LANTRONIX SM4T4DPA
Managed Switch, 4-port 10/100/1000Base-T, 4-port 100/1000 SFP
CONSOLE
POWER
RESET
1
2
3
4
5
6
7
8

SM4T4DPA

Managed Layer 2 Gigabit Ethernet Switch

(4) 10/100/1000Base-T Ports + (4) 100/1000Base-X SFP Slots

Web User Guide

Part Number 33868
Revision A August 2023

Intellectual Property

© 2022, 2023 Lantronix, Inc. All rights reserved. No part of the contents of this publication may be transmitted or reproduced in any form or by any means without the written permission of Lantronix.

Lantronix is a registered trademark of Lantronix, Inc. in the United States and other countries.

All other trademarks and trade names are the property of their respective holders.

Patented: https://www.lantronix.com/legal/patents/; additional patents pending.

Warranty

For details on the Lantronix warranty policy, go to http://www.lantronix.com/support/warranty.

Contacts

Lantronix Corporate Headquarters
48 Discovery, Suite 250
Irvine, CA 92618, USA
Toll Free: 800-526-8766
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support

Online: https://www.lantronix.com/technical-support/

Sales Offices

For a current list of our domestic and international sales offices, go to www.lantronix.com/about/contact.

Disclaimer

All information contained herein is provided "AS IS." Lantronix undertakes no obligation to update the information in this publication. Lantronix does not make, and specifically disclaims, all warranties of any kind (express, implied or otherwise) regarding title, non-infringement, fitness, quality, accuracy, completeness, usefulness, suitability or performance of the information provided herein. Lantronix shall have no liability whatsoever to any user for any damages, losses and causes of action (whether in contract or in tort or otherwise) in connection with the user's access or usage of any of the information or content contained herein. The information and specifications contained in this document are subject to change without notice.

Revision History

Rev	Date	Description
A	8/21/23	Initial Lantronix release at FW v 2.66.

Contents

Chapter 1. Introduction

1-1 Product Description

This switch is a high performance Layer 2 managed switch with (4) 10/100/1000Base-T copper ports and (4) dual speed 100/1000Base-X SFP slots.

1-2 Ordering Information

SM4T4DPA	Managed Layer 2 Gigabit Ethernet Switch wit (4) 10/100/1000Base-T Ports + (4) 100/1000Base-X SFP Slots.
SFP Modules	See Lantronix full line of SFP transceivers on our SFP webpage.
RMSM4-01	19“ Rack Mount Bracket.
BRSM8-01	Wall Mount Bracket.
Power Cord Included	To order the corresponding country specific power cord, add the appropriate extension to the end of the SKU: -NA = North America, -LA = Latin America, -EU = Europe, -UK = United Kingdom, -SA = South Africa, -JP = Japan, -OZ = Australia, or -BR = Brazil.

1-3 About this Manual

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

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). Transition Networks is now Lantronix. Some products/firmware items are still in process of being re-branded and may still reflect the Transition Networks name/logo.

1-4 Related Manuals

- SM4T4DPA Install Guide, 33687
- SM4T4DPA CLI Reference, 33689
- Software Release Note (version specific)

1-5 For More Information

For Lantronix Documentation, Firmware, App Notes, etc. go to https://www.lantronix.com/technical-support/. Note that this manual provides links to third party web sites for which Lantronix is not responsible.

1-6 Cautions and Warnings

Cautions indicate that there is the possibility of poor equipment performance or potential damage to the equipment. **Warnings** indicate that there is the possibility of injury to person.

Cautions and Warnings appear here and may appear throughout this manual where appropriate. Failure to read and understand the information identified by this symbol could result in poor equipment performance, damage to the equipment, or injury to persons.

⚠ **Caution**: While installing or servicing the power supply module, wear a grounding device and observe all electrostatic discharge precautions. Failure to observe this caution could result in damage to, or failure of the power module.

⚠ **Warning**: Do not connect the power module to an external power source before installing it into the chassis. Failure to observe this warning could result in an electrical shock, even death.

Warning: Equipment grounding is vital to ensure safe operation. The installer must ensure that the power module is properly grounded during and after installation. Failure to observe this warning could result in an electric shock, even death.

Warning: A readily accessible, suitable National Electrical Code (NEC) or local electrical code approved disconnect device and branch-circuit protector must be part of the building's installed wiring to accommodate permanently connected equipment. Failure to observe this warning could result in an electric shock, even death.

Warning: Turn any external power source OFF and ensure that the power module is disconnected from the external power source before performing any maintenance. Failure to observe this warning could result in an electrical shock, even death.

Warning: Ensure that the disconnect device for the external power source is OPEN *(turned OFF)* before disconnecting or connecting the power leads to the power module. Failure to observe this warning could result in an electric shock, even death.

Regulatory Approvals

- FCC Class A
- EN60950
- CE
- EN55022 Class A
- EN55024

Canadian EMI Notice

This Class A digital apparatus meets all the requirements of the Canadian Interference-Causing Equipment Regulations.
Cet appareil numerique de la classe A respecte toutes les exigences du Reglement sur le materiel brouilleur du Canada.

European Notice

Products with the CE Marking comply with both the EMC Directive (2004/108/EC) and the Low Voltage Directive (2006/95/EC) issued by the Commission of the European Community Compliance with these directives imply conformity to the following European Norms:
EN55022 (CISPR 22) - Radio Frequency Interference
EN60950 (IEC950) - Product Safety

1-7 Initial Configuration

This chapter describes how to configure and manage the SM4T4DPA via the web user interface (UI). With this facility you can easily set switch parameters and view switch and port status of the switch, including Spanning tree, port aggregation, multicast traffic, VLANs, etc.

The default values of the SM4T4DPA are:

IP Address	192.168.1.77
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Username	admin
Password	admin

After the signing in to the SM4T4DPA, you can configure it with a Web browser. You can type 192.168.1.77 in a Web browser to display the LOGIN screen prompting you to enter a username and password in order to login for access authentication.

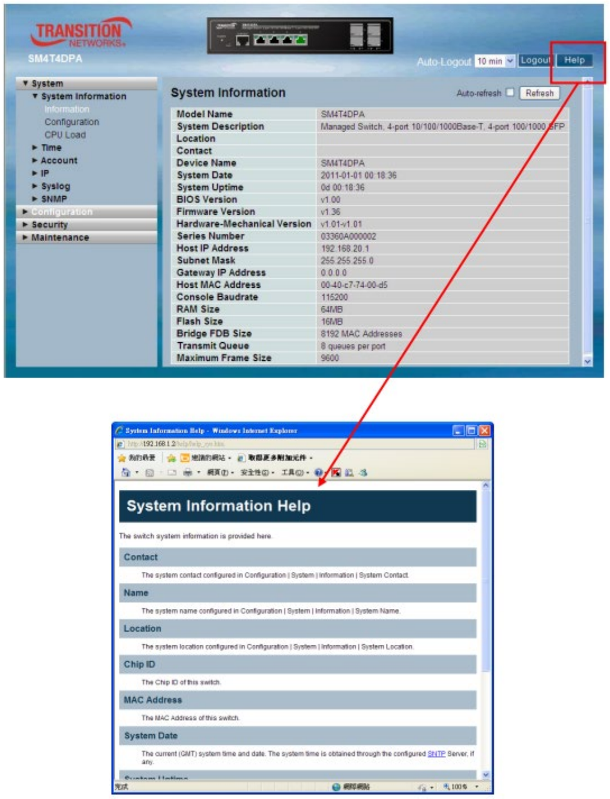
The default username is “admin” and password is admin. For the first time to use, enter the default username and password, and then click the <Login> button.

The SM4T4DPA supports a simple user management function allowing one administrator to configure the system at the same time. If there are two or more users using administrator’s identity, it will only allow the one who logs in first to configure the system. Other users, even with administrator’s identity, can only monitor the system. Those who have no administrator’s identity can only monitor the system. A maximum of three users can log in to the switch simultaneously.

After the switch has finished configuration in the CLI via the switch’s serial interface, you can browse it. For instance, type http://192.168.1.77 in the address row in a browser, it will show the following screen and ask you to enter a username and password in order to login and access authentication. The default username and password are both “admin”. For first time use, enter the default username and password, and then click the <Login> button. The login process now is completed.

1-8 Web User Interface

Note: If you need to set other parameters, refer to the detail in the related. You can also access the Switch and click the "help" button under the web GUI and the switch will pop-up simple help content on how to set the parameters:



System Information

Model Name	SM4T4DPA
System Description	Managed Switch, 4-port 10/100/1000Base-T, 4-port 100/1000 SFP
Location	
Contact	
Device Name	SM4T4DPA
System Date	2011-01-01 00:18:36
System Uptime	0d 00:18:36
BIOS Version	v1.00
Firmware Version	v1.36
Hardware-Mechanical Version	v1.01-v1.01
Series Number	03360A000002
Host IP Address	192.168.20.1
Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0
Host MAC Address	00-40-c7-74-00-d5
Console Baudrate	115200
RAM Size	64MB
Flash Size	16MB
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.

Chip ID

The Chip ID of this switch.

MAC Address

The MAC Address of this switch.

System Date

The current (GMT) system time and date. The system time is obtained through the configured SNTP Server, if any.

1-9 Webpage Controls

The webpage icons and buttons are described below.

Save: Click to apply the webpage settings to the running-config file.

Reset: Click to reset the webpage information.

Auto-refresh: Click to automatically refresh the webpage every 3 seconds.

Chapter 2 - System Configuration

This chapter describes the basic configuration tasks including System Information and managing switch functions (e.g., Time, Account, IP, Syslog and SNMP).

2-1 System Information

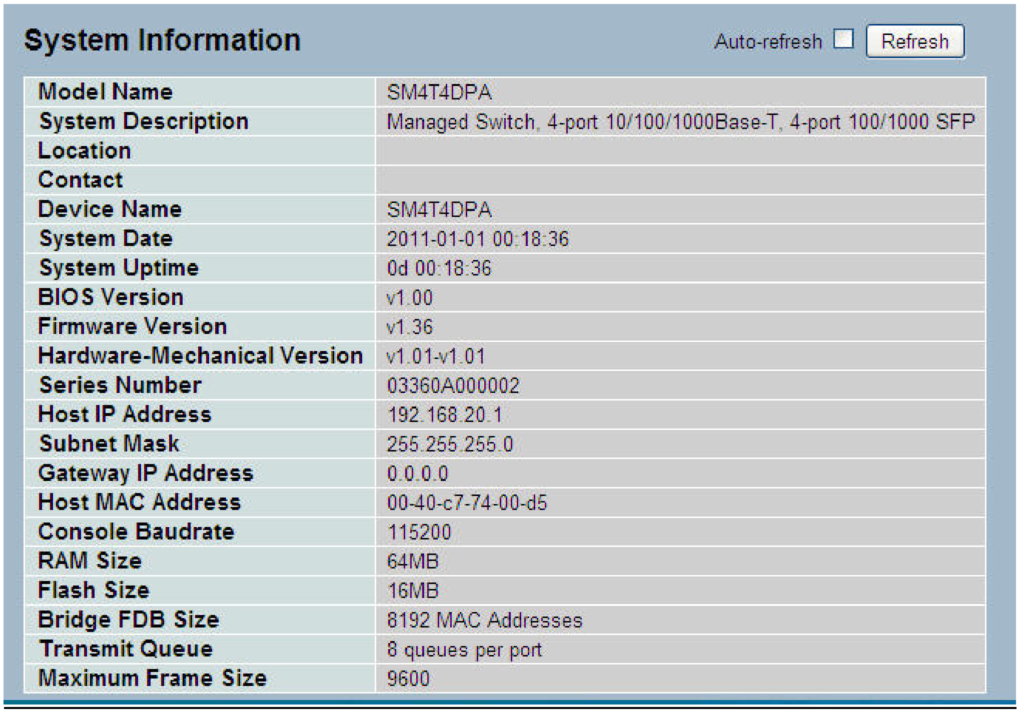
After you login, the switch shows you the system information. This page is default and tells you the basic information of the system, including "Model Name", "System Description", "Contact", "Device Name", "System Up Time", "BIOS Version", "Firmware Version", "Hardware-Mechanical Version", "Serial Number", "Host IP Address", "Host Mac Address", "Device Port", "RAM Size" , "Flash Size" and. With this information, you will know the software version used, MAC address, serial number, how many ports good and so on. This is helpful while malfunctioning.

2-1.1 Information

Switch system information is provided here. To configure System Information in the web UI:

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

Figure 2-1.1: System Information



System Information

Model Name	SM4T4DPA
System Description	Managed Switch, 4-port 10/100/1000Base-T, 4-port 100/1000 SFP
Location	
Contact	
Device Name	SM4T4DPA
System Date	2011-01-01 00:18:36
System Uptime	0d 00:18:36
BIOS Version	v1.00
Firmware Version	v1.36
Hardware-Mechanical Version	v1.01-v1.01
Series Number	03360A000002
Host IP Address	192.168.20.1
Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0
Host MAC Address	00-40-c7-74-00-d5
Console Baudrate	115200
RAM Size	64MB
Flash Size	16MB
Bridge FDB Size	8192 MAC Addresses
Transmit Queue	8 queues per port
Maximum Frame Size	9600

Parameter descriptions:

Model Name: Displays the model name of this device.

System description: Displays "Managed Switch, 4-port 10/100/1000Base-T, 4-port 100/1000 SFP".

Location: Displays the location where this switch is put. User-defined.

Contact: Enter the contact person and phone to contact for help.

Device Name: The name of the switch. User-defined.

System Date: Show the system time of the switch. Its format: day of week, month, day, hours : minutes : seconds, year.

System up time: The time accumulated since this switch is powered up. Its format is day, hour, minute, second.

BIOS version: The version of the BIOS in this switch.

Firmware version: The firmware version in this switch.

