 NAS

The section provides configurations for the NAS parameters. The NAS server can be employed to connect users to a variety of resources including internet access, conference calls, printing documents on shared printers, or by simply logging on to the Internet.

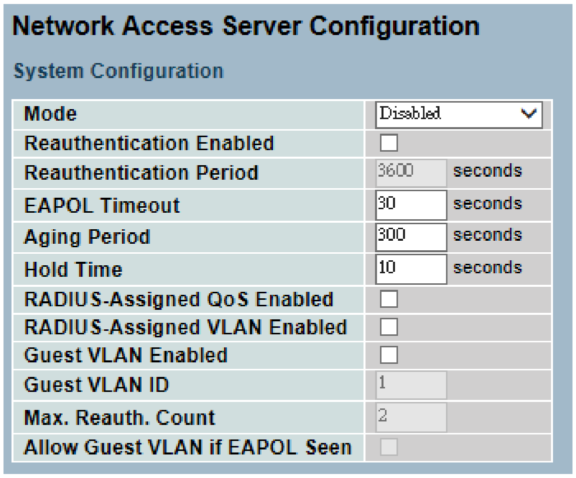
4-5.1 Configuration

This section provides configuration information for the NAS setting of IEEE 802.1X, Mac-bsed authentication system and port settings. The NAS configuration consists of two sections: system-wide and port-wide.

Web Interface

To configure a system configuration of network access server in the web interface:

1. Select “Enabled” in the mode of netwrok access server configuration.
2. Checked reauthentication enabled.
3. Set the reauthentication period. The default is 3600 seconds.
4. Set the EAPOL timeout. The default is is 30 seconds.
5. Set the aging peroid. The default is 300 seconds.
6. Set the hold time. The default is 10 seconds.
7. Checked radius-assigned QoS enabled.
8. Checked radius-assigned VLAN enabled.
9. Checked guest VLAN enabled.
10. Specify the guest VLAN ID.
11. Specify the max. reauth. count.
12. Checked allow guest VLAN if EAPOL seen.
13. Click save.

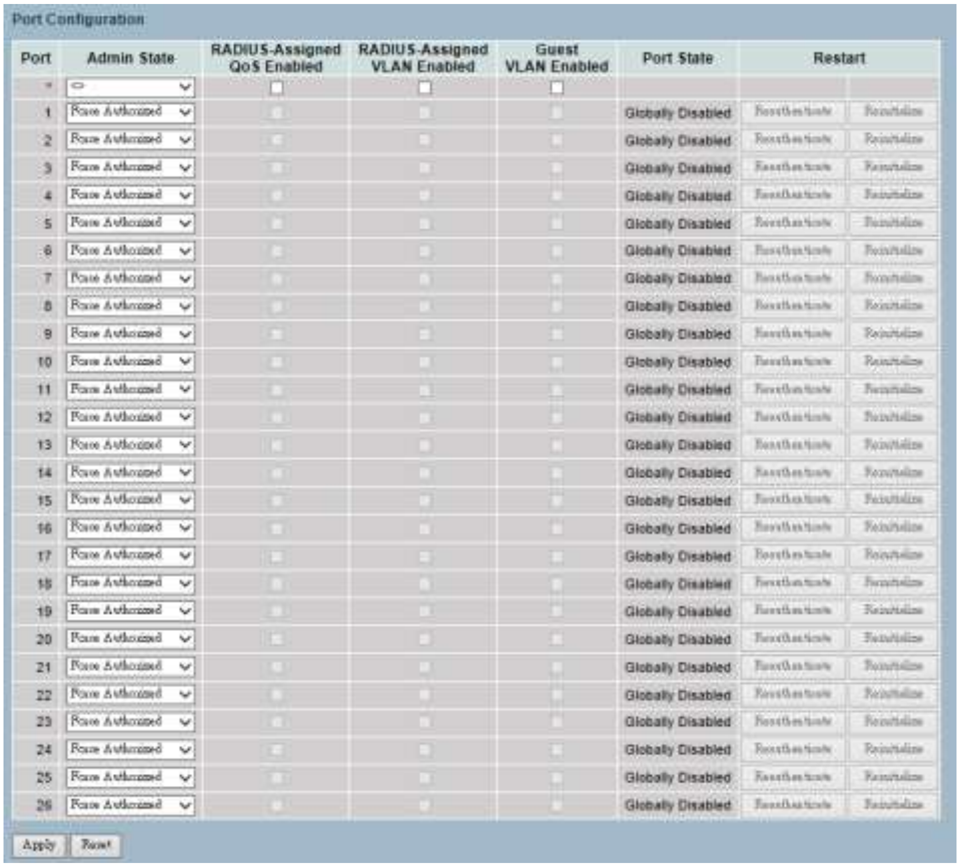


Network Access Server Configuration

System Configuration

Mode	Disabled	
Reauthentication Enabled	□	
Reauthentication Period	3600	seconds
EAPOL Timeout	30	seconds
Aging Period	300	seconds
Hold Time	10	seconds
RADIUS-Assigned QoS Enabled	□	
RADIUS-Assigned VLAN Enabled	□	
Guest VLAN Enabled	□	
Guest VLAN ID	1	
Max. Reauth. Count	2	
Allow Guest VLAN if EAPOL Seen	□	

Figure 4-5.1: The Network Access Server Configuration



Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
*	<>	□	□	□			
1	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
3	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
4	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
5	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
6	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
7	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
8	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
9	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
10	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
11	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
12	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
13	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
14	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
15	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
16	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
17	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
18	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
19	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
20	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
21	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
22	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
23	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
24	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
25	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
26	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize

Parameter Description

Mode: This indicates if the NAS is globally enabled or disabled on the switch. If it's globally disabled, all ports are allowed to forward the frames.

Reauthentication Enabled: If this is 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: This determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the reauthentication is enabled. Valid values are in the range 1 to 3600 seconds.

EAPOL Timeout: This determines the time for retransmission of request identity EAPOL frames. Valid values are in the range 1 to 255 seconds. This has no effect for MAC-based ports.

Aging Period: This setting applies to the following modes (e.g. 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 the MAC addresses, the port security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds.

If reauthentication is enabled and the port is in 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 doesn't cause direct communication between the switch and the client. 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 (e.g. modes using the port security functionality to secure MAC addresses):

- Single 802.1X
- Multi 802.1X
- MAC-Based Auth.

If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration→Security→AAA" page) - the client is put on hold in the unauthorized state. The hold timer does not count during an on-going authentication.

In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time.

The hold time can be set to a number between 10 and 1000000 seconds.

RADIUS-Assigned QoS Enabled: RADIUS-assigned QoS provides a means to centrally control the traffic class, to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-assigned QoS enabled below).

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 the RADIUS-assigned QoS Class is enabled on that port. When unchecked, the 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 below).

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 the RADIUS-assigned VLAN is enabled on that port. When unchecked, the 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.

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 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 of 1 to 4095.

Max. Reauth. Count: This is the number of times the switch transmits an EAPOL request identity frame without responses, before considering entering the guest VLAN. The value can only be changed if the guest VLAN option is globally enabled. Valid values are in the range 1 to 255.

Allow Guest VLAN if EAPOL Seen: The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port. The value can only be changed if the guest VLAN option is globally enabled.

Port Configuration

The table has one row for each port on the selected switch and a number of columns, which are:

Port: This is the port number which the configuration applies to.

Admin State: If the 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 becuase it allows for different authentication methods such as MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When the authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

NOTE: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead). If the supplicant retransmits EAPOL start frames at a rate faster than X seconds, then it will never get authenticated because the switch will cancel the on-going backend authentication server requests whenever it receives a new EAPOL start frame from the supplicant.

Since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL start frame retransmission rate.

Single 802.1X: In a 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 (through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the single 802.1X variant. Single 802.1X is really 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 doesn't 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: In a 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 (through a hub) to piggy-back on the successfully authenticated client and get network access, even though they really aren't authenticated. To overcome this security breach, use the multi 802.1X variant.

Multi 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. 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. 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 supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.

MAC-base Auth.: Unlike the port-based 802.1X, the MAC-based authentication is not a standard. It is merely a best-practices method adopted by the industry. In the 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. In turn, it 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”. A dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-challenge authentication method, so the RADIUS server must be configured accordingly.

When the authentication is complete, the RADIUS server sends a success or failure indication. In turn, it causes the switch to open up or block traffic for that particular client by 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. Therefore, a 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. The clients don't need special supplicant software to authenticate. The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. 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 the RADIUS-Assigned QoS is both globally enabled and enabled 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 it’s 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. This may be changed by the administrator without affecting the RADIUS-assigned.

This option is only available for single-client modes.

- Port-based 802.1X
- Single 802.1X

RADIUS attributes used in identifying a QoS Class:

Refer to the written documentation for a description of the RADIUS attributes needed in order to successfully identify 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 of 0 to 3, which translates into the desired QoS class in the range of 0 to 3.

RADIUS-Assigned VLAN Enabled: When the RADIUS-assigned VLAN is both globally enabled and enabled 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 it’s present and valid, the port's 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. This may be changed by the administrator without affecting the RADIUS-assigned.

This option is only available for single-client modes.

- Port-based 802.1X
- Single 802.1X

For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" 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 fulfill 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 of 0 to 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 of 1 to 4095.

Guest VLAN Enabled: When the guest VLAN is both globally enabled and enabled 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.

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" 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 and no EAPOL frames have been received, 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” is enabled, the port will now be placed in the guest VLAN. If it’s 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. If it’s not, the port will be placed in the guest VLAN.

Otherwise, it will not move to the guest VLAN and will 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. 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: This is 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 or a single-supplicant mode and the supplicant is authorized.
- **Unauthorized:** The port is in force unauthorized 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 is in an EAPOL-based or MAC-based mode.

Clicking these buttons will not cause settings changed on the page to take effect.

- **Reauthenticate:** Schedules a reauthentication when 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:** This 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.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

Upper Right Icon (Refresh): Click to manually refresh the information.

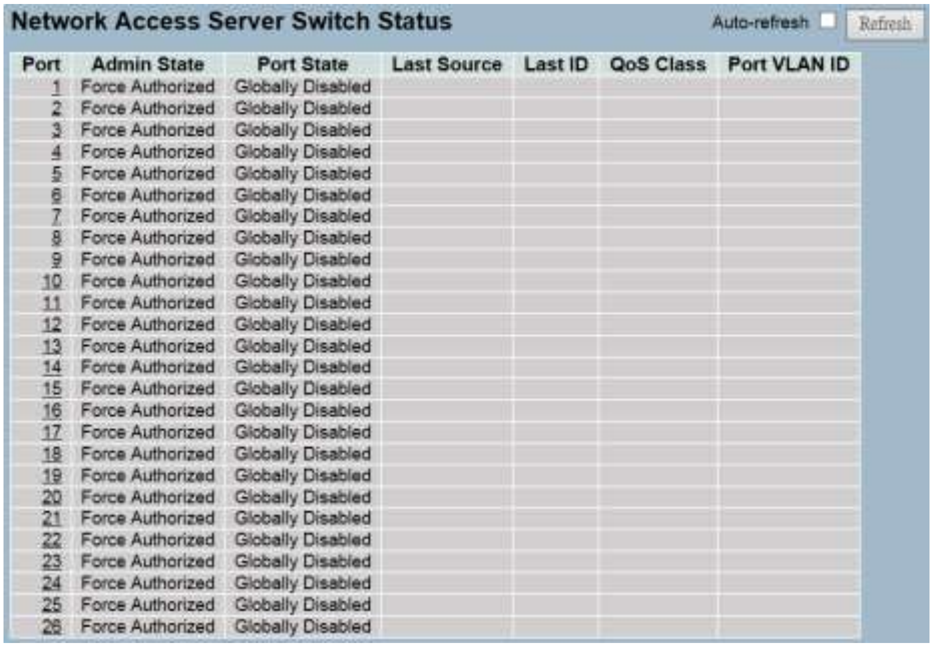
4-5.2 Switch Status

The section provides information for each port NAS status. This includes admin state port state, last source, last ID, QoS class, and port VLAN ID.

Web Interface

To configure a NAS switch status configuration in the web interface:

1. Check "Auto-refresh".



Network Access Server Switch Status

Auto-refresh □ Refresh

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled				
2	Force Authorized	Globally Disabled				
3	Force Authorized	Globally Disabled				
4	Force Authorized	Globally Disabled				
5	Force Authorized	Globally Disabled				
6	Force Authorized	Globally Disabled				
7	Force Authorized	Globally Disabled				
8	Force Authorized	Globally Disabled				
9	Force Authorized	Globally Disabled				
10	Force Authorized	Globally Disabled				
11	Force Authorized	Globally Disabled				
12	Force Authorized	Globally Disabled				
13	Force Authorized	Globally Disabled				
14	Force Authorized	Globally Disabled				
15	Force Authorized	Globally Disabled				
16	Force Authorized	Globally Disabled				
17	Force Authorized	Globally Disabled				
18	Force Authorized	Globally Disabled				
19	Force Authorized	Globally Disabled				
20	Force Authorized	Globally Disabled				
21	Force Authorized	Globally Disabled				
22	Force Authorized	Globally Disabled				
23	Force Authorized	Globally Disabled				
24	Force Authorized	Globally Disabled				
25	Force Authorized	Globally Disabled				
26	Force Authorized	Globally Disabled				

Figure 4-5.2: The Network Access Server Switch Status

Parameter Description

Port: This is the switch port number. Click to navigate to detailed NAS statistics for this port.

Admin State: This is the port's current administrative state. Refer to NAS admin state for a description of possible values.

Port State: This is the current state of the port. Refer to NAS port state for a description of the individual states.

Last Source: This is 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: This is the user name (supplicant identity) carried in the most recently received response identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

QoS Class: This is the QoS class assigned to the port by the RADIUS server if enabled.

Port VLAN ID: This is 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. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.

Auto-Refresh: Click to automatically refresh the information.

Upper Right Icon (Refresh): Click to manually refresh the information.

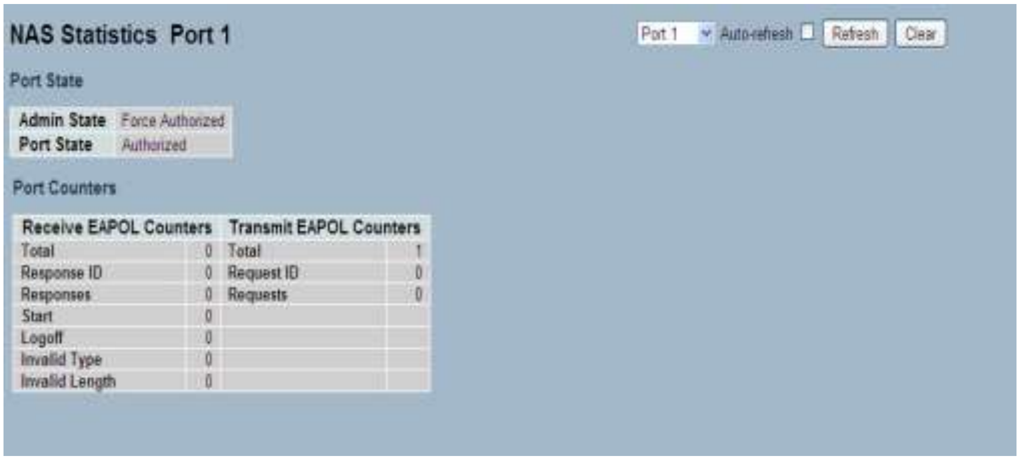
4-5.3 Port Status

The section provides detailed NAS statistics for a specific port that is running EAPOL-based IEEE 802.1X authentication.

Web Interface

To configure a NAS port status configuration in the web interface:

1. Specify which port you would like to check.
2. Check “Auto-refresh”.



NAS Statistics Port 1

Port State

Admin State	Force Authorized
Port State	Authorized

Port Counters

Receive EAPOL Counters		Transmit EAPOL Counters	
Total	0	Total	1
Response ID	0	Request ID	0
Responses	0	Requests	0
Start	0		
Logoff	0		
Invalid Type	0		
Invalid Length	0		

Figure 4-5.3: The NAS Statistics

Parameter Description

Port State

Admin State: This is the port's current administrative state. Refer to NAS admin state for a description of possible values.

Port State: This is the current state of the port. Refer to NAS port state for a description of the individual states.

QoS Class: This is the QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.

Port VLAN ID: This is 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. If the port is moved to the guest VLAN, "(Guest)" is appended to the VLAN ID.

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

Backend Server Counters: These backend (RADIUS) frame counters are available for the following administrative states:

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

Last Supplicant/Client Info: This is information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states:

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

Selected Counters

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 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: This 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. As long as the backend server hasn't 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: This shows the date and time of the last authentication of the client (successful and unsuccessful).

Auto-Refresh: Click to automatically refresh the information.

Upper Right Icon (Refresh, Clear): Click to manually refresh or clear the information.

4-6 AAA

This section provides information on using an AAA (Authentication, Authorization, Accounting) server to provide access control to the network. The AAA server can be a TACACS+ or RADIUS server to create and manage objects that contain settings for using AAA servers.

4-6.1 Configuration

This section provides configuration information for AAA settings of TACACS+ or RADIUS server.

Web Interface

To configure a common configuration of AAA in the web interface:

1. Set the timeout. The default is 15 seconds.
2. Set the dead time. The default is 300 seconds.

To configure a TACACS+ authorization and accounting configuration of AAA in the web interface:

1. Select “Enabled” in the authorization.
2. Select “Enabled” in the failback to local authorization.
3. Select “Enabled” in the account.

To configure a RADIUS authentication server configuration of AAA in the web interface:

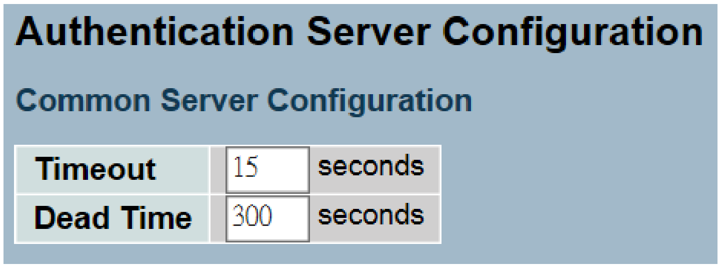
1. Check “Enabled”.
2. Specify the IP address or hostname for radius server.
3. Specify the authentication port for radius server. The default is 1812.
4. Specify the secret with radius server.

To configure a RADIUS accounting server configuration of AAA in the web interface:

1. Check “Enabled”.
2. Specify the IP address or hostname for radius server.
3. Specify the accounting port for radius server. The default is 1813.
4. Specify the secret with radius server.

To configure a TACACS+ authentication server configuration of AAA in the web interface:

1. Check “Enabled”.
2. Specify the IP address or hostname for TACACS+ server.
3. Specify the authentication port for TACACS+ server. The default is 49.
4. Specify the secret with TACACS+ server.