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

Serial number: The serial number is assigned by the Manufacture.

Host IP address: The IP address of the switch.

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

Console Baudrate: Shows the baud rate currently set for the switch console.

RAM size: The size of the RAM in this switch.

Flash size: The size of the flash memory in this switch.

Bridge FDB size : To display the bridge FDB size information.

Transmit Queue : To display the device’s transmit hardware priority queue information.

Maximum Frame size : To display the device’s maximum frame size information.

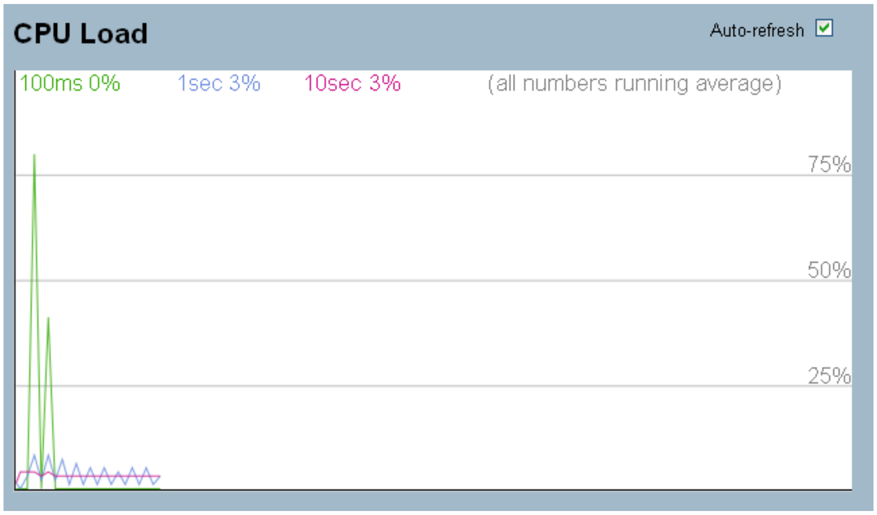
2-1.3 CPU Load

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

To configure System Information in the web interface:

1. Click System, System Information, CPU Load .
2. Display the CPU Load on the screen
3. Click Auto-refresh .

Figure 2-1.3: CPU Load



Parameter descriptions:

Auto-refresh: Check the box to refresh the webpage automatically every 3 seconds.

2-2 Time

This page lets you configure switch Time parameters, including Time Configuration and NTP Configuration

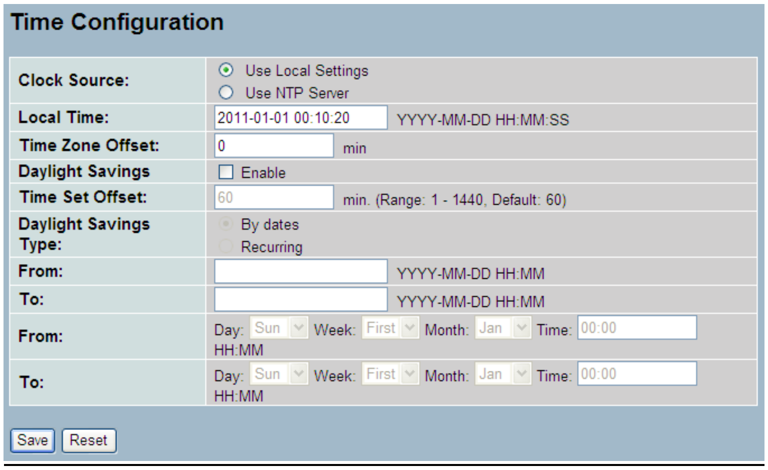
2-2.1 Manual

The switch provides manual and automatic ways to set the system time via NTP. Manual setting is simple and you just input “Year”, “Month”, “Day”, “Hour”, “Minute” and “Second” within the valid value range indicated in each item.

To configure Time in the web UI:

1. Click Time , Manual.
2. Specify the Time parameter in manual parameters.
3. Click Save.

Figure 2-2.1: Time Configuration



Time Configuration

Clock Source:	● Use Local Settings ○ Use NTP Server
Local Time:	2011-01-01 00:10:20 YYYY-MM-DD HH:MM:SS
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:	YYYY-MM-DD HH:MM
To:	YYYY-MM-DD HH:MM
From:	Day: Sun Week: First Month: Jan Time: 00:00 HH:MM
To:	Day: Sun Week: First Month: Jan Time: 00:00 HH:MM

Parameter descriptions:

Clock Source: Click the clock source for the SM4T4DPA. You can select “Use local Settings” or “Use NTP Server” for SM4T4DPA time clock source.

Local Time: Shows the current time of the system.

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

Daylight Savings: Daylight saving is adopted in some countries. If set, it will adjust the time lag or in advance in unit of hours, according to the starting date and the ending date. For example, if you set the day light saving to be 1 hour. When the time passes over the starting time, the system time will be increased one hour after one minute at the time since it passed over. And when the time passes over the ending time, the system time will be decreased one hour after one minute at the time since it passed over.

The switch supports valid configurable day light saving time is –5 ~ +5 step one hour. The zero for this parameter means it need not have to adjust current time, equivalent to in-act daylight saving. You don’t have to set the starting/ending date as well. If you set daylight saving to be non-zero, you have to set the starting/ending date as well; otherwise, the daylight saving function will not be activated.

Time Set Offset: Provide the Daylight saving time set offset. The offset is given in minutes east of GMT. The valid range is from 1 to 1440 minutes. The default is 60 minutes.

Daylight Savings Type: Provide the Daylight savings type selection. You can select “ By Dates” or “Recurring” two type for Daylight saving type.

From: To configure when Daylight saving start date and time, the format is “YYYY-MM-DD HH:MM”.

To: To configure when Daylight saving end date and time, the format is “YYYY-MM-DD HH:MM”.

Note: The “from” and “to” displays what you set in the “From” and “To” field information.

2-2.2 NTP

NTP (Network Timing Protocol) is used to sync the network time based Greenwich Mean Time (GMT). If use the NTP mode and select a built-in NTP time server or manually specify an user-defined NTP server as well as Time Zone, the switch will sync the time in a short after pressing <Apply> button. Though it synchronizes the time automatically, NTP does not update the time periodically without user action.

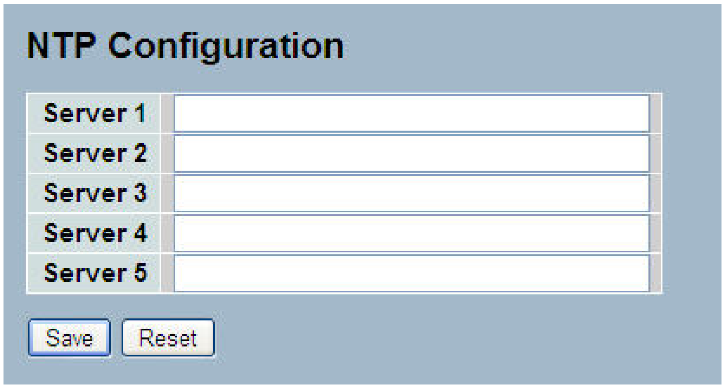
Time Zone is an offset time off GMT. You have to select the time zone first and then perform time sync via NTP because the switch will combine this time zone offset and updated NTP time to come out the local time, otherwise, you will not be able to get the correct time.

The switch supports configurable time zones from –12 to +13 with each step 1 hour. The default Time zone is +8 Hours.

To configure NTP in the web UI:

1. Click System, NTP.
2. Specify the Time parameter in manual parameters.
3. Click Save.

Figure 2-2.2: NTP Configuration



NTP Configuration

Server 1	
Server 2	
Server 3	
Server 4	
Server 5	

Parameter descriptions:

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

Buttons

Save : Click to save changes.

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

2-3 Account

In this function, only administrator can create, modify or delete the username and password. Administrator can modify other guest identities' password without confirming the password but it is necessary to modify the administrator-equivalent identity. Guest-equivalent identity can modify his password only. Please note that you must confirm administrator/guest identity in the field of Authorization in advance before configuring the username and password. Only one administrator is allowed to exist and is unable to be deleted. In addition, up to 4 guest accounts can be created.

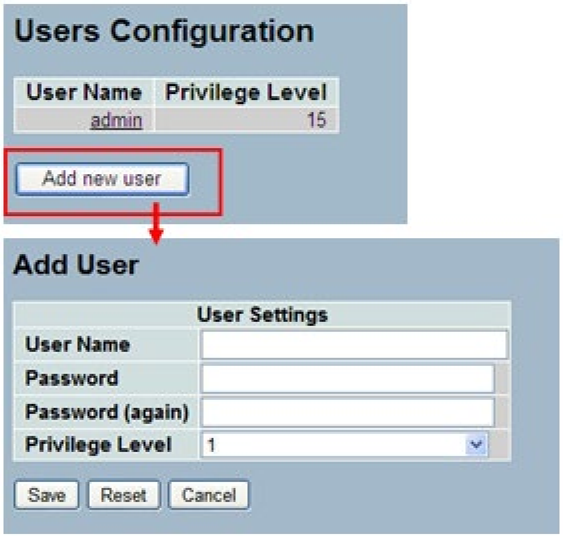
2-3.1 Users

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

To configure User account parameters in the web UI:

1. Click SYSTEM, Account, Users.
2. Click Add new user
3. Specify the User Name parameter.
4. Click Save.

Figure 2- 3.1: Users Configuration



Users Configuration

User Name	Privilege Level
admin	15

Add User

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

Parameter descriptions:

User Name : The name identifying the user. This is also a link to Add/Edit User.

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

Privilege Level : The privilege level of the user. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups (i.e., that is granted full control of the device). But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

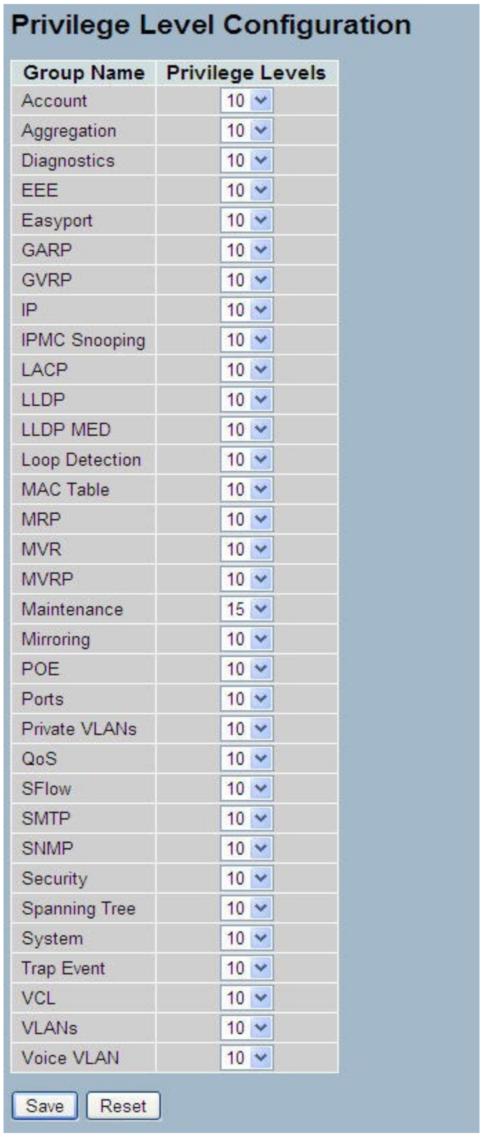
2-3.2 Privilege Level

This page provides an overview of the privilege levels. The switch provides user set Account, Aggregation, Diagnostics, EEE, GARP, GVRP, IP, IPMC Snooping, LACP, LLDP, LLDP-MED, MAC Table, MRP, MVR, MVRP, Maintenance, Mirroring, POE, Ports, Private VLANs, QoS, SMTP, SNMP, Security, Spanning Tree, System Trap Event, VCL, VLANs, Voice VLAN; Privilege Levels 1 - 15.

To configure Privilege Level in the web UI:

1. Click SYSTEM, Account, Privilege Level.
2. Specify the Privilege parameter.
3. Click Save.

Figure 2- 3.2: Privilege Level Configuration



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 Detection	10
MAC Table	10
MRP	10
MVR	10
MVRP	10
Maintenance	15
Mirroring	10
POE	10
Ports	10
Private VLANs	10
QoS	10
SFlow	10
SMTP	10
SNMP	10
Security	10
Spanning Tree	10
System	10
Trap Event	10
VCL	10
VLANs	10
Voice VLAN	10

Parameter descriptions:

Group Name : The name identifies the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in detail:

System: Contact, Name, Location, 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 and 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 to have the access to that group.

2-4 IP

The IP (Internet Protocol) is 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 substantial movement to adopt a new version of the Internet Protocol, IPv6, which has 128-bit 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.

2-4.1 IPV4

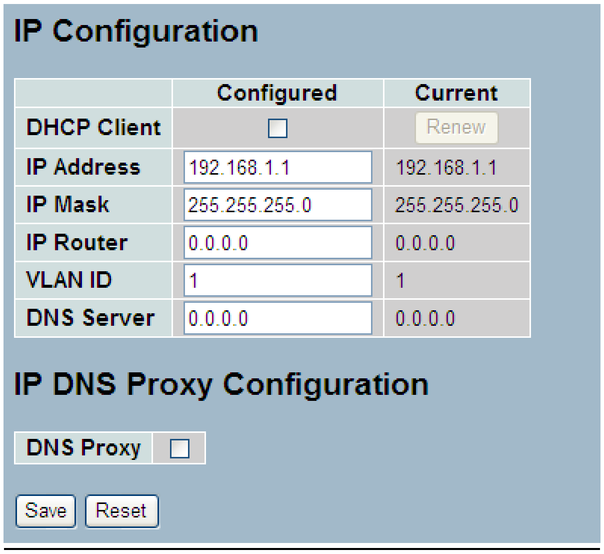
The IPv4 address for the switch can be obtained via DHCP Server for VLAN 1. To manually configure an address, you need to change the switch's default settings to values that are compatible with your network. You may also need to establish a default gateway between the switch and management stations that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

To configure an IP address in the web UI:

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

Figure 2- 4.1: IP Configuration



IP Configuration

	Configured	Current
DHCP Client	□	Renew
IP Address	192.168.1.1	192.168.1.1
IP Mask	255.255.255.0	255.255.255.0
IP Router	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 □

Parameter descriptions:

DHCP Client : Enable the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.