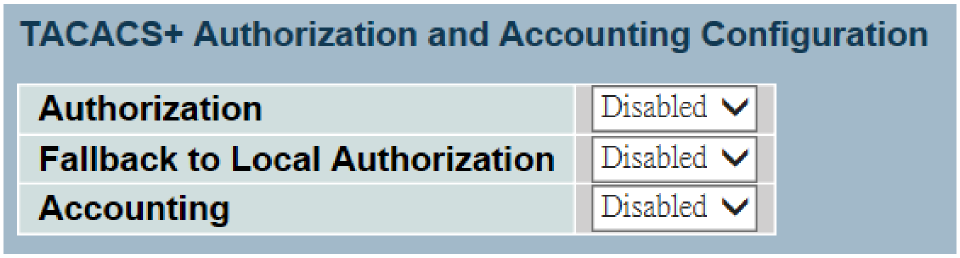


Authentication Server Configuration

Common Server Configuration

Timeout	15	seconds
Dead Time	300	seconds

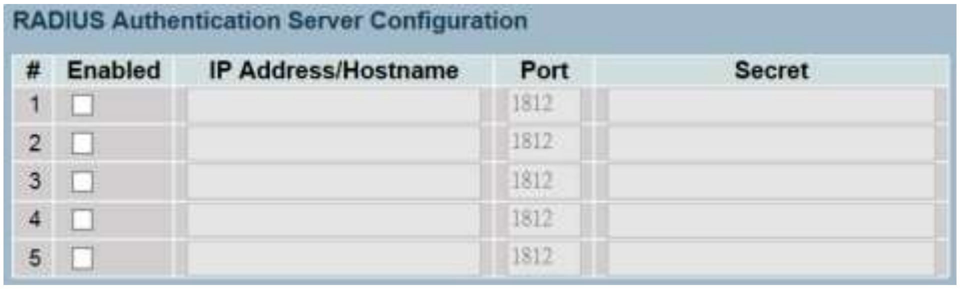
Figure 4-5.3.1: The Common Server Configuration



TACACS+ Authorization and Accounting Configuration

Authorization	Disabled
Fallback to Local Authorization	Disabled
Accounting	Disabled

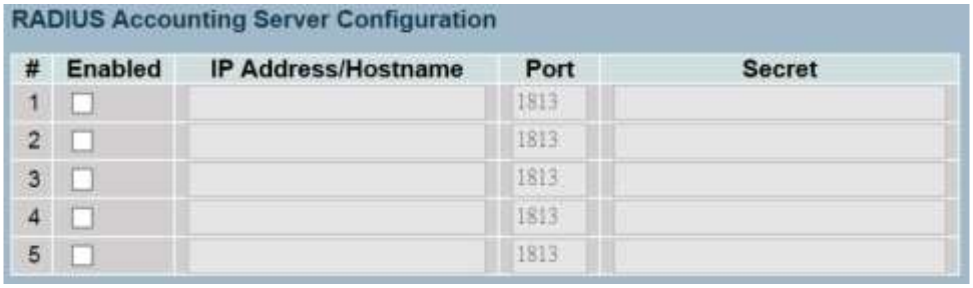
Figure 4-5.3.2: The TACACS+ Accounting Configuration



RADIUS Authentication Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	□		1812	
2	□		1812	
3	□		1812	
4	□		1812	
5	□		1812	

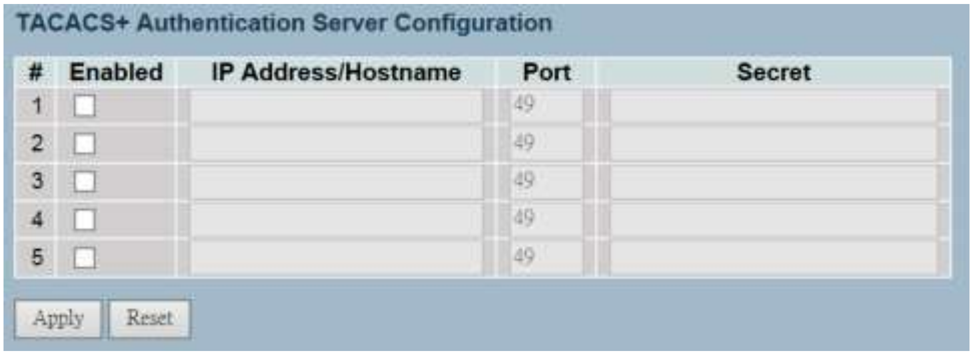
Figure 4-5.3.3: The RADIUS Configuration



RADIUS Accounting Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	□		1813	
2	□		1813	
3	□		1813	
4	□		1813	
5	□		1813	

Figure 4-5.3.4: The RADIUS Accounting Configuration



TACACS+ Authentication Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	□		49	
2	□		49	
3	□		49	
4	□		49	
5	□		49	

Figure 4-5.3.4: The TACACS+ Authentication Configuration

Parameter Description

Timeout: The timeout is the maximum time to wait for a reply from a server. This can be set to a number between 3 and 3600 seconds. If the server does not reply within this timeframe, we will consider it to be dead and continue with the next enabled server (if any).

RADIUS servers are using the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead.

Dead Time: The dead time 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 can be set to a number between 0 and 3600 seconds. This will stop the switch from continually trying to contact a server that it has already determined as dead.

Setting the dead time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

TACACS+ Authorization and Accounting Configuration

Authorization: Every CLI commands will be authorized by TACACS+ server when enabled. The authorization table on the TACACS+ server is able to configure which CLI command can pass successfully. For example, the TACACS+ server is set to accept STP command but deny VLAN command. The server will block the command related to STP which entered by user, but it can allow VLAN command to configure successfully when user enter VLAN command.

Fallback to Local Authorization: Enable to allow the user who typed wrong account or password to login successfully when the user account is on the local authorization list of the local switch. For example, when user entered the wrong account or password, the TACACS+ server will refer to the account information on the local end of switch. If the account is recorded on the local switch, the user will be authorized to login with the privilege level set on the local switch.

Accounting: Enable to record all the command user entered. All the log data will be recorded on the server when enable. For instance, login time, log out time, IGMP setting, VLAN setting, etc.

RADIUS Authentication Server Configuration

The table has one row for each RADIUS authentication server and a number of columns, which are:

#: This is the RADIUS authentication server number for which the configuration below applies.

Enabled: This enables the RADIUS authentication server.

IP Address/Hostname: This is the IP address or hostname of the RADIUS authentication server. IP address is expressed in dotted decimal notation.

Port: This is the UDP port to use on the RADIUS authentication server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS authentication server.

Secret: This is the secret (up to 29 characters long) shared between the RADIUS authentication server and the switch.

RADIUS Accounting Server Configuration

The table has one row for each RADIUS Accounting Server and a number of columns, which are:

#: This is the RADIUS accounting server number for which the configuration below applies.

Enabled: This enables the RADIUS accounting server.

IP Address/Hostname: The IP address or hostname of the RADIUS accounting server. IP address is expressed in dotted decimal notation.

Port: This is the UDP port to use on the RADIUS accounting server. If the port is set to 0 (zero), the default port (1813) is used on the RADIUS accounting server.

Secret: This is the secret (up to 29 characters long) shared between the RADIUS accounting server and the switch.

TACACS+ Authentication Server Configuration

The table has one row for each TACACS+ authentication server and a number of columns, which are:

#: This is the TACACS+ authentication server number for which the configuration below applies.

Enabled: This enables the TACACS+ authentication server.

IP Address/Hostname: This is the IP address or hostname of the TACACS+ authentication server. IP address is expressed in dotted decimal notation.

Port: This is the TCP port to use on the TACACS+ authentication server. If the port is set to 0 (zero), the default port (49) is used on the TACACS+ authentication server.

Secret: This is the secret (up to 29 characters long) shared between the TACACS+ authentication server and the switch.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

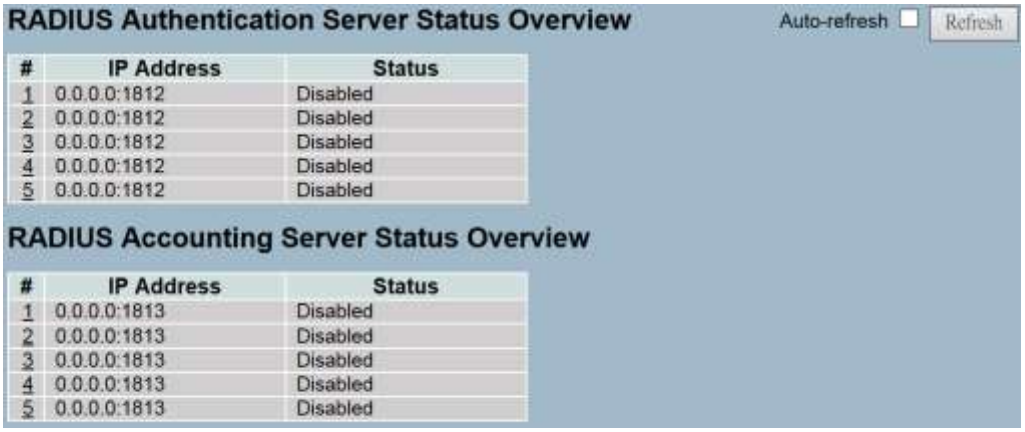
4-6.2 Radius Overview

This section provide an overview of the RADIUS authentication and accounting servers status.

Web Interface

To configure a RADIUS overview configuration in the web interface:

1. Check “Auto-refresh”.



RADIUS Authentication Server Status Overview

#	IP Address	Status
1	0.0.0.0:1812	Disabled
2	0.0.0.0:1812	Disabled
3	0.0.0.0:1812	Disabled
4	0.0.0.0:1812	Disabled
5	0.0.0.0:1812	Disabled

RADIUS Accounting Server Status Overview

#	IP Address	Status
1	0.0.0.0:1813	Disabled
2	0.0.0.0:1813	Disabled
3	0.0.0.0:1813	Disabled
4	0.0.0.0:1813	Disabled
5	0.0.0.0:1813	Disabled

Figure 4-6.2: The RADIUS Authentication Server Status Overview

Parameter Description

#: This is the RADIUS server number. Click to navigate to detailed statistics for this server.

IP Address: This is the IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

State: This is the current state 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.

RADIUS Accounting Servers

#: This is the RADIUS server number. Click to navigate to detailed statistics for this server.

IP Address: This is the IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

State: This is the current state 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 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.

Auto-Refresh: Click to automatically refresh the information.

Upper Right Icon (Refresh): Click to manually refresh the information.

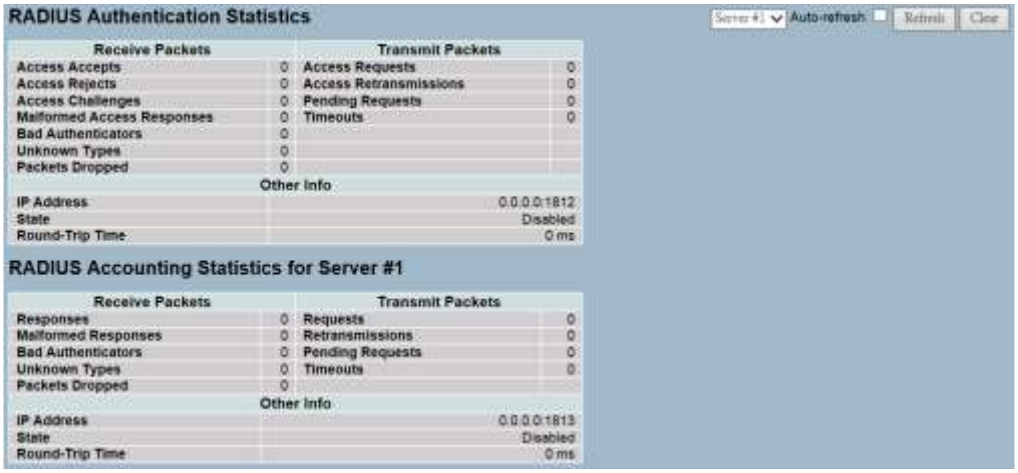
4-6.3 RADIUS Details

This section provides detailed statistics of the RADIUS authentication and accounting servers. The statistics map closely to those specified in RFC4668 - RADIUS authentication client MIB.

Web Interface

To configure a RADIUS details configuration in the web interface:

1. Specify which port you would like to check.
2. Check “Auto-refresh”.



RADIUS Authentication Statistics

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		

Other Info	
IP Address	0.0.0.0:1812
State	Disabled
Round-Trip Time	0 ms

RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		

Other Info	
IP Address	0.0.0.0:1813
State	Disabled
Round-Trip Time	0 ms

Figure 4-6.3: The RADIUS Authentication Statistics Server

Parameter Description

RADIUS Authentication Statistics

The statistics map closely to those specified in RFC4668 - RADIUS authentication client MIB. To view details, use the server select box to switch between the backend servers.

Packet Counters

RADIUS authentication server packet counter. There are seven receive and four transmit counters.

Direction	Name	RFC4668 Name	Description
Rx	**Access Accepts**	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Rx	**Access Rejects**	radiusAuthClientExtAccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Rx	**Access Challenges**	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Rx	**Malformed Access Responses**	radiusAuthClientExtMalformedAccessResponses	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.
Rx	**Bad Authenticators**	radiusAuthClientExtBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Rx	**Unknown Types**	radiusAuthClientExtUnknownTypes	The number of RADIUS packets that were received 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**	radiusAuthClientExtAccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.

Tx	**Pending Requests**	radiusAuthClientExtPendingRequests	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.
Tx	**Timeouts**	radiusAuthClientExtTimeouts	The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit and a timeout. A send to a different server is counted as a request and a timeout.

Other Info

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4668 Name	Description
IP Address	-	IP address and UDP port for the authentication server in question.
State	-	Shows the state of the server. It takes one of the following values: **Disabled:** The selected server is disabled. **Not Ready:** The server is enabled, but IP communication is not yet up and running. **Ready:** The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. **Dead (X seconds left):** Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	radiusAuthClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

RADIUS Accounting Statistics

The statistics map closely to those specified in RFC4670 - RADIUS accounting client MIB. To show details, use the server select box to switch between the backend servers.

Packet Counters

RADIUS accounting server packet counter. There are five receive and four transmit counters.

Direction	Name	RFC4670 Name	Description
Rx	**Responses**	radiusAccClientExt Responses	The number of RADIUS packets (valid or invalid) received from the server.
Rx	**Malformed Responses**	radiusAccClientExt MalformedResponses	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**	radiusAcctClientExt BadAuthenticators	The number of RADIUS packets containing invalid authenticators received from the server.
Rx	**Unknown Types**	radiusAccClientExt UnknownTypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Rx	**Packets Dropped**	radiusAccClientExt PacketsDropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
Tx	**Requests**	radiusAccClientExt Requests	The number of RADIUS packets sent to the server. This does not include retransmissions.
Tx	**Retransmissions**	radiusAccClientExt Retransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.
Tx	**Pending Requests**	radiusAccClientExt PendingRequests	The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a request is sent and decremented due to receipt of a Response, timeout, or retransmission.
Tx	**Timeouts**	radiusAccClientExt Timeouts	The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit and a timeout. A send to a different server is counted as a request and 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 mea surement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

Buttons:

- **Auto-Refresh** – Click to automatically refresh the information.
- **Refresh –** Click to manually refresh the information.
- **Clear –** Click to clear the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

4-7 Port Security

This section provides configurations for the port security settings. This feature is used to restrict input to an interface by limiting and identifying the MAC addresses.

4-7.1 Limit Control

This section provides configuration information for the port security settings.

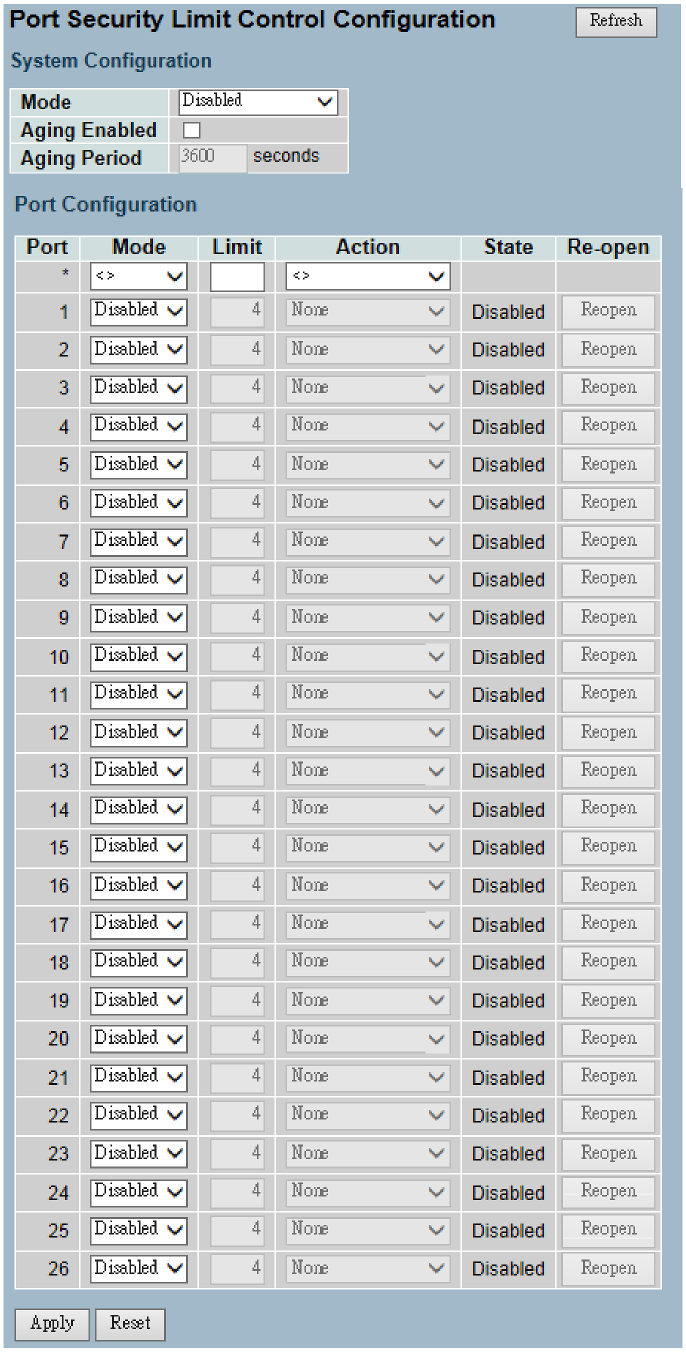
Web Interface

To configure a system configuration of limit control in the web interface:

1. Select “Enabled” in the mode of system configuration.
2. Checked aging enabled.
3. Set the aging period. The default is 3600 seconds.

To configure a port configuration of limit control in the web interface:

1. Select “Enabled” in the mode of port configuration.
2. Specify the maximum number of MAC addresses in the limit of port configuration.
3. Set the action (Trap, Shutdown, or Trap & Shutdown)
4. Click save.



Port Security Limit Control Configuration

System Configuration

Mode	Disabled
Aging Enabled	□
Aging Period	3600 seconds

Port Configuration

Port	Mode	Limit	Action	State	Re-open
*	<>		<>		
1	Disabled	4	None	Disabled	Reopen
2	Disabled	4	None	Disabled	Reopen
3	Disabled	4	None	Disabled	Reopen
4	Disabled	4	None	Disabled	Reopen
5	Disabled	4	None	Disabled	Reopen
6	Disabled	4	None	Disabled	Reopen
7	Disabled	4	None	Disabled	Reopen
8	Disabled	4	None	Disabled	Reopen
9	Disabled	4	None	Disabled	Reopen
10	Disabled	4	None	Disabled	Reopen
11	Disabled	4	None	Disabled	Reopen
12	Disabled	4	None	Disabled	Reopen
13	Disabled	4	None	Disabled	Reopen
14	Disabled	4	None	Disabled	Reopen
15	Disabled	4	None	Disabled	Reopen
16	Disabled	4	None	Disabled	Reopen
17	Disabled	4	None	Disabled	Reopen
18	Disabled	4	None	Disabled	Reopen
19	Disabled	4	None	Disabled	Reopen
20	Disabled	4	None	Disabled	Reopen
21	Disabled	4	None	Disabled	Reopen
22	Disabled	4	None	Disabled	Reopen
23	Disabled	4	None	Disabled	Reopen
24	Disabled	4	None	Disabled	Reopen
25	Disabled	4	None	Disabled	Reopen
26	Disabled	4	None	Disabled	Reopen

Figure 4-7.1: The Port Security Limit Control Configuration

Parameter Description

System Configuration

Mode: This indicates whether the limit control is globally enabled or disabled on the switch. If it’s globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.