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

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

IP Router : Provide the IP address of the router in dotted decimal notation.

SNTP Server : Provide the IP address of the SNTP Server in dotted decimal notation.

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

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

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

2-4.2 IPV6

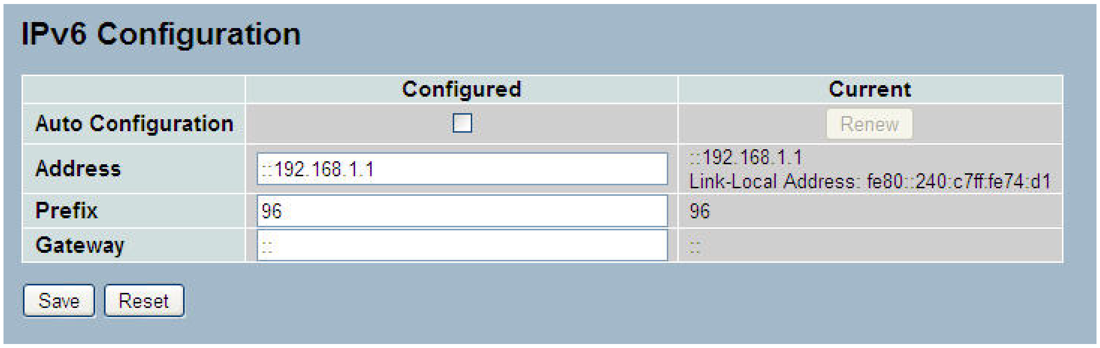
This section describes how to configure the switch-managed IPv6 information. The Configured column is used to view or change the IPv6 configuration. The Current column is used to show the active IPv6 configuration.

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.

To configure IPv6 parameters in the web UI:

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

Figure2- 4.2: IPv6 Configuration



IPv6 Configuration

	Configured	Current
Auto Configuration	□	Renew
Address	::192.168.1.1	::192.168.1.1 Link-Local Address: fe80::240:c7ff:fe74:d1
Prefix	96	96
Gateway	::	::

Parameter descriptions:

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

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

Prefix : Provide the IPv6 Prefix of this switch. The allowed range is 1 to 128.

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

2-5 Syslog

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 well a generalized informational, analysis and debugging messages. It is supported by a wide variety of devices and receivers across multiple platforms.

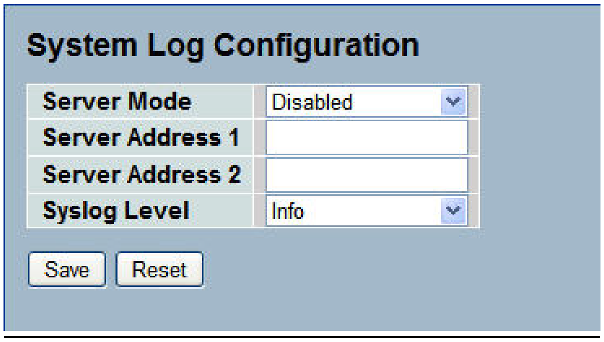
2-5.1 Configuration

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

To configure Syslog configuration in the web UI:

1. Click SYSTEM, Syslog.
2. Specify the syslog parameters includes IP Address of Syslog server and Port number.
3. Select Enable to enable Syslog.
4. Click Save.

Figure2- 5.1: System Log Configuration



System Log Configuration

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

Parameter descriptions:

Server Mode : Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist. Possible modes are:

Enabled: Enable server mode operation.

Disabled: Disable server mode operation.

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

Syslog Level : Indicates what kind of message will send to syslog server. Possible modes are:

Info: Send information, warnings and errors.

Warning: Send warnings and errors.

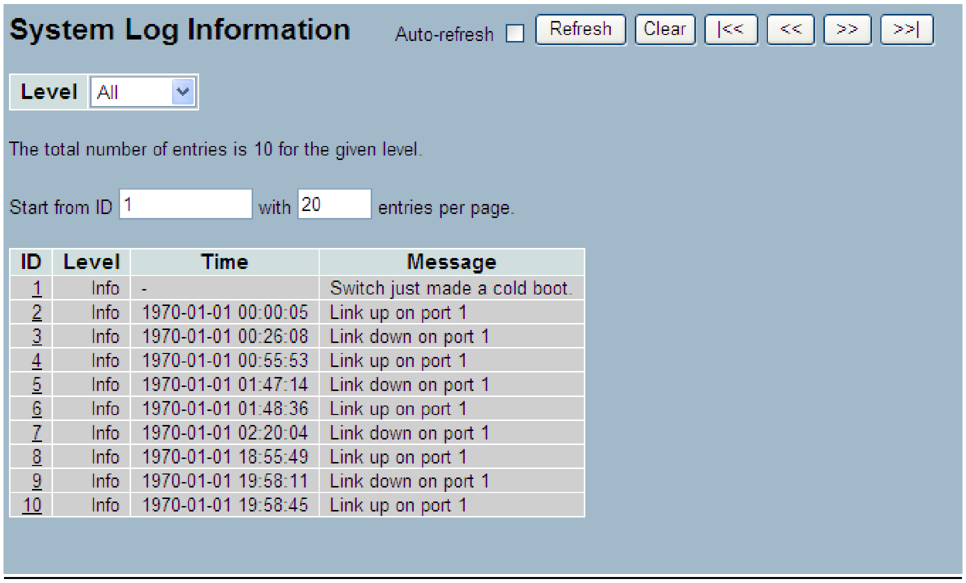
Error: Send errors.

2-5.2 Log

This page displays system log information of the switch. To display the log configuration in the web UI:

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

Figure 2- 5.2: System Log Configuration



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

Parameter descriptions:

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

Information level of the system log.

Warning: Warning level of the system log.

Error: Error level of the system log.

All: All levels.

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

Time : It will display the log record by device time. The time of the system log entry.

Message : It will display the log detail message. The message of the system log entry.

Buttons:

Auto-refresh : Check Auto-refresh box then the device will refresh the log automatically.

Refresh: Click to refresh the system log page.

Clear : Click to clear the page information manually.

|<< : Starting page.

<< : Previous page.

>> : Next page.

>>| : Last page.

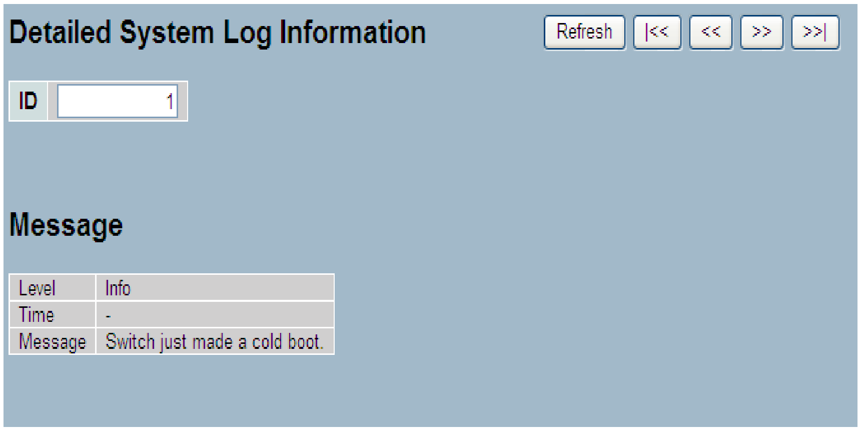
.

2-5.3 Detailed Log

This page displays the detailed log information of the switch. To display the detailed log configuration in the web UI:

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

Figure 2- 5.3: Detailed System Log Information



Detailed System Log Information

ID: 1

Message

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

Parameter descriptions:

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

Message : The detailed message of the system log entry.

Buttons:

Refresh: Click to refresh the system log page.

|<< : Starting page.

<< : Previous page.

>> : Next page.

>>| : Last page.

2-6 SNMP

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with 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 and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. SNMP agent is running on the switch to response the request issued by SNMP manager.

Basically, it is passive except issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP "Enable", SNMP agent will be started up. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If the field SNMP is set "Disable", SNMP agent will be de-activated, the related Community Name, Trap Host IP Address, Trap and all MIB counters will be ignored.

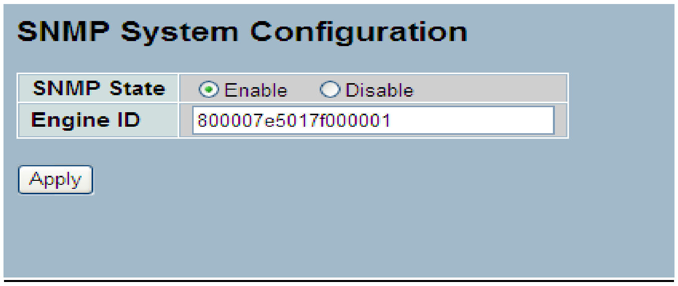
2-6.1 System

This section describes how to configure SNMP System on the switch. This function is used to configure SNMP settings, community name, trap host and public traps as well as the throttle of SNMP. A SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. So, both parties must have the same community name. Once completing the setting, click <Apply> button, the setting takes effect.

To configure SNMP System parameters in the web UI:

1. Click SNMP, System.
2. Evoke SNMP State to enable or disable the SNMP function .
3. Specify the Engine ID
4. Click Apply.

Figure 2- 6.1: SNMP System Configuration



SNMP System Configuration

SNMP State	● Enable ○ Disable
Engine ID	800007e5017f000001

Parameter descriptions:

SNMP State : Used for the activation or de-activation of SNMP.

Enable: Enable SNMP state operation (default).

Disable: Disable SNMP state operation.

Engine ID : The SNMPv3 engine ID. Syntax: 0-9,a-f,A-F, min 5 octet, max 32 octet, fifth octet can't input 00. Changing the Engine ID will clear all original user information.

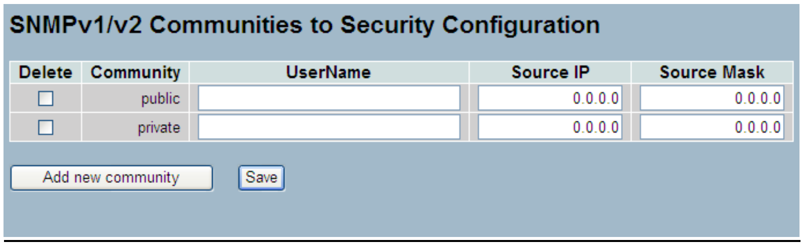
2-6.2 Communities

This function is used to configure SNMPv3 communities. The Community and UserName is unique. To create a new community account, please check <Add new community> button, and enter the account information then click the Save button. Max Group Number : 4.

To configure SNMP Communities in the web UI:

1. Click SNMP, Communities.
2. Click the Add new community button.
3. Specify the SNMP communities' parameters.
4. Click Save.

Figure 2- 6.2: SNMPv1/v2 Communities to Security Configuration



SNMPv1/v2 Communities to Security Configuration

Delete	Community	UserName	Source IP	Source Mask
□	public		0.0.0.0	0.0.0.0
□	private		0.0.0.0	0.0.0.0

Parameter descriptions:

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

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

UserName: The UserName access string to permit access to SNMPv3 agent. The length of "UserName" string is restricted to 1-32.

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

Source Mask : Indicates the SNMP access source address mask.

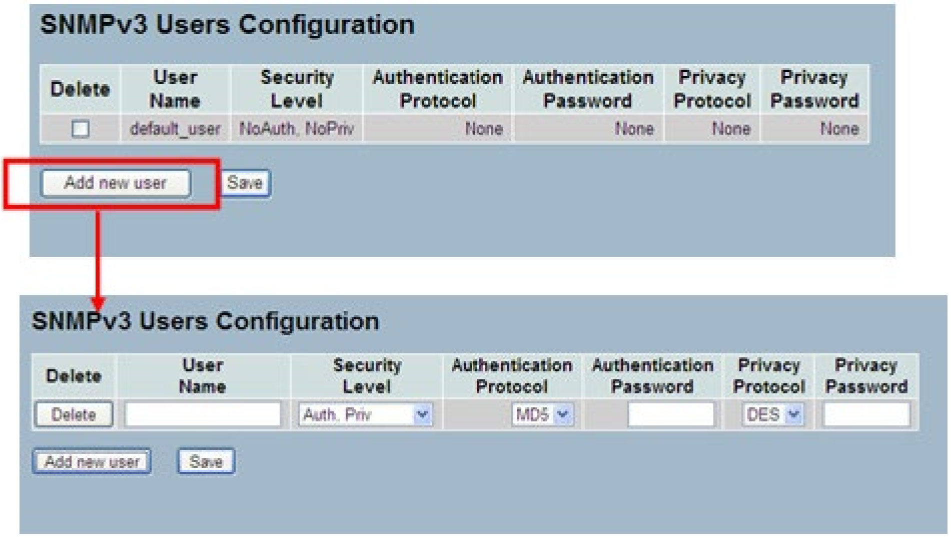
2-6.3 Users

The function is used to configure SNMPv3 users. The Entry index key is UserName. To create a new UserName account, click the Add new user button, enter the user information ,then click Save. Max Group Number : 10.

To display the configure SNMP Users in the web UI:

1. Click SNMP, Users.
2. Specify the Privilege parameter.
3. Click Save.

Figure 2-6.3: SNMP Users Configuration



SNMPv3 Users Configuration

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

SNMPv3 Users Configuration

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

Parameter descriptions:

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

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

Security Level : Indicates the security model that this entry should belong to. Possible security models are:

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

The value of security level cannot be modified if an entry already exists. That means it must first be ensured that the value is set correctly.

Authentication Protocol : 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 authentication protocol cannot be modified if entry already exists. That means must first ensure that the value is set correctly.

Authentication Password : A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8-32 characters. For SHA authentication protocol, the allowed string length is 8 to 40 characters. The allowed content is ASCII characters 33 - 126.

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

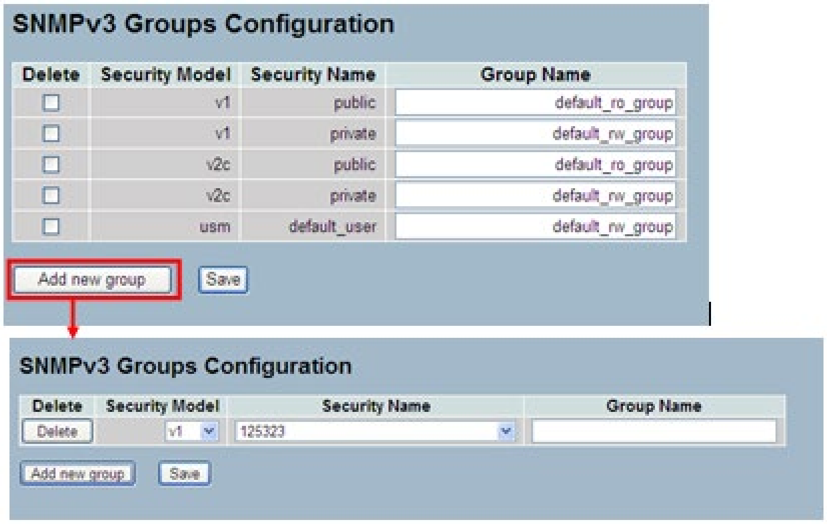
2-6.4 Groups

This function is used to configure SNMPv3 group. The Entry index key is Security Model and Security Name. To create a new group account, please check <Add new group> button, and enter the group information then check <Save>. Max Group Number: v1: 2, v2: 2, v3:10.

To display the configure SNMP Groups in the web UI:

1. Click SNMP, Groups.
2. Specify the Privilege parameter.
3. Click Save.

Figure 2-6.4: SNMP Groups Configuration



SNMPv3 Groups Configuration

Delete	Security Model	Security Name	Group Name
□	v1	public	default_ro_group
□	v1	private	default_rw_group
□	v2c	public	default_ro_group
□	v2c	private	default_rw_group
□	usm	default_user	default_rw_group

SNMPv3 Groups Configuration

Delete	Security Model	Security Name	Group Name
Delete	v1	125323	

Parameter descriptions:

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

Security Model : Indicates the security model that this entry should belong to. Possible security models are:

***v1*:** Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

usm: User-based Security Model (USM).

Security Name : A string identifying the security name that this entry should belong to. The allowed string length is 1 - 32 characters, and the allowed content is ASCII characters 33 - 126.

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

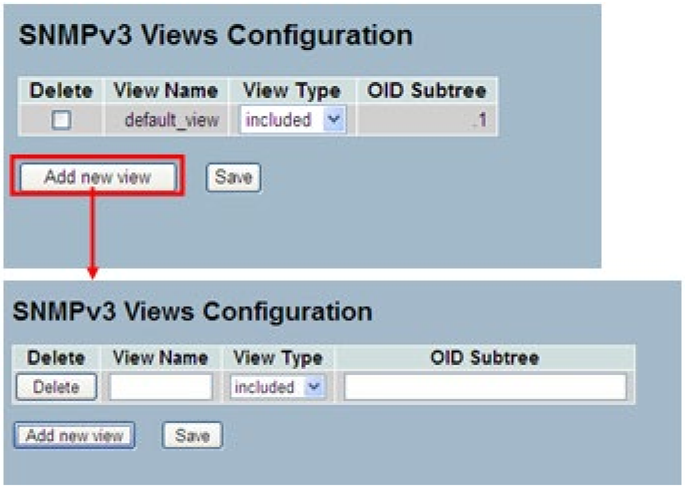
2-6.5 Views

The function is used to configure SNMPv3 view. The Entry index key are OID Subtree and View Name. To create a new view account, please check <Add new view> button, and enter the view information then click Save.
Max Group Number : 28.

Configure SNMPv3 view table on this page. The entry index keys are View Name and OID Subtree.

1. Click SNMP, 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.

Figure 2-6.5: SNMP Views Configuration



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	

Parameter descriptions:

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

View Name : A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32 characters, and the allowed content is ASCII characters from 33 - 126.

View Type : 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 it's OID subtree should overstep the 'excluded' view entry.

OID Subtree : The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).

Save : Click the Save button to save the configuration to ROM.

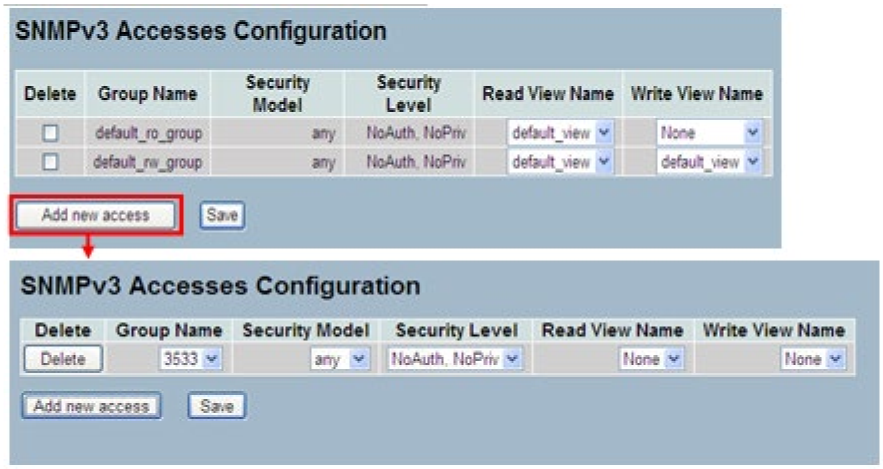
2-6.6 Access

This function is used to configure SNMPv3 accesses. The Entry index key are Group Name, Security Model and Security level. To create a new access account, please check <Add new access> button, and enter the access information then click Save. Max Group Number : 14

To configure SNMP Access in the web UI:

1. Click SNMP, 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.

.Figure 2-6.6: SNMP Accesses Configuration



SNMPv3 Accesses Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
☐	default_ro_group	any	NoAuth, NoPriv	default_view	None
☐	default_rw_group	any	NoAuth, NoPriv	default_view	default_view

SNMPv3 Accesses Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
Delete	3533	any	NoAuth, NoPriv	None	None

Parameter descriptions:

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

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

Security Model : Indicates the security model that this entry should belong to. Possible security models are:

any: Any security model accepted(v1|v2c|usm).

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

usm: User-based Security Model (USM).

Security Level : Indicates the security model that this entry should belong to. Possible security models are:

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

Read View Name : The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1-32 characters, and the allowed content is ASCII characters 33-126.

Write View Name : The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1-32 characters, and the allowed content is ASCII characters 33-126.

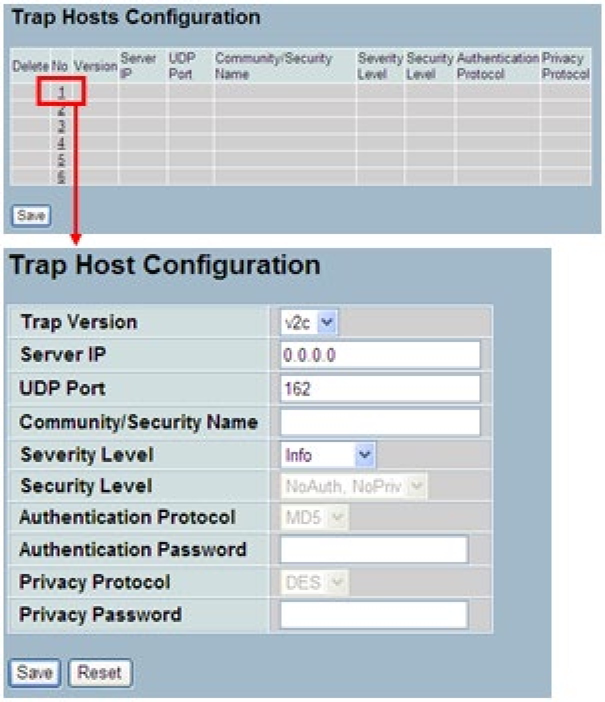
2-6.7 Trap

The function is used to configure SNMP trap. To create a new trap account, click a linked instance in the No (Number) column, and enter the trap information then click Save. Max Group Number : 6.

To configure SNMP Trap setting:

1. Click SNMP, Trap .
2. Display the SNMP Trap Hosts information table.
3. Choice a entry to display and modify the detail parameters or click the delete button to delete the trap hosts entry.

Figure 2-6.7: SNMP Trap Host Configuration



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	

Parameters descriptions:

Delete: Check <Delete> entry then check <Save> button, the entry will be delete.

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

Server IP: To assign the SNMP Host IP address.

UDP Port: To assign Port number. Default: 162

Community / Security Name:_The length of "Community / Security Name" string is restricted to 1-32 characters.

Security Level: Indicates what kind of message will send to Security Level. Possible modes are:

Info: Send information, warnings and errors.

Warning: Send warnings and errors.

Error: Send errors.

Security Level: There are three choices.

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

Authentication Protocol: You can choose MD5 or SHA for authentication.

Authentication Password:

__MD5__: The length of 'MD5 Authentication Password' is restricted to 8 – 32.

__SHA__: The length of 'SHA Authentication Password' is restricted to 8 – 40.

Privacy Protocol: You can set DES encryption for UserName.

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

Chapter 3. Configuration

This chapter describes all of the basic network configuration tasks which includes the Ports, Layer 2 network protocol (e.g., VLANs, QoS, IGMP, ACLs and PoE etc.) and other switch settings.

3-1 Port

The section describes how to configure the Port detail parameters of the switch. Others you could using the Port configure to enable or disable the Port of the switch. Monitor the ports content or status in the function.

3-1.1 Configuration

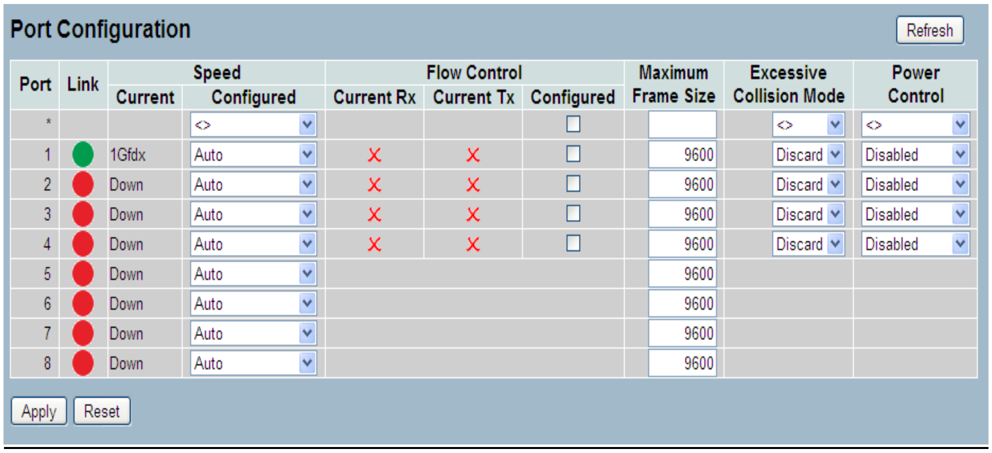
This chapter describes how to view the current port configuration and how to configure ports to non-default settings, including:

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

To configure Port parameters in the web UI:

1. Click Configuration, Port, then Configuration
2. Specify the Speed Configured, Flow Control, Maximum Frame size, Excessive Collision mode, and Power Control.
3. Click Save.

Figure 3-1.1: Port Configuration



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		
6	🔴	Down	Auto				9600		
7	🔴	Down	Auto				9600		
8	🔴	Down	Auto				9600		

Parameter descriptions:

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 that it is down.

Current Link Speed : Provides the current link speed of the port.

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

Auto 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.

Configured : Check the box in 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 : Configure port transmit collision behavior.

Discard: Discard frame after 16 collisions (default).

Restart: Restart 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

Refresh : Click to refresh the page manually.

Apply : Click to save changes.

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

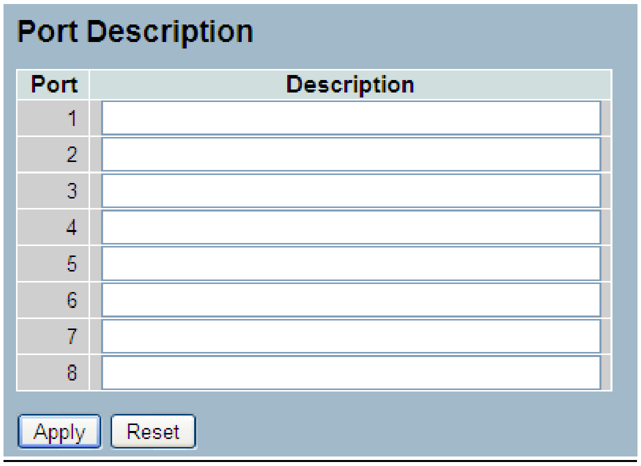
3-1.2 Port Description

This section describes how to configure the Port's alias or any descriptions for the Port Identity. It provides user to write down an alphanumeric string describing the full name and version identification for the system's hardware type, software version, and networking application

To configure Port descriptions in the web UI:

1. Click Configuration, Port, then Port Description
2. Specify the detail 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.