Aging Enabled: If it’s 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 that has limit control enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host is 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.

Port Configuration

The table has one row for each port on the selected switch and a number of columns, which are:

Port: This is thee port number to apply the configuration to.

Mode: This controls whether limit control is enabled on this port. Both this and the global mode must be 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: This is the maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.

The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a port security-enabled port. Since all ports draw from the same pool, a configured maximum may not be granted if the remaining ports have already used all available MAC addresses.

Action: If the limit is reached, the switch can take one of the following actions:

- **None:** Does not allow more than limit MAC addresses on the port, but take no further action.
- **Trap:** If the limit + 1 MAC addresses is seen on the port, it sends a SNMP trap. If aging is disabled, only one SNMP trap will be sent. If aging is enabled, new SNMP traps will be sent everytime the limit gets exceeded.
- **Shutdown:** If the limit + 1 MAC addresses is seen on the port, it shuts down the port. This implies that all secured MAC addresses will be removed from the port and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:
    1) Boot the switch.
    2) Disable and re-enable limit control on the port or the switch.
    3) Click the reopen button.
- **Trap & Shutdown:** If the limit + 1 MAC addresses is seen on the port, both the trap and the shutdown actions described above will be taken.

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:** This 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:** This indicates that the limit is reached on this port. This state can only be shown if action is set to none or trap.
- **Shutdown:** This indicates that the port is shut down by the limit control module. This state can only be shown if action is set to shutdown or trap & shutdown.

Re-open Button: If a port is shutdown by this module, you may reopen it by clicking this button. This will only be enabled, if this is the case. For other methods, refer to shutdown in the action section.

NOTE: Clicking the reopen button causes the page to refresh, so non-committed changes will be lost.

Upper Right Icon (Refresh): Click to manually refresh the information.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

4-7.2 Switch Status

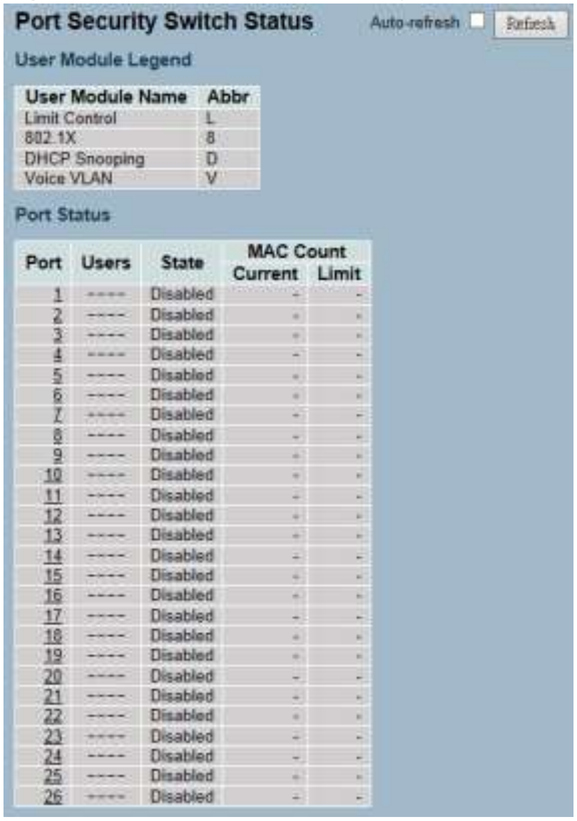
This section provides information regarding the port security status. Port security is a module with no direct configuration. Configuration comes indirectly from other user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed onto 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 Interface

To configure a port security status configuration in the web interface:

1. Check "Auto-refresh".

Figure 4-7.2: The Port Security Switch Status



Port Security Switch Status

User Module Legend

User Module Name	Abbr
Limit Control	L
802.1X	8
DHCP Snooping	D
Voice VLAN	V

Port Status

Port	Users	State	MAC Count	
			Current	Limit
1	----	Disabled	-	-
2	----	Disabled	-	-
3	----	Disabled	-	-
4	----	Disabled	-	-
5	----	Disabled	-	-
6	----	Disabled	-	-
7	----	Disabled	-	-
8	----	Disabled	-	-
9	----	Disabled	-	-
10	----	Disabled	-	-
11	----	Disabled	-	-
12	----	Disabled	-	-
13	----	Disabled	-	-
14	----	Disabled	-	-
15	----	Disabled	-	-
16	----	Disabled	-	-
17	----	Disabled	-	-
18	----	Disabled	-	-
19	----	Disabled	-	-
20	----	Disabled	-	-
21	----	Disabled	-	-
22	----	Disabled	-	-
23	----	Disabled	-	-
24	----	Disabled	-	-
25	----	Disabled	-	-
26	----	Disabled	-	-

Parameter Description

User Module Legend: This is the legend that shows all user modules that may request port security services.

User Module Name: This is the full name of a module that may request port security services.

Abbr: This is a one-letter abbreviation of the user module.

Port Status: The table has one row for each port on the selected switch and a number of columns.

Port: This is the port number for which the status applies. Click the port number to see the status for this particular port.

Users: Each of the user modules has a column that shows whether that module has enabled port security or not. A dash (-) means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.

State: This shows the current state of the port. It can take one of four values:

- **Disabled:** No user modules are currently using the port security service.
- **Ready:** The port security service is in use by at least one user module and is awaiting frames from unknown MAC addresses to arrive.
- **Limit Reached:** The port security service is enabled by at least the limit control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.
- **Shutdown:** The port security service is enabled by at least the limit control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the limit control configuration page.

MAC Count (Current, Limit): The two columns indicate the number of currently learned MAC addresses (forwarding and blocked) and the maximum number of MAC addresses that can be learned on the port.

If no user modules are enabled on the port, the current column will show a dash (-).

If the limit control user module is not enabled on the port, the limit column will show a dash (-).

This indicates the number of currently learned MAC addresses (forwarding and blocked) on the port. If no user modules are enabled on the port, a dash (-) will be shown.

Auto-Refresh: Click to automatically refresh the information.

Upper Right Icon (Refresh): Click to manually refresh the information.

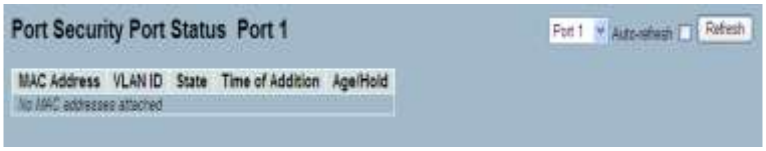
4-7.3 Port Status

This section shows the MAC addresses secured by the port security status module. Port security is a module with no direct configuration. Configuration comes indirectly from other 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.

Web Interface

To configure a port security status configuration in the web interface:

1. Specify the port you would like to monitor.
2. Checked “Auto-refresh”.



Port Security Port Status Port 1

MAC Address	VLAN ID	State	Time of Addition	Age/Hold
No MAC addresses attached				

Figure 4-7.3: The Port Security Port Status

Parameter Description

MAC Address & VLAN ID: These are the MAC address and VLAN ID on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.

State: This indicates whether the corresponding MAC address is blocked or forwarded. In the blocked state, it will not be allowed to transmit or receive traffic.

Time of Addition: This 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.

Auto-Refresh: Click to automatically refresh the information.

Upper Right Icon (Refresh): Click to manually refresh the information.

4-8 Access Management

This section provides configurations for the access management table which includes HTTP/HTTPS, SNMP, and TELNET/SSH. The switch can be managed over over an Ethernet LAN or over the internet.

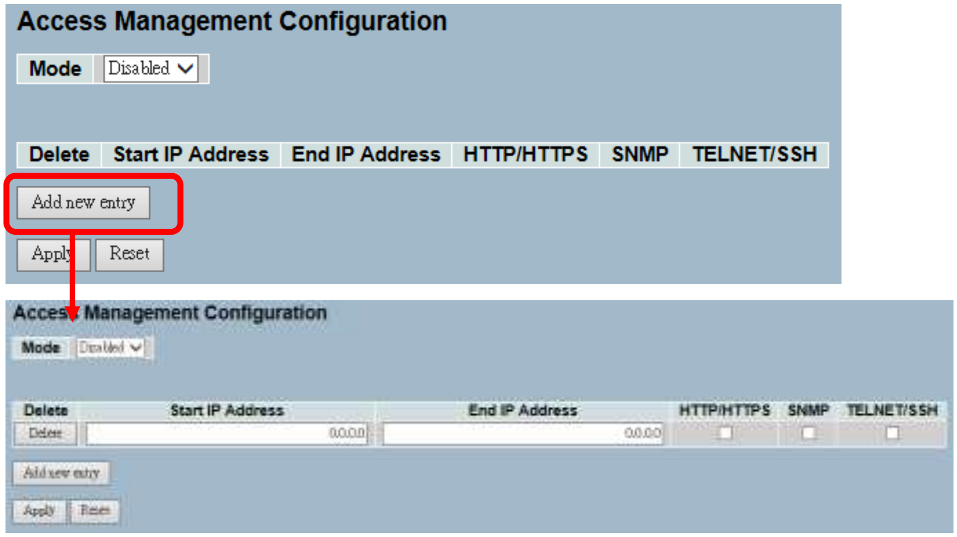
4-8.1 Configuration

This section provides configurations for the access management table. The maximum entry number is 16. If the application's type match any one of the access management entries, it will allow access to the switch.

Web Interface

To configure an access management configuration in the web interface:

1. Select “Enabled” in the mode of access management configuration.
2. Click “Add New Entry”.
3. Specify the start IP address and end IP address.
4. Check the access management method (HTTP/HTTPS, SNMP, and TELNET/SSH) in the entry.
5. Click save.



Access Management Configuration

Mode	Disabled

Delete	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH

Access Management Configuration

Mode	Disabled

Delete	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
Delete	0.0.0.0	0.0.0.0	□	□	□

Figure 4-8.1: The Access Management Configuration

Parameter Description

Mode: This indicates the access management mode operation. Possible modes are:

- **Enabled:** This enables the access management mode operation.
- **Disabled:** This disables the access management mode operation.

Delete: Click delete to remove the entry.

Start IP Address: This indicates the start IP address for the access management entry.

End IP Address: This indicates the end IP address for the access management entry.

HTTP/HTTPS: This 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: This 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: This 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:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

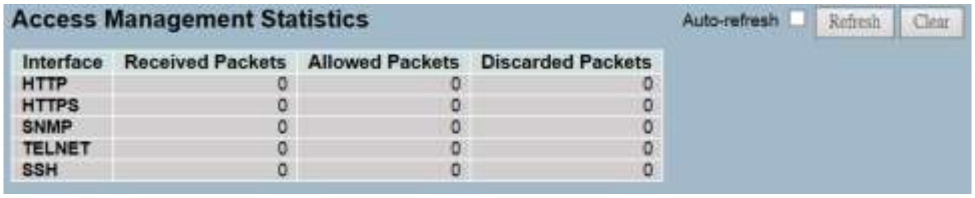
4-8.2 Statistics

This section provides detailed statistics of the access management including HTTP, HTTPS, SSH/TELNET, and SSH.

Web Interface

To configure an assess management statistics in the web interface:

1. Check “Auto-refresh”.



Access Management Statistics

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

Figure 4-8.2: The Access Management Statistics

Parameter Description

Interface: This is the interface type through which the remote host can access the switch.

Received Packets: This is the number of received packets from the interface when access management mode is enabled.

Allowed Packets: This is the number of allowed packets from the interface when access management mode is enabled

Discarded Packets: This is the number of discarded packets from the interface when access management mode is enabled.

Auto-Refresh: Click to automatically refresh the information.

Upper Right Icons (Refresh, Clear): Click to manually refresh or clear the information.

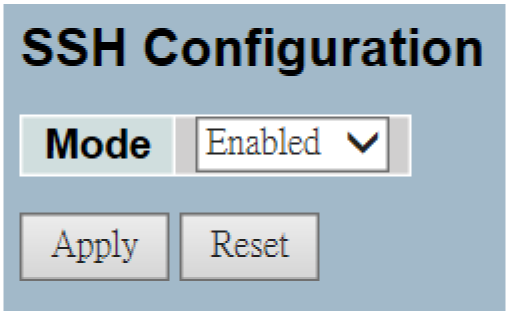
4-9 SSH

This section provides information regarding SSH (Secure Shell) to securely access the switch. SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication.

Web Interface

To configure a SSH configuration in the web interface:

1. Select “Enabled” in the mode of ssh configuration.
2. Click save.



SSH Configuration

Mode: Enabled

Figure 4-9.1: The SSH Configuration

Parameter Description

Mode: This indicates the SSH mode operation. Possible modes are:

- **Enabled:** This enables the SSH mode operation.
- **Disabled:** This disables the SSH mode operation.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

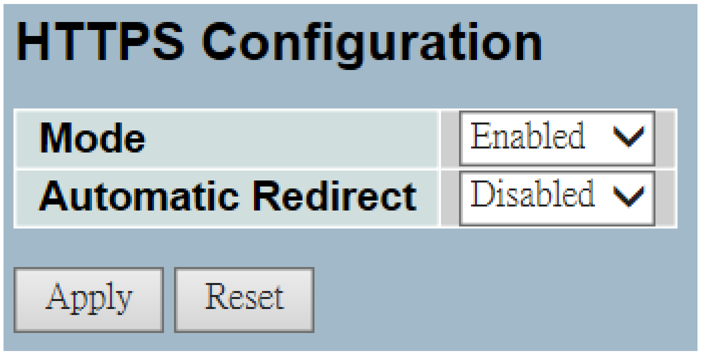
4-10 HTTPs

This section provides information regarding HTTPS to securely access the switch. HTTPS is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication via the browser.

Web Interface

To configure a HTTPS configuration in the web interface:

1. Select "Enabled" in the mode of https configuration.
2. Select "Enabled" in the automatic redirect of HTTPS configuration.
3. Click save.



HTTPS Configuration

Mode	Enabled
Automatic Redirect	Disabled

Figure 4-10.1: The HTTPS Configuration

Parameter Description

Mode: This indicates the HTTPS mode operation. Possible modes are:

- **Enabled:** This enables the HTTPS mode operation.
- **Disabled:** This disables the HTTPS mode operation.

Automatic Redirect: This indicates the HTTPS redirect mode operation. Automatically redirect web browser to HTTPS when HTTPS mode is enabled. Possible modes are:

- **Enabled:** This enables the HTTPS redirect mode operation.
- **Disabled:** This disables the HTTPS redirect mode operation.

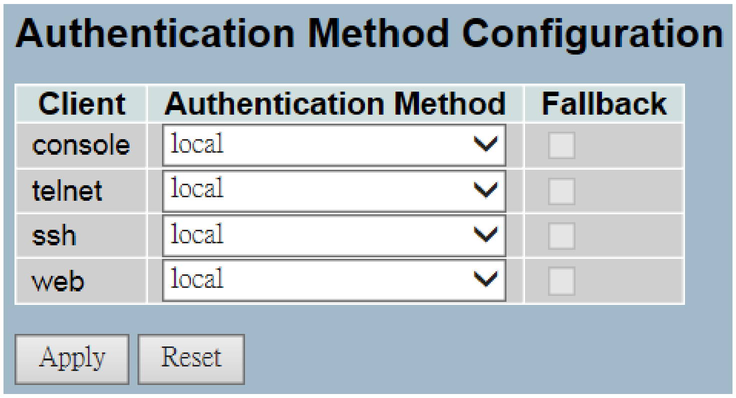
4-11 Auth Method

This section provides configurations for an authenticated user when logging into the switch via one of the management client interfaces.

Web Interface

To configure an authentication method configuration in the web interface:

1. Specify the client (console, telent, SSH, web) that you want to monitor.
2. Specify the authentication method (none, local, radius, TACACS+)
4. Check fallback.
5. Click save.



Authentication Method Configuration

Client	Authentication Method	Fallback
console	local	□
telnet	local	□
ssh	local	□
web	local	□

Figure 4-11.1: The HTTPS Configuration

Parameter Description

Client: This is the management client that the configuration applies to.
Authentication Method: Authentication method can be set to one of the following values:

- **None:** Authentication is disabled and login is not possible.
- **Local:** Uses the local user database on the switch for authentication.
- **Radius:** Uses a remote RADIUS server for authentication.
- **TACACS+:** Uses a remote TACACS+ server for authentication.

Fallback: This enables fallback to local authentication.

If none of the configured authentication servers are alive, the local user database is used for authentication.

This is only possible if the authentication method is set to a value other than none or local.

Buttons:

- **Save** – Click to save changes.
- **Reset-** Click to restore default settings.

Chapter 5: Maintenance

Chapter 5 provides an overview of the switch's maintenance configuration tasks to enhance the performance of local network. This includes restart device, firmware upgrade, save/restore, import/export, and diagnostics.

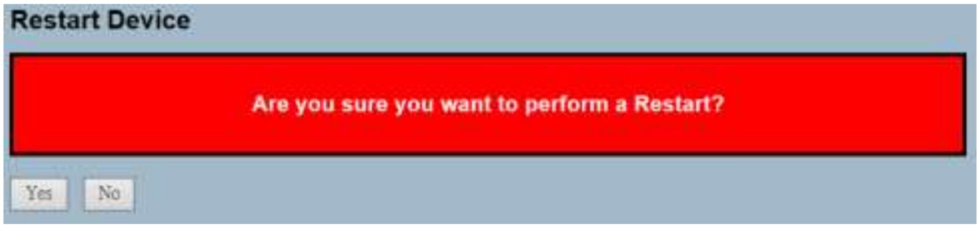
5-1 Restart Device

This section provides information on how to restart the switch for any maintenance needs. Any configuration files or scripts that you saved in the switch should still be available afterwards.

Web Interface

To configure a restart device configuration in the web interface:

1. Click restart device.
2. Click yes.



Restart Device

Are you sure you want to perform a Restart?

Figure 5-1.1: The Restart Device

Parameter Description

Restart Device: You can restart the switch on this page. After restart, the switch will boot normally.

Buttons:

- **Yes** – Click "Yes" to restart the device.
- **No** – Click "No" to undo any restarting actions.

5-2 Firmware

This section provides information on how to upgrade firmware. The switch can be enhanced with more value-added functions by installing firmware upgrades.

5-2.1 Firmware Upgade

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

Web Interface

To configure a firmware upgrade configuration in the web interface:

1. Click browse to select firmware.
2. Click upload.

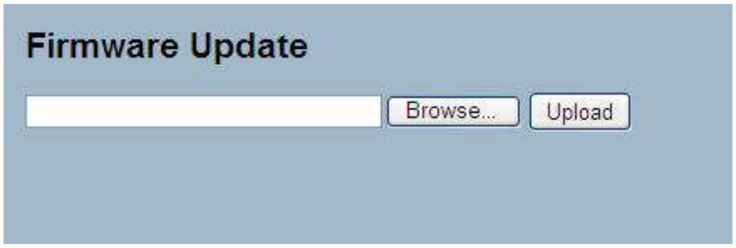


Figure 5-2.1: The Firmware Update

Parameter Description

Browse: Click the “Browse” button to search the firmware URL and filename.

Upload: Click the “Upload” button to upload the firmware.

NOTE: This page facilitates an update of the firmware controlling the switch. Uploading software will update all managed switches to the location of a software image. After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and all managed switches will restart.

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.