Figure 3-1.2: Port Configuration



Port Description

Port	Description
1	
2	
3	
4	
5	
6	
7	
8	

Parameter descriptions:

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

Description : The description of device ports cannot include " # % & ' + \.

Buttons

Apply : Click to save changes.

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

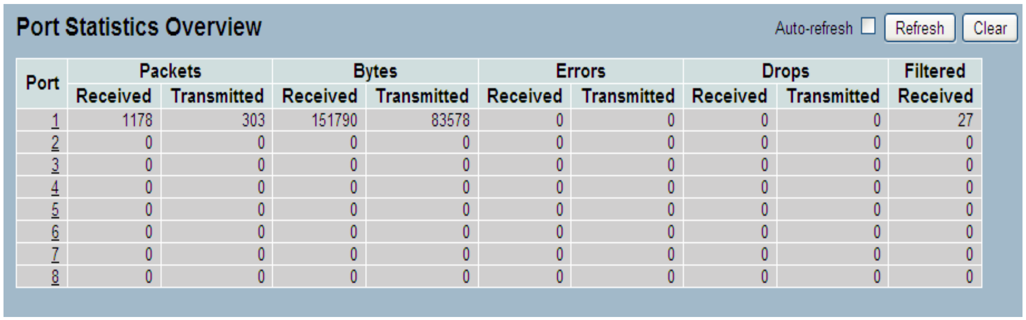
3-1.3 Traffic Overview

This page displays Port statistics information and provides overview of general traffic statistics for all switch ports.

To display Port Statistics in the web UI:

1. Click Configuration, Port, then Traffic Overview
2. If you want to auto-refresh then you need to evoke the “Auto-refresh” .
3. Click “ Refresh“ to refresh the port statistics or clear all information when you click “ Clear”.

Figure 3-1.3: Port Statistics Overview



Port Statistics Overview

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	1178	303	151790	83578	0	0	0	0	27
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

Parameter descriptions:

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

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

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

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

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

Filtered : The number of received frames filtered by the forwarding.

Buttons:

Auto-refresh : To evoke the auto-refresh icon then the device will refresh the information automatically.

Refresh : Click to refresh the Port Statistics information manually.

Clear : Click to clear all Port Statistics.

3-1.4 Detailed Statistics

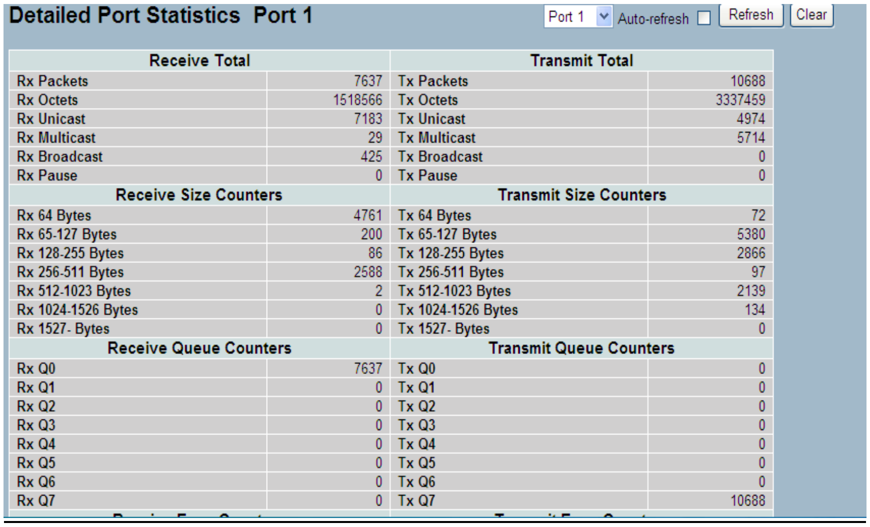
This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

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

To display per Port detailed Statistics in the web interface:

1. Click Configuration, Port, then Detailed Port Statistics
2. Scroll the Port Index to select which port you want to show the detailed Port statistical overview" .
3. If you want to auto-refresh the information then check the "Auto-refresh" box.
4. Click " Refresh" to refresh the port detailed statistics or clear all information when you click " Clear".

Figure 3-1.4: Detailed Port Statistics



Detailed Port Statistics Port 1

Receive Total		Transmit Total	
Rx Packets	7637	Tx Packets	10688
Rx Octets	1518566	Tx Octets	3337459
Rx Unicast	7183	Tx Unicast	4974
Rx Multicast	29	Tx Multicast	5714
Rx Broadcast	425	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	4761	Tx 64 Bytes	72
Rx 65-127 Bytes	200	Tx 65-127 Bytes	5380
Rx 128-255 Bytes	86	Tx 128-255 Bytes	2866
Rx 256-511 Bytes	2588	Tx 256-511 Bytes	97
Rx 512-1023 Bytes	2	Tx 512-1023 Bytes	2139
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	134
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	7637	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	10688

Parameter descriptions:

Auto-refresh: Click to refresh the Port Statistics information automatically.

Port select box: At the dropdown select which port to display the Port statistics (e.g., 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 indicating a PAUSE operation.

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

Receive and Transmit Queue Counters: The number of received and transmitted packets per input and output queue.

Receive Error Counters

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.

Buttons:

Auto-refresh : To evoke the auto-refresh icon then the device will refresh the information automatically.

Refresh : Click to refresh the Port Statistics information manually.

Clear : Click to clear all Port Statistics.

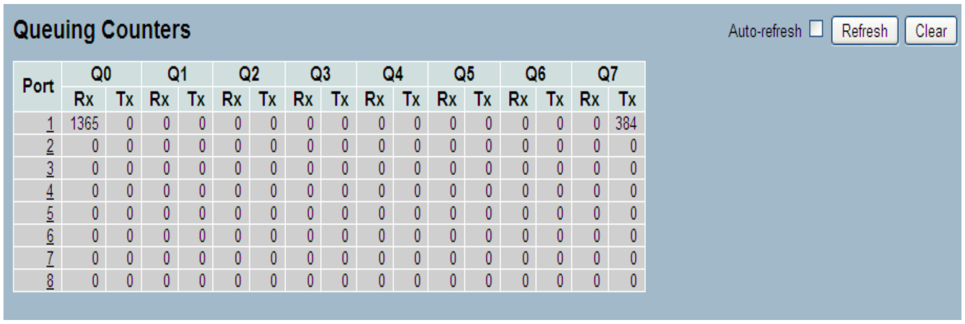
3-1.5 QoS Statistics

The section describes that switch could display the QoS detailed Queuing counters for a specific switch port. for the different queues for all switch ports.

To display the Queuing Counters in the web UI:

1. Click Configuration, Port, then QoS Statistics
2. Click to auto-refresh the page automatically.
3. Click “Refresh“ to refresh the Queuing Counters or clear all information when you click “ Clear”.

Figure 3-1.5: Queuing 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	1365	0	0	0	0	0	0	0	0	0	0	0	0	0	0	384
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

Parameter descriptions:

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

Qn : The Queue number (0-7); the QoS queues per port. Q0 is the lowest priority queue.

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

Buttons:

Auto-refresh : To evoke the auto-refresh icon then the device will refresh the information automatically.

Refresh : Click to refresh the Port Statistics information manually.

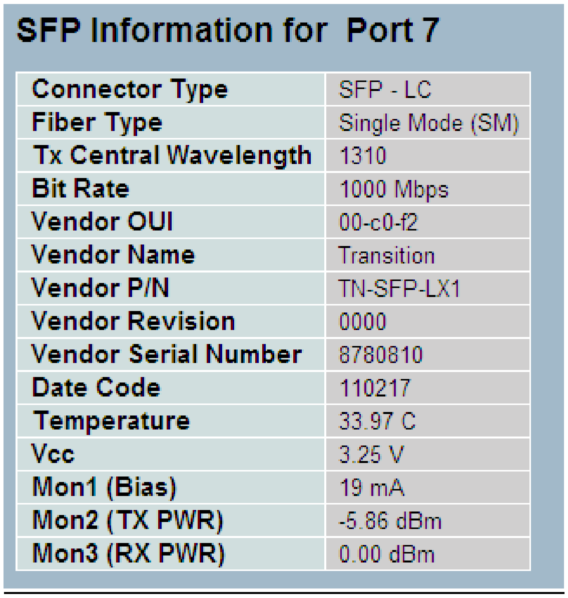
Clear : Click to clear all Port Statistics.

3-1.6 SFP Information

This page displays SFP module detail information which you connect it to the switch. The information includes: Connector type, Fiber type, wavelength, bound rate and Vendor OUI etc. To display SFP information in the web UI:

1. Click Configuration, Port, then SFP Information.
2. View the SFP Information.

Figure 3-1.6: SFP Information



SFP Information for Port 7

Connector Type	SFP - LC
Fiber Type	Single Mode (SM)
Tx Central Wavelength	1310
Bit Rate	1000 Mbps
Vendor OUI	00-c0-f2
Vendor Name	Transition
Vendor P/N	TN-SFP-LX1
Vendor Revision	0000
Vendor Serial Number	8780810
Date Code	110217
Temperature	33.97 C
Vcc	3.25 V
Mon1 (Bias)	19 mA
Mon2 (TX PWR)	-5.86 dBm
Mon3 (RX PWR)	0.00 dBm

Parameter descriptions:

Connector Type: Displays the connector type, for instance, UTP, SC, ST, LC and so on.

Fiber Type: Displays the fiber mode, for instance, Multi-Mode, Single-Mode.

Tx Central Wavelength: Displays the fiber optic transmitting central wavelength (e.g., 850nm, 1310nm, 1550nm).

Baud Rate: Displays the maximum baud rate of the fiber module supported (e.g., 10M, 100M, 1G).

Vendor OUI: Displays the Manufacturer's Organizationally Unique Identifier which is assigned by IEEE.

Vendor Name: Displays the company name of the module manufacturer.

Vendor P/N: Displays the product name of the naming by module manufacturer.

Vendor Revision: Displays the module revision.

Vendor Serial Number: Shows the serial number assigned by the manufacturer.

Date Code: Shows the date this SFP module was made.

Temperature: Shows the current temperature of SFP module.

Vcc: Shows the working DC voltage of SFP module.

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

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

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

3-1.7 EEE

The function lets you view and set current EEE port settings. Energy Efficient Ethernet 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 named wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange information about the devices wakeup time using the LLDP protocol.

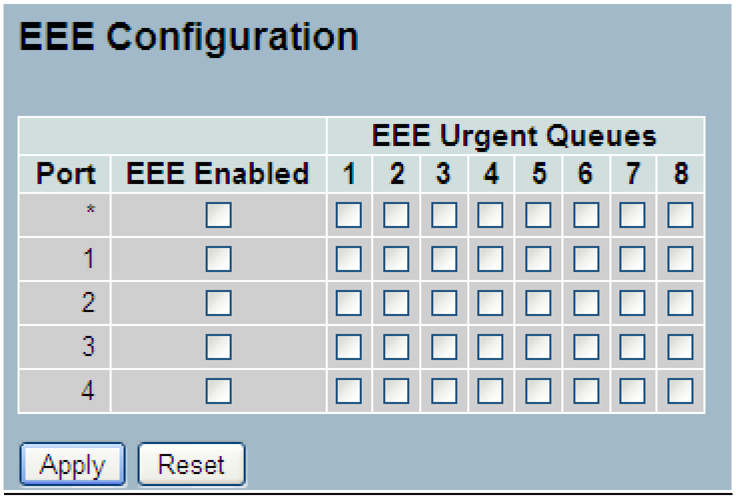
For maximizing the power saving, the circuit isn't started at once transmit data are ready for a port but is instead queued until 3000 bytes of data are ready to be transmitted. For not introducing a large delay in case that data less than 3000 bytes will be transmitted, data are always transmitted after 48 us, giving a maximum latency of 48 us + the wakeup time.

If desired 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.

To configure the EEE parameters in the web UI:

1. Click Configuration, Port, then EEE
2. To evoke which port wants to enable the EEE function. To evoke which
3. EEE Urgent Queues level and the range from 1 to 8. the queue will postpone the transmission until 3000 bytes are ready to be transmitted.
4. Click the save to save the setting
5. If you want to cancel the setting then you need to click the reset button. It will revert to previously saved values.

Figure 3-1.7: EEE Configuration



EEE Configuration

		EEE Urgent Queues							
Port	EEE Enabled	1	2	3	4	5	6	7	8
*	□	□	□	□	□	□	□	□	□
1	□	□	□	□	□	□	□	□	□
2	□	□	□	□	□	□	□	□	□
3	□	□	□	□	□	□	□	□	□
4	□	□	□	□	□	□	□	□	□

Parameter descriptions:

Port : The switch port number of the logical EEE port

EEE Enabled : Controls whether EEE is enabled for this switch port

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

3-2 ACL

The SM4T4DPA switch access control list (ACL) is probably the most commonly used object in the IOS. It is used for packet filtering but also for selecting types of traffic to be analyzed, forwarded, or influenced in some way. The ACLs are divided into EtherTypes. IPv4, ARP protocol, MAC and VLAN parameters etc. Here we will just go over the standard and extended access lists for TCP/IP. As you create ACEs for ingress classification, you can assign a policy for each port, the policy number is 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.