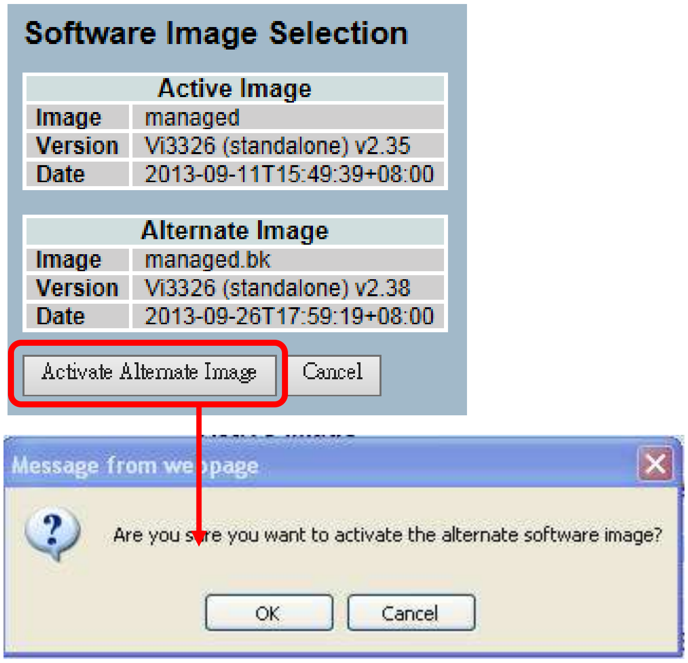
5-2.2 Firmware Selection

The switch supports dual image for firmware redundancy purpose. You can select which firmware image would be for the start firmware or operating firmware. This section provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image.

Web Interface

To configure a firmware selection in the web interface:

1. Click activate alternate image.
2. Click yes.



Software Image Selection

Active Image	
Image	managed
Version	Vi3326 (standalone) v2.35
Date	2013-09-11T15:49:39+08:00

Alternate Image	
Image	managed.bk
Version	Vi3326 (standalone) v2.38
Date	2013-09-26T17:59:19+08:00

Message from webpage

Are you sure you want to activate the alternate software image?

Figure 5-2.2: The Firmware Selection

Parameter Description

Image: This is the flash index name of the firmware image. The name of primary (preferred) image is “image”. The alternate image is named “image.bk.”.

Version: This is the version of the firmware image.

Date: This is 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.

NOTE:

1. In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the activate alternate image button is also disabled.
2. If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.
3. The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

5-3 Save/Restore

This section provides information on how to save and restore the switch configuration including reset to factory defaults, save start, save users, and restore users for any maintenance needs.

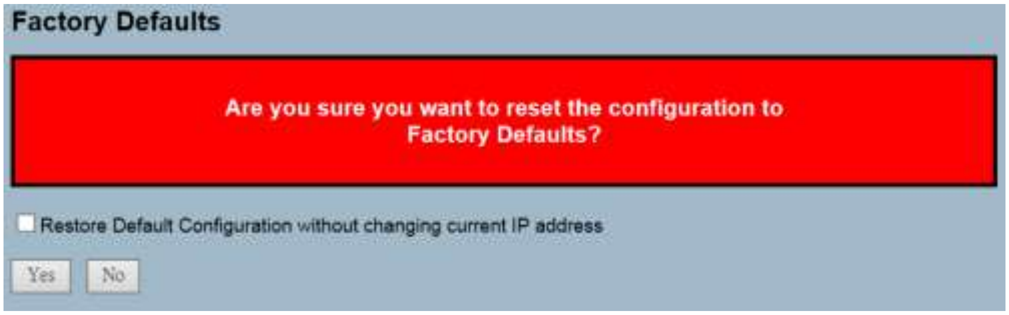
5-3.1 Factory Defaults

This section provides information on resetting the switch configuration to factory defaults. Any configuration files or scripts will recover to factory default values.

Web Interface

To configure a factory defaults configuration in the web interface:

1. Click factory defaults.
2. Click yes.



Factory Defaults

Are you sure you want to reset the configuration to Factory Defaults?

☐ Restore Default Configuration without changing current IP address

Figure 5-3.1: The Factory Defaults

Parameter Description

Buttons:

- **Yes** – Click to reset the configuration to factory defaults.
- **No-** Click to return to the port state page without resetting the configuration.

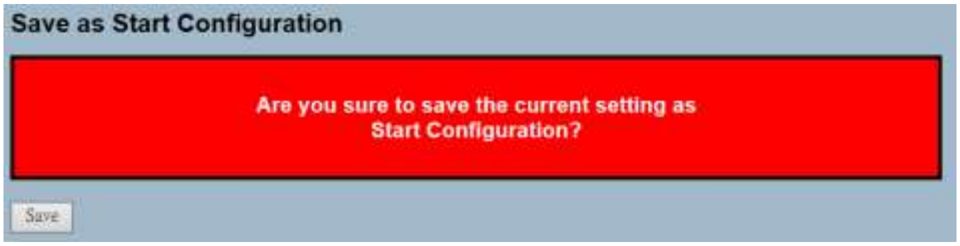
5-3.2 Save Start

This section provides information on how to save the switch start configuration. Any current configuration files will be saved as XML format.

Web Interface

To configure a save start configuration in the web interface:

1. Click save start.
2. Click yes.



Save as Start Configuration

Are you sure to save the current setting as Start Configuration?

Figure 5-3.2: The Save Start configuration

Parameter Description

Buttons:

- **Save** – Click to save current setting as start configuration.

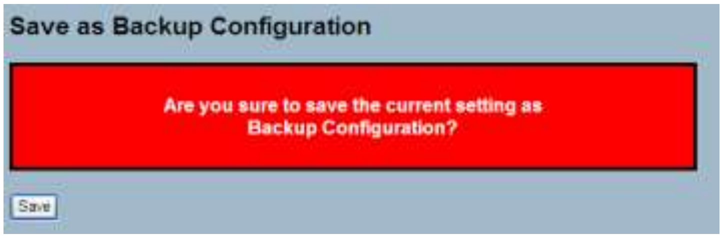
5-3.3 Save User

This section provides information on how to save users information. Any current configuration files will be saved as XML format.

Web Interface

To configure a save user configuration in the web interface:

1. Click save user.
2. Click yes.



Save as Backup Configuration

Are you sure to save the current setting as Backup Configuration?

Figure 5-3.3: The Save as Backup Configuration

Parameter Description

Buttons:

- **Save –** Click to save current setting as backup configuration.

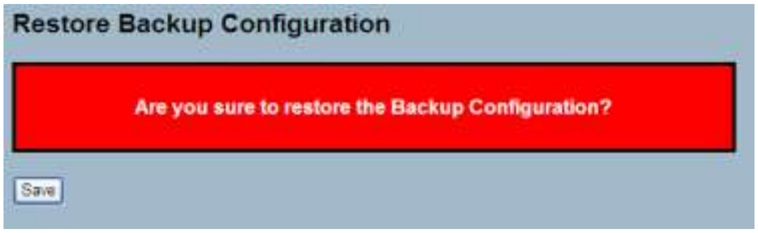
5-3.4 Restore User

This section provides information on how to restore users information back to the switch. Any current configuration files will be restored via XML format.

Web Interface

To configure a restore user configuration in the web interface:

1. Click restore user.
2. Click yes.



Restore Backup Configuration

Are you sure to restore the Backup Configuration?

Figure 5-3.4: The Restore the Backup Configuration

Parameter Description

Buttons:

- **Save –** Click to restore the backup configuration to the switch.

5-4 Export/Import

This section provides information on how to export and import the switch configuration. Any current configuration files will be exported as XML format.

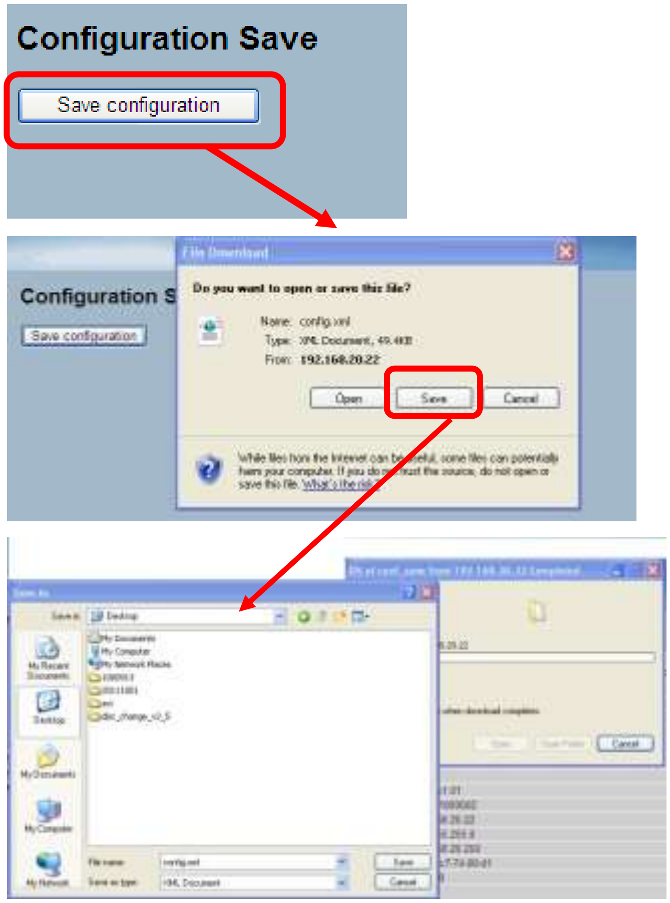
5-4.1 Export Config

This section provides information on how to export the switch configuration for maintenance needs. Any current configuration files will be exported as XML format.

Web Interface

To configure an export config configuration in the web interface:

1. Click save configuration.
2. Save the file in your device.



Do you want to open or save this file?

Name: config.xml
Type: XML Document, 49.4KB
From: 192.168.20.22

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

Figure 5-4.1: The Restore the Backup Configuration

Parameter Description

Save – Click to store the configuration to the PC or Server.