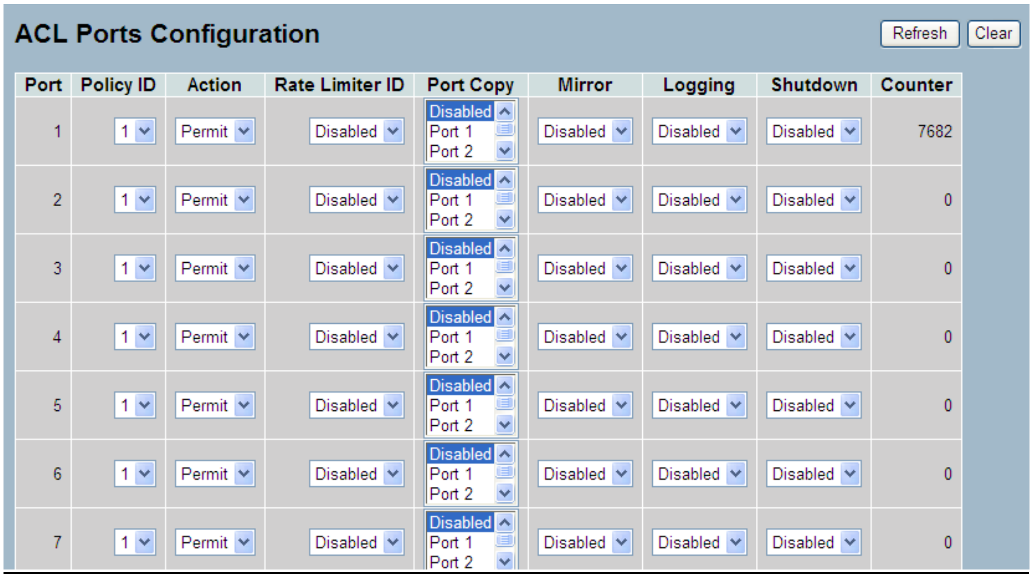
3-2.1 Ports

This page lets you set ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

To configure ACL Ports in the web UI:

1. Click Configuration, ACL, then Ports
2. To scroll the specific parameter value to select the correct value for port ACL setting.
3. Click the save to save the setting
4. If you want to cancel the setting then you need to click the reset button. It will revert to previously saved values.
5. After you configure complete then you could see the Counter of the port then you could click refresh to update the counter or Clear the information.

Figure 3-2.1: ACL Ports Configuration



ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Copy	Mirror	Logging	Shutdown	Counter
1	1	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	7682
2	1	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	0
3	1	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	0
4	1	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	0
5	1	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	0
6	1	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	0
7	1	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	0

Parameter descriptions:

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

Policy ID : Select the policy to apply to this port. The allowed values are 1 through 8. The default value is 1.

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

Rate Limiter ID : Select which rate limiter to apply on this port. The allowed values are Disabled or the values 1 through 16. The default value is "Disabled".

Port Copy : Select which port frames are copied on. The allowed values are Disabled or a specific port number. The default value is "Disabled".

Mirror : Specify the mirror operation of this port. The allowed values are:

Enabled: Frames received on the port are mirrored.

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

Logging : Specify the logging operation of this port. The allowed values are:

Enabled: Frames received on the port are stored in the System Log.

Disabled: Frames received on the port are not logged.

The default value is "Disabled". Please note that the System Log memory size and logging rate is limited.

Shutdown : Specify the port shut down operation of this port. The allowed values are:

Enabled: If a frame is received on the port, the port will be disabled.

Disabled: Port shut down is disabled. The default value is "Disabled".

Counter : Counts the number of frames that match this ACE.

Buttons

Save: Click to save changes.

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

Refresh : Click to refresh the page.

Clear : Click to clear the page.

3-2.2 Rate Limiters

The section describes how to configure the switch's ACL Rate Limiter parameters. The Rate Limiter Level from 1 to 16 that allow user to set rate limiter value and units with pps or kbps.

To configure ACL Rate Limiter in the web UI:

1. Click Configuration, ACL, then Rate Limiter

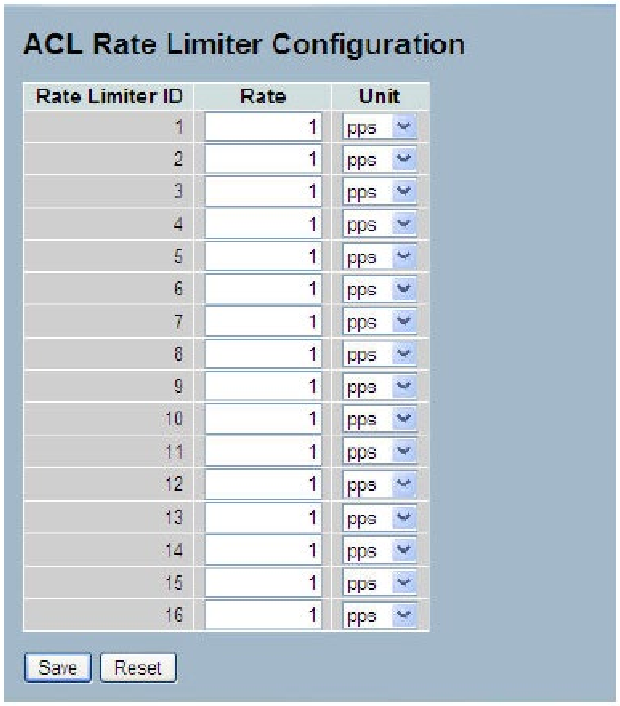
2. Specify the Rate field and the range from 0 to 3276700.

3. Set the Unit to pps or kbps

4. Click the Save button to save the setting

5. To cancel the settings click the Reset button to revert to previously saved values.

Figure 3-2.2: ACL Rate Limiter Configuration



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

Parameter descriptions:

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. Valid values are:

pps: packets per second.

kbps: Kbits per second.

Buttons

Save – Click to save changes.

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

3-2.3 Access Control List

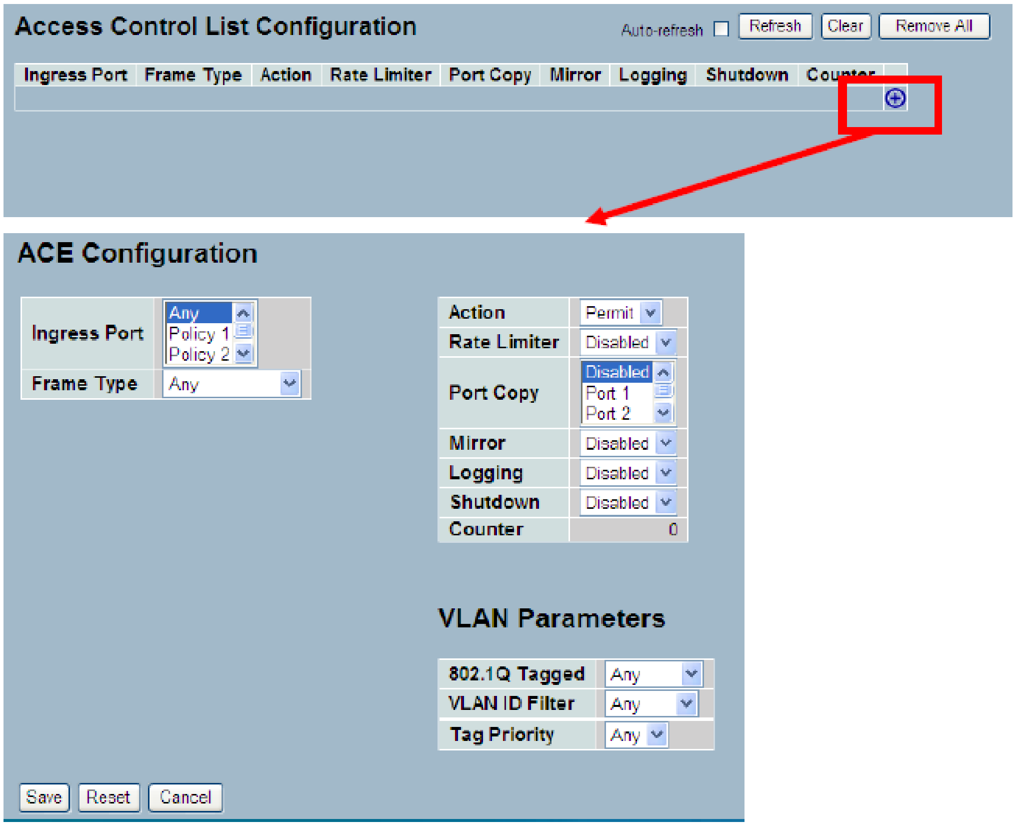
The section describes how to configure Access Control List rule. An Access Control List (ACL) is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress packets against the conditions in an ACL one by one. A 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.

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 256 on each switch. Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed and the priority is highest

To configure Access Control List in the web UI:

1. Click Configuration, ACL, then Configuration.
2. Click the ⊕ button to add a new ACL, or use the other ACL modification buttons to specify the editing action (i.e., edit, delete, or moving the relative position of entry in the list).
3. Specify the ACE parameters.
4. Click the Save button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.
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).

Figure 3-2.3: ACL Rate Limiter Configuration



Ingress Port	Frame Type	Action	Rate Limiter	Port Copy	Mirror	Logging	Shutdown	Counter
								⊕

Ingress Port	Any Policy 1 Policy 2
Frame Type	Any

Action	Permit
Rate Limiter	Disabled
Port Copy	Disabled Port 1 Port 2
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any

Parameter descriptions:

Ingress Port : Indicates the ingress port of the ACE. Possible values are:

Any: The ACE will match any ingress port.

Policy: The ACE will match ingress ports with a specific policy.

Port: The ACE will match a specific ingress port.

Frame Type : Indicates the frame type of the ACE. Possible values are:

Any: The ACE will match any frame type.

Ethernet T***ype***: 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.

Action : Indicates the forwarding action of the ACE.

Permit: Frames matching the ACE may be forwarded and learned.

Deny: Frames matching the ACE are dropped.

Rate Limiter : Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

Port Copy : Indicates the port copy 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 : Specify the mirror operation of this port. The allowed values are:

Enabled: Frames received on the port are mirrored.

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

Logging : 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.

Note that the System Log memory size and logging rate is limited.

Shutdown : 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.

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

⊕ : Inserts a new ACE before the current row.

ⓔ : Edits the ACE row.

↑ : Moves the ACE up the list.

↓ : Moves the ACE down the list.

⊗ : Deletes the ACE.

⊕ : The lowest plus sign adds a new entry at the bottom of the ACE listings.

Buttons

Save: Click to save changes.

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

Auto-refresh: Check to refresh the information automatically.

Refresh: Click to manually refresh the page immediately.

Clear: Click to clear the table settings.

Remove All: Clear all ACL configurations on the table.

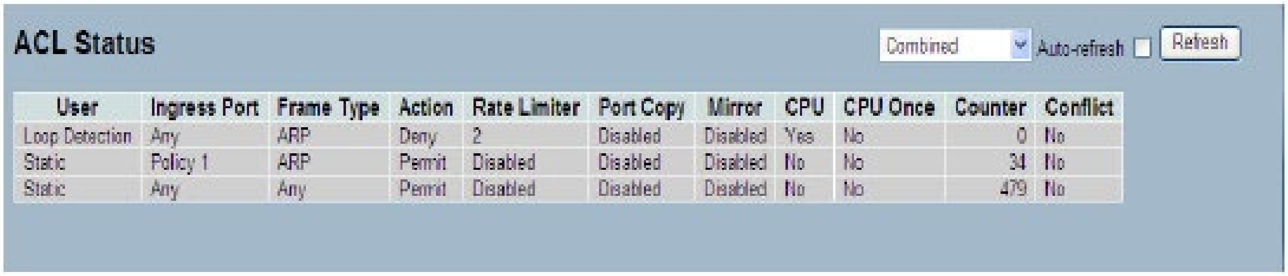
3-2.4 ACL Status

The section describes how to shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 256 on each switch.

To display the ACL status in the web UI:

1. Click Configuration, ACL, then ACL status.
2. At the user select dropdown select the desired user.
3. To automatically refresh the information check the "Auto-refresh" box.
4. Click " Refresh" to refresh the ACL Status.

Figure 3-2.4: ACL Rate Limiter Configuration



ACL Status

Combined Auto-refresh □ Refresh

User	Ingress Port	Frame Type	Action	Rate Limiter	Port Copy	Mirror	CPU	CPU Once	Counter	Conflict
Loop Detection	Any	ARP	Deny	2	Disabled	Disabled	Yes	No	0	No
Static	Policy 1	ARP	Permit	Disabled	Disabled	Disabled	No	No	34	No
Static	Any	Any	Permit	Disabled	Disabled	Disabled	No	No	479	No

Parameter descriptions:

User : Indicates the ACL user.

Ingress Port : Indicates the ingress port of the ACE. Possible values are:

Any: The ACE will match any ingress port.

Policy: The ACE will match ingress ports with a specific policy.

Port: The ACE will match a specific ingress port.

Frame Type : Indicates the frame type of the ACE. Possible values are:

Any: The ACE will match any frame type.

EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

Action : Indicates the forwarding action of the ACE.

Permit: Frames matching the ACE may be forwarded and learned.

Deny: Frames matching the ACE are dropped.

Rate Limiter : Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

Port Copy : Indicates the port copy 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 : Specify the mirror operation of this port. The allowed values are:

Enabled: Frames received on the port are mirrored.

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

CPU : Forward packet that matched the specific ACE to CPU.

CPU Once : Forward 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 : Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

Buttons:

Auto-refresh : To evoke the auto-refresh to refresh the information automatically.

Refresh : Click to refresh the ACL status information manually.

3-3 Aggregation

The 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

The 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.

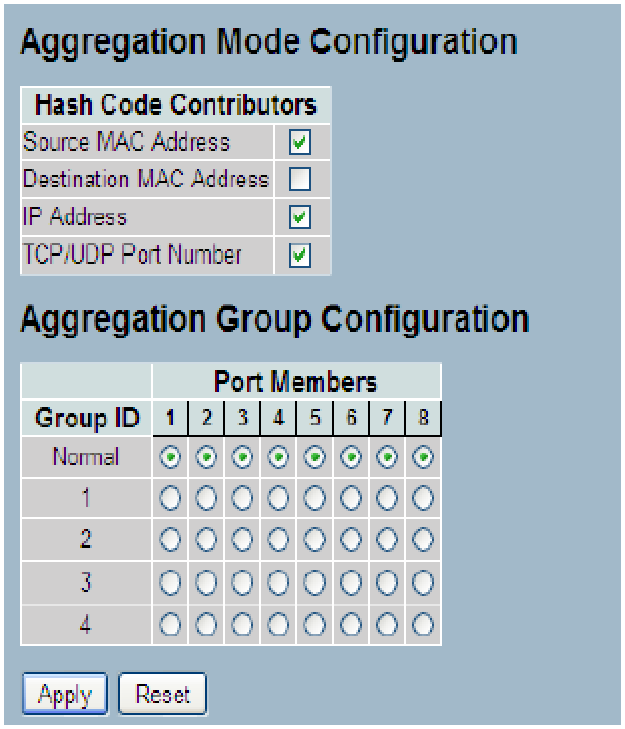
3-3.1.1 Static Trunk

Ports using Static Trunk as their trunk method can choose their unique Static GroupID to form a logic "trunked port". The benefit of using 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 your 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 "not ready" state when using static trunk to aggregate with high speed links.

To configure the Trunk Aggregation Hash mode and Aggregation Group in the web UI:

1. Click Configuration, Static Trunk, and then Aggregation Mode Configuration.
2. Enable or disable the Aggregation Mode function.
1. Evoke Aggregation Group ID and Port members
2. Click the Save button to save the settings.
3. To cancel the settings click the Reset button to revert to previously saved values.

Figure 3-3.1.1: Aggregation Mode Configuration



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
Normal	●	●	●	●	●	●	●	●
1	○	○	○	○	○	○	○	○
2	○	○	○	○	○	○	○	○
3	○	○	○	○	○	○	○	○
4	○	○	○	○	○	○	○	○

Parameter descriptions:

Hash Code Contributors

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

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

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

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

Aggregation Group Configuration

Locality : Indicates the aggregation group type. This field is only valid for switches.

> ***Global***: The group members may reside on different units. The device supports two 8-port global aggregations.
>
> ***Local***: The group members reside on the same unit. Each local aggregation may consist of up to 16 members.

Group ID : Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.

Port Members : Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.

Buttons

Save : Click to save changes.

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

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.

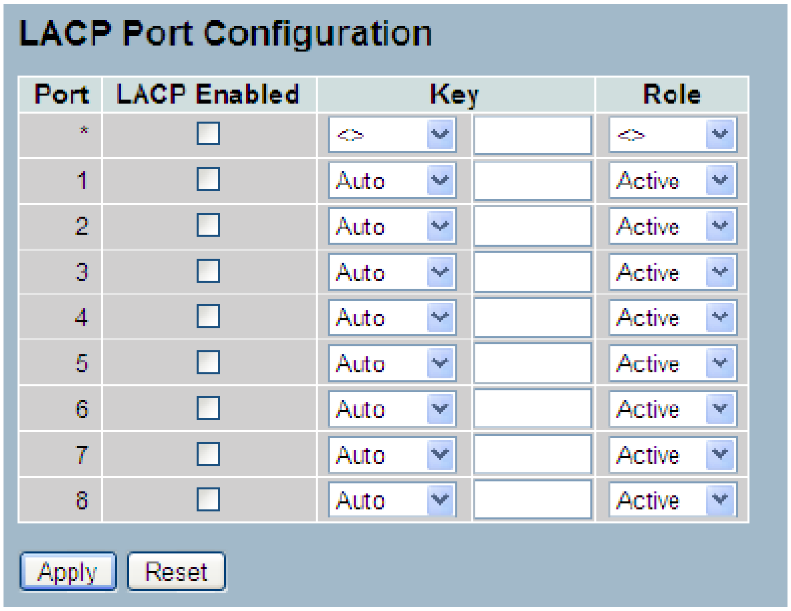
3-3.2.1 Configuration

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

To configure LACP parameters in the web UI:

1. Click Configuration, LACP, Configuration.
2. Enable or disable LACP on the switch ports.
3. Set the Key parameter to Auto or Specific. The default is Auto.
4. Set the Role to Active or Passive. The default is Active
5. Click the Save button to save the settings.
6. To cancel the settings click the Reset button to revert to previously saved values.

Figure 3-3.2.1: LACP Port Configuration



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

Parameter descriptions:

Port : The switch port number.

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

Key : The Key value incurred by the port, range 1-65535. 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 : Shows LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to).

Buttons

Apply : Click to save changes.

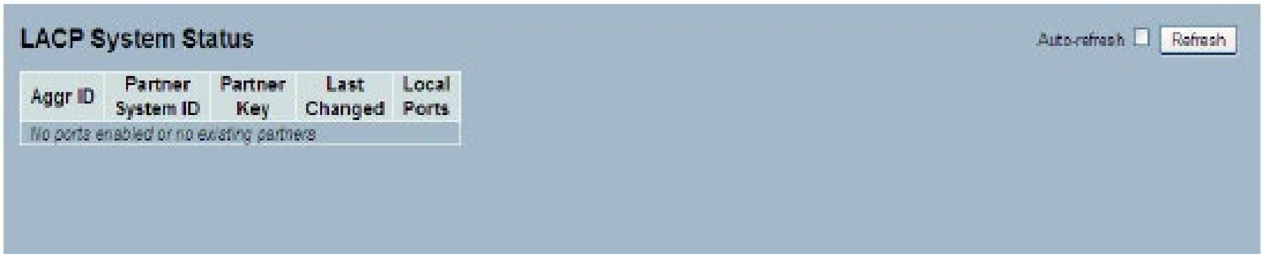
Reset : Click to undo any changes made locally and revert to previously saved values.

3-3.2.2 System Status

This page displays a status overview for all LACP instances. To display the LACP System status in the web UI:

1. Click Configuration, LACP, System Status.
2. To automatically refresh the information check the “Auto-refresh” box.
3. Click “ Refresh“ to refresh the LACP System Status.

Figure 3-3.2.2: 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				

Parameter descriptions:

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

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

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

Last changed : The time since this aggregation changed.

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

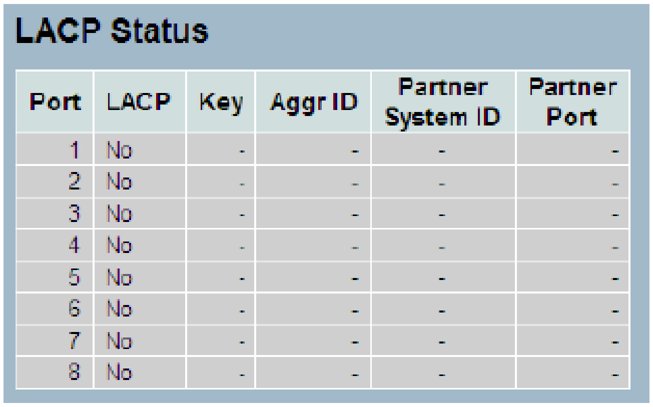
Buttons:
Auto-refresh: Check to automatically refresh page information.
Refresh : Click to immediately refresh the page manually.

3-3.2.3 Port Status

This page displays Port Status overview for all LACP instances. To display the LACP Port status in the web UI:

1. Click Configuration, LACP, Port Status.
2. To automatically refresh the page check the "Auto-refresh" checkbox.
3. Click " Refresh" to refresh the LACP Port Status.

Figure 3-3.2.3: LACP Status



LACP 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	-	-	-	-

Parameter descriptions:

Port : 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 it's 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 : The partner's System ID (MAC address).

Partner Port : The partner's port number connected to this port.

Buttons:

Auto-refresh: Click to automatically refresh the page.

Refresh : Click to manually refresh the LACP port status information manually.

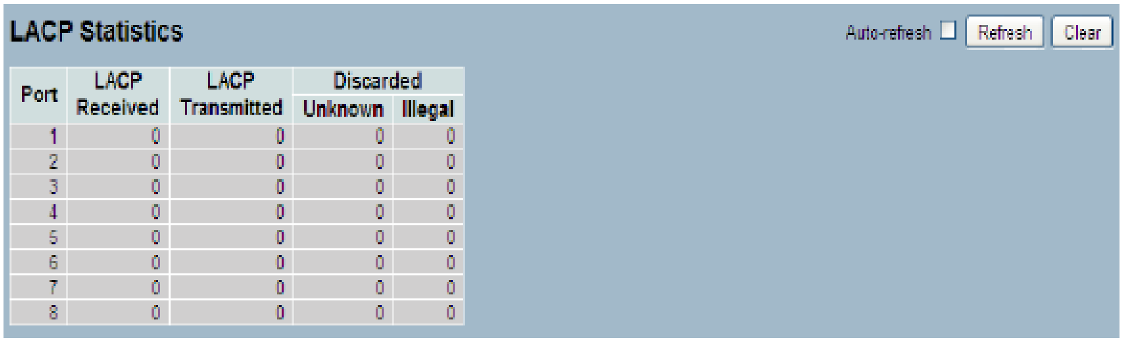
3-3.2.4 Port Statistics

This section describes that when you complete to set LACP function on the switch then it provides a Port Statistics overview for all LACP instances

To display LACP Port status in the web UI:

1. Click Configuration, LACP, Port Statistics.
2. To auto-refresh the information check “Auto refresh”.
3. Click “ Refresh“ to manually refresh the LACP Statistics.

Figure 3-3.2.4: 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

Parameter descriptions:

Port : The switch port number.

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

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

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

Buttons:

Auto-refresh: Click to automatically refresh the page.

Refresh : Click to manually refresh the LACP port status information manually.

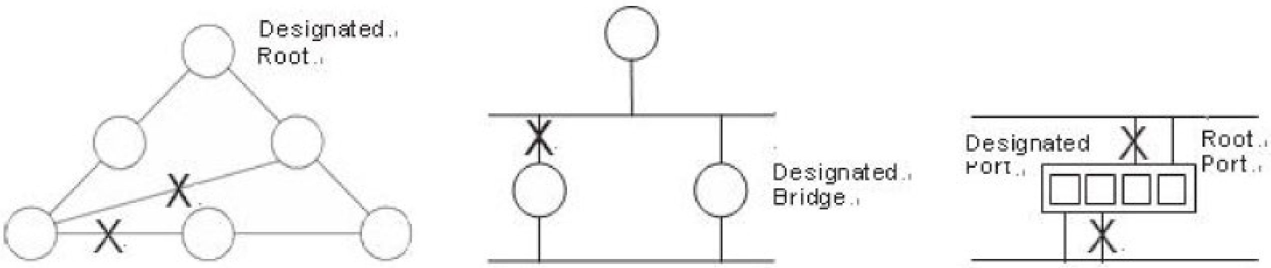
Clear : Click to clear the statistics.

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 (that is, an 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 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 ports, eliminating 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.



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.

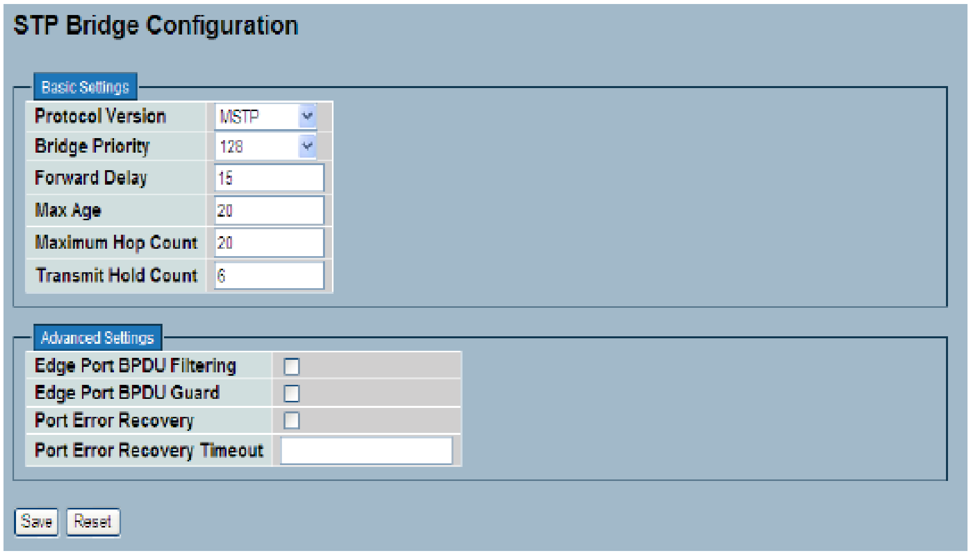
3-4.1 Bridge Settings

The section describes that how to configure the Spanning Tree Bridge and STP System settings. It allows you to configure STP System settings are used by all STP Bridge instances in the Switch.

To configure Spanning Tree Bridge Settings parameters in the web UI:

1. Click Configuration, Spanning Tree, Bridge Settings
2. Scroll to select the parameters and write down available value of parameters in blank field in Basic Settings
3. Enable or disable the parameters and write down available value of parameters in blank field in Advanced settings.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

Figure 3-4.1: STP Bridge Configuration



STP Bridge Configuration

Basic Settings

Protocol Version	MSTP
Bridge Priority	128
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	

Parameter descriptions:

Basic Settings

Protocol Version : The STP protocol version setting. Valid values are STP, RSTP and MSTP.

Bridge Priority : Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.

Forward Delay :The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

Max Age : The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2.

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

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

Advanced Settings

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

Edge Port BPDU Guard : Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.

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

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

Buttons

Save – Click to save changes.

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

values.

2-4.2 MSTI Mapping

When you implement an Spanning Tree protocol on the switch that the bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.