5-4.2 Import Config

This section provides information on how to export the switch configuration for maintenance needs. Any current configuration files will be exported as XML format.

Web Interface

To configure an import config configuration in the web interface:

1. Click browsr to select the config file in the device.
2. Click upload.

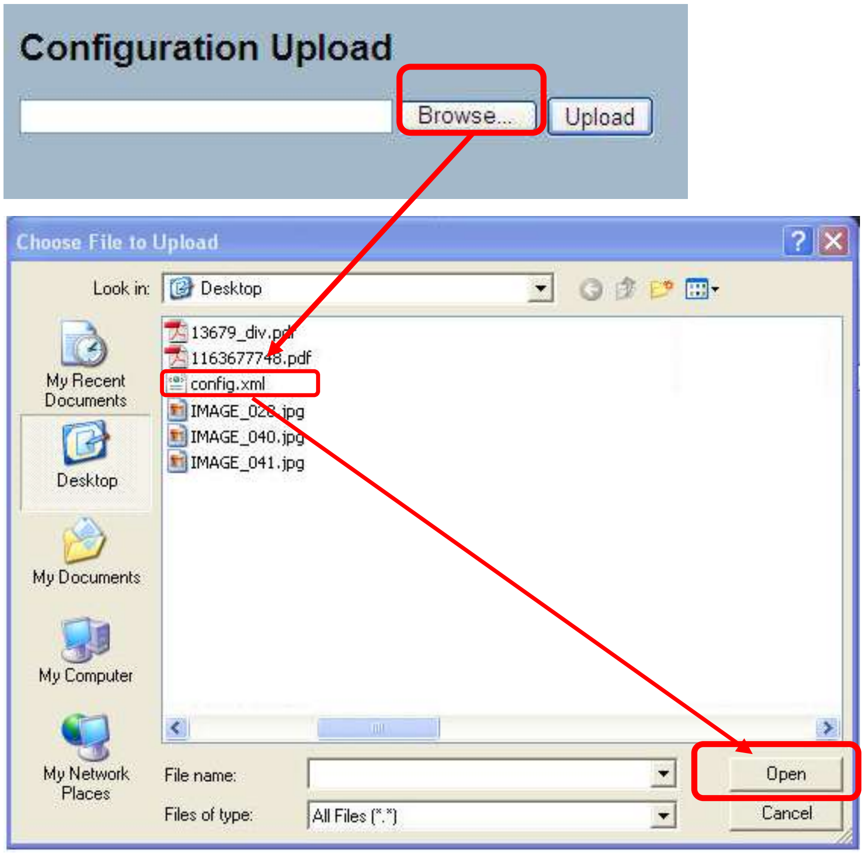


Figure 5-4.2: The Import Config

Parameter Description

Browse: Click the “Browse” button to search the configuration URL and filename.

Upload: Click the “Upload” button to upload the configuration from configuration stored location PC or server.

5-5 Diagnostics

This section provides information on a set of basic system diagnosis. It let users know whether the system is healthy or needs to be fixed. The basic system check includes ICMP ping, ICMPv6, and VeriPHY cable diagnostics.

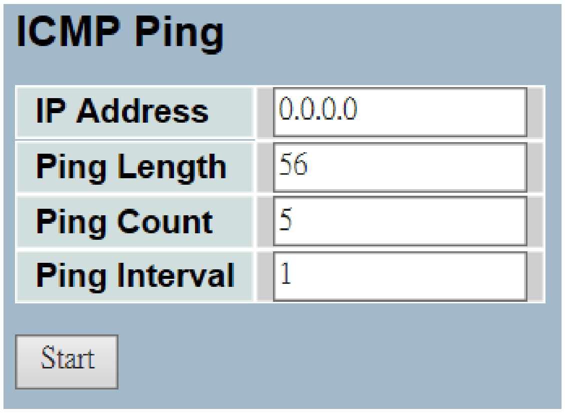
5-5.1 Ping

This section allows you to issue ICMP PING packets to troubleshoot IPv6 connectivity issues.

Web Interface

To configure an ICMP PING configuration in the web interface:

1. Specify ICMP PING IP address.
2. Specify ICMP PING size.
3. Click start.



ICMP Ping

IP Address	0.0.0.0
Ping Length	56
Ping Count	5
Ping Interval	1

Figure 5-5.1: The ICMP Ping

Parameter Description

IP Address: This is the destination IP address to ping.

Ping Length: This is the payload size of the ICMP packet. The values range from 2 bytes to 1452 bytes.

Ping Count: This is the count of the ICMP packet. The values range from 1 time to 60 times.

Ping Interval: This is the interval of the ICMP packet. The values range from 0 second to 30 seconds.

After you press, 5 ICMP packets are transmitted. 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.

```
PING6 server ::10.10.132.20
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
```

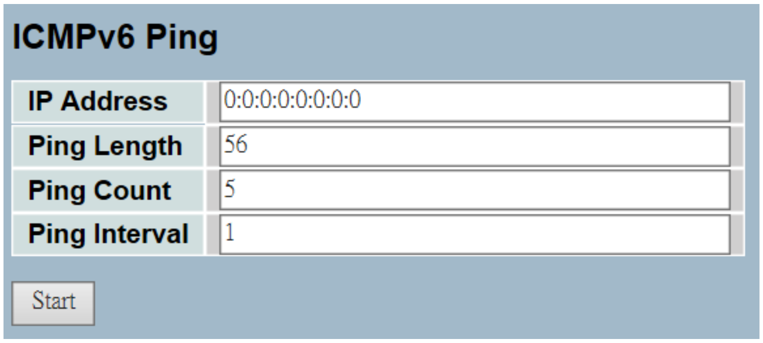
5-5.2 Ping6

This section provides troubleshooting information for IPv6 connectivity issues.

Web Interface

To configure an ICMPv6 PING configuration in the web interface:

1. Specify the ICMPv6 PING IP address.
2. Specify the ICMPv6 PING size.
3. Click start.



ICMPv6 Ping

IP Address	0:0:0:0:0:0:0:0
Ping Length	56
Ping Count	5
Ping Interval	1

Figure 5-5.2: The ICMPv6 Ping

Parameter Description

IP Address: This is the destination IP Address you want to ping it.

Ping Length: This is the payload size of the ICMP packet. The values range from 2 bytes to 1452 bytes.

Ping Count: This is the count of the ICMP packet. The values range from 1 time to 60 times.

Ping Interval: This is the interval of the ICMP packet. The values range from 0 second to 30 seconds.

Glossary of Web-based Management

A

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 or deny). The ACE also contains many detailed parameter options that are available for individual application.

ACL

ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex. For example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

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 from highest (top) to lowest (bottom). The default 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 for 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 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.
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.
C	
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.
D	
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). 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 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, the 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 (e.g. banking.), or other services that rely on the affected computer.
Dotted Decimal Notation	Dotted decimal notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets. An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.
DSCP	DSCP is an acronym for differentiated services code point. It is a field in the header of IP packets for packet classification purposes.
E	
EEE	EEE is an abbreviation for energy efficient ethernet defined in IEEE 802.3az.
EPS	EPS is an abbreviation for ethernet protection switching defined in ITU/T G.8031.
Ethernet Type	Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.

F	
FTP	FTP is an acronym for 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 IGMP and MLD.
H	
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 the web servers and browsers should take in response to various commands. 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 and serves 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.

I	
ICMP	ICMP is an acronym for internet control message protocol. It is a protocol that generates the error response, diagnostic, or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchange such as time-stamp or echo transactions.
IEEE 802.1X	IEEE 802.1X is an IEEE standard for port-based network access control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.
IGMP	IGMP is an acronym for internet group management protocol. It is a communications protocol used to manage the membership of internet protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.
IGMP Querier	A router sends IGMP query messages onto a particular link. This router is called the querier.
IMAP	IMAP is an acronym for 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.
IP Source Guard	IP source guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP snooping table or manually configured IP source bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.
L	
LACP	LACP is an IEEE 802.3ad standard protocol. The link aggregation control protocol, allows bundling several physical ports together to form a single logical port.
LLC	The IEEE 802.2 logical link control (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 link layer discovery protocol(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 extendsion 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 by EPS.
M	
MAC Table	Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports. The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.
MEP	MEP is an acronym for 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 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.
MVR	Multicast VLAN registration (MVR) is a protocol for layer 2 (IP) networks that enables multicast-traffic from a source VLAN to be shared with subscriber VLANs. The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them (Wikipedia).
N	
NAS	NAS is an acronym for network access server. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.
NetBIOS	NetBIOS is an acronym for 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. This means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NTP	NTP is an acronym for network time protocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer
O	
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.
P	
PCP	PCP is an acronym for priority code point. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as user priority.
PHY	PHY is an abbreviation for physical interface transceiver and is the device that implement the Ethernet physical layer (IEEE-802.3).
PING	Ping is a program that sends a series of packets, over a network or the internet, to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected. ping uses internet control message protocol (ICMP) packets. The PING request is the packet from the origin computer, and the PING reply is the packet response from the target.
Policer	A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

POP3	POP3 is an acronym for 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.
Private VLAN	In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.
PTP	PTP is an acronym for precision time protocol, a network protocol for synchronizing the clocks of computer systems.
Q	
QCE	QCE is an acronym for 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.

R	
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 dial in 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.
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.
S	
SHA	SHA is an acronym for secure hash algorithm. It was 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 (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 subnetwork access protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 service access point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values. It also supports vendor-private protocol identifier.
SNMP	SNMP is an acronym for 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 time protocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

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 contains 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.
SyncE	SyncE Is an abbreviation for synchronous Ethernet. This functionality is used to make a network “clock frequency” synchronized. Not to be confused with real time clock synchronized (IEEE 1588).
T	
TACACS+	TACACS+ is an acronym for terminal acess controller access control 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 (e.g. 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.
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.
U	
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 doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP. UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact. Common network applications that use UDP include the domain name system (DNS), streaming media applications such as IPTV, voice over IP (VoIP), and trivial file transfer protocol (TFTP).

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