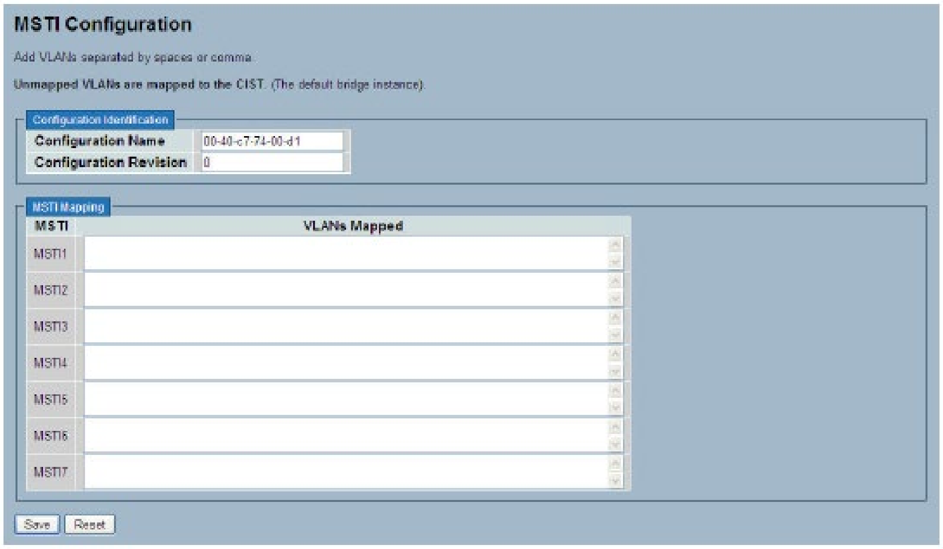
Due to the reason that you need to set the list of VLANs mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.)

This section describes it allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

To configure Spanning Tree MSTI Mapping parameters in the web UI:

1. Click Configuration, Spanning Tree, MSTI Mapping.
2. Specify the Configuration Identification parameters in the field.
3. Specify the VLANs Mapped blank field.
4. Click the Save button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

Figure 3-4.2: MSTI Configuration



MSTI Configuration

Add VLANs separated by spaces or comma.

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

Configuration Identification

Configuration Name	00-40-c7-74-00-d1
Configuration Revision	0

MSTI Mapping

MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

Parameter descriptions:

Configuration Identification

Configuration Name : The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name can be up to 32 characters long.

Configuration Revision : The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI Mapping

MSTI : The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.

VLANs Mapped : The list of 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. (i.e., not having any VLANs).

Buttons

Save : Click to save changes.

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

3-4.3 MSTI Priorities

When you implement an Spanning Tree protocol on the switch that the bridge instance. The CIST is the default instance which is always active. For 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.

This section describes how to set and view current STP MSTI bridge instance priority parameters.

To configure the Spanning Tree MSTI Priorities parameters in the web UI:

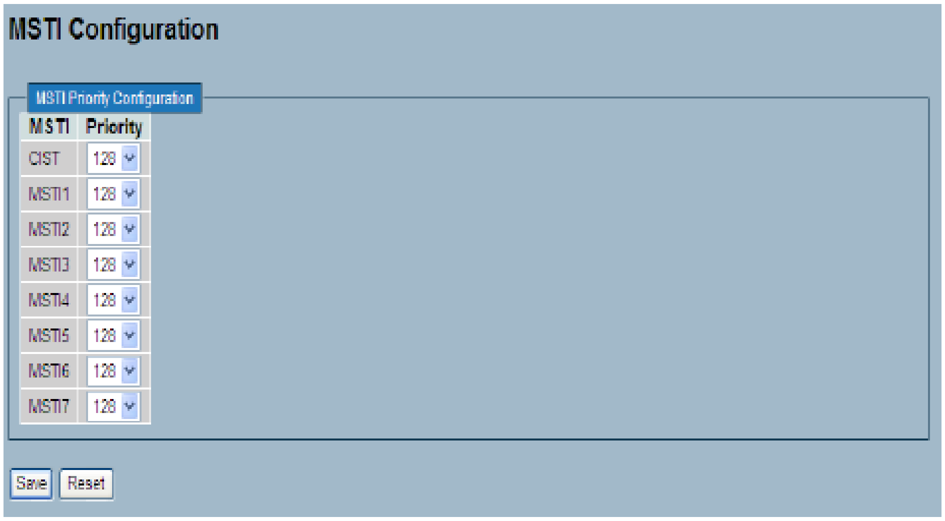
1. Click Configuration, Spanning Tree, MSTI Priorities.

2. Set the Priority; the maximum is 240. The default is 128.

3. Click the Save button to save the settings.

4. To cancel the settings click the Reset button to revert to previously saved values.

Figure 3-4.3: MSTI Configuration



MSTI	Priority
CIST	128
MSTI1	128
MSTI2	128
MSTI3	128
MSTI4	128
MSTI5	128
MSTI6	128
MSTI7	128

Parameter descriptions:

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

Priority : Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

Buttons

Save – Click to save changes.

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

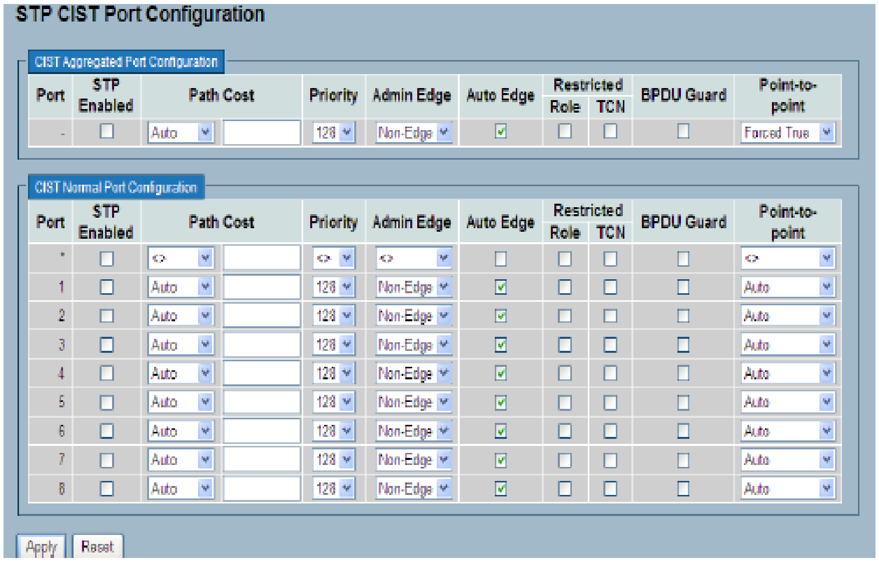
3-4.4 CIST Ports

When you implement a Spanning Tree protocol on the switch that the bridge instance. You need to configure the CIST Ports. This page lets you set and view current STP CIST port parameters.

To configure Spanning Tree CIST Ports parameters in the web UI:

1. Click Configuration, Spanning Tree, CIST Ports.
2. Scroll and evoke to set all parameters of CIST Aggregated Port Configuration.
3. Evoke to enable or disable the STP, then scroll and evoke to set all parameters of the CIST normal Port configuration.
4. Click the Save button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

Figure 3-4.4: STP CIST Port Configuration



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

Parameter descriptions:

Port : The switch port number of the logical STP port.

STP Enabled : Controls whether STP is enabled on this switch port.

Path Cost : Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.

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

operEdge (state flag) : Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). 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 : Controls whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized).

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

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

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

BPDU Guard : If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not affect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.

Point to Point : Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. The 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 undo any changes made locally and revert to previously saved values.

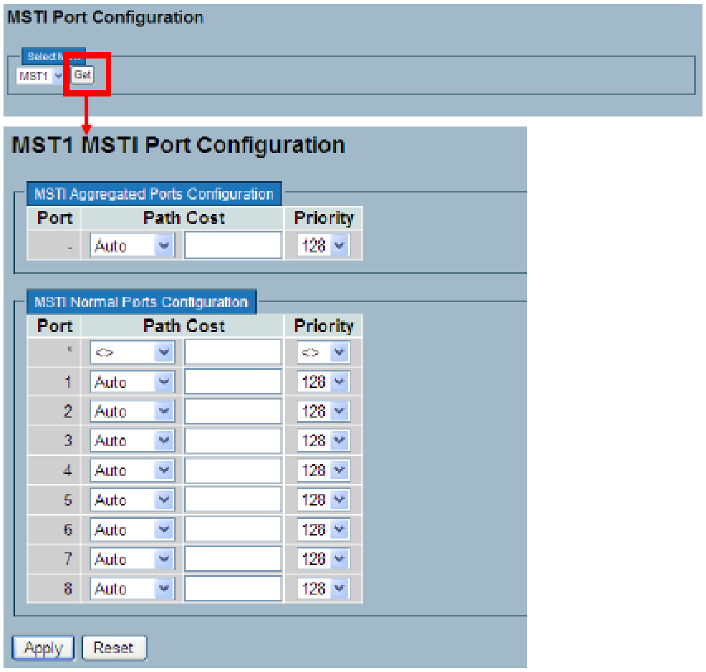
3-4.5 MSTI Ports

The section describes how to set and view 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.

To configure Spanning Tree MSTI Port parameters in the web UI:

1. Click Configuration, Spanning Tree, MSTI Ports.
2. Select the MST1 or other MSTI Port.
3. Click Get to set the detail parameters of the MSTI Ports.
4. Set all parameters of the MSTI Port configuration.
5. Click the Save button to save the settings.
6. To cancel the settings click the Reset button to revert to previously saved values.

Figure 3-4.5: MSTI Port Configuration



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

Parameter descriptions:

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

Path Cost : Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.

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

Buttons

Save : Click to save changes.

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

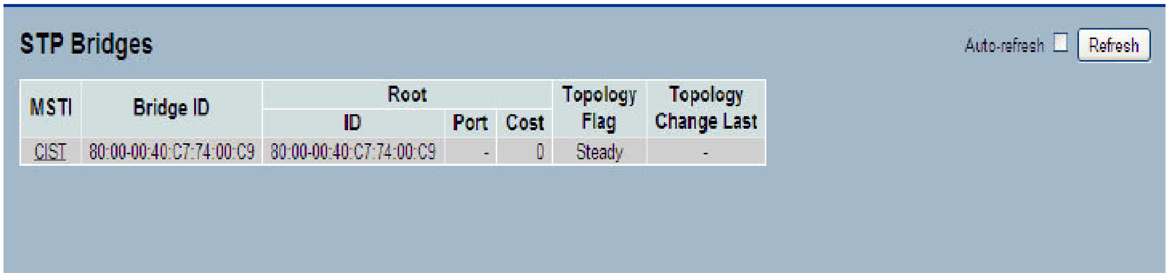
3-4.6 Bridge Status

After you complete the MSTI Port configuration then you can view the Bridge Status. This page provides a status overview of all STP bridge instances. The displayed table contains a row for each STP bridge instance.

To display STP Bridges status in the web UI:

1. Click Configuration, Spanning Tree, STP Bridges.
2. To auto-refresh the information check “Auto-refresh”.
3. Click “Refresh“ to refresh the STP Bridges.

Figure 3-4.6: STP Bridges status



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

Parameter descriptions:

MSTI : The Bridge Instance. This is also a link to the STP Detailed Bridge Status.

Bridge ID : The Bridge ID of this Bridge instance.

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

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

Root Cost : Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Topology Flag : The current state of the Topology Change Flag of this Bridge instance.

Topology Change Last : The time since last Topology Change occurred.

Buttons

Auto-refresh: Check to automatically refresh the page.

Refresh : Click for refresh the STP Bridges status information manually.

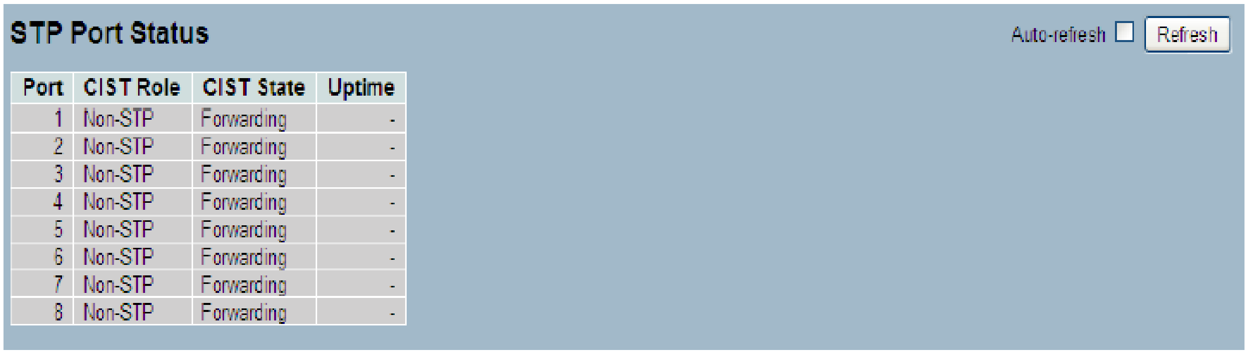
3-4.7 Port Status

After you complete the STP configuration you can view the STP Port Status. This page displays the STP CIST port status for physical ports of the switch.

To display STP Port status in the web UI:

1. Click Configuration, Spanning Tree, STP Port Status.
2. To automatically refresh the information check the “Auto-refresh” checkbox.
3. Click “Refresh“ to refresh the STP Bridges.

Figure 3-4.7: STP Port status



STP Port Status

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

Parameter descriptions:

Port : The switch port number of the logical STP port.

CIST Role : The current STP port role of the CIST port. The port role can be one of the following values: AlternatePort, BackupPort, RootPort, DesignatedPort, or Disabled.

CIST State : The current STP port state of the CIST port. The port state can be one of the following values: Blocking, Learning, or Forwarding.

Uptime : The time since the bridge port was last initialized.

Buttons:

Auto-refresh: Check the box to automatically refresh the information automatically.

Refresh: Click to refresh the STP Port status information manually.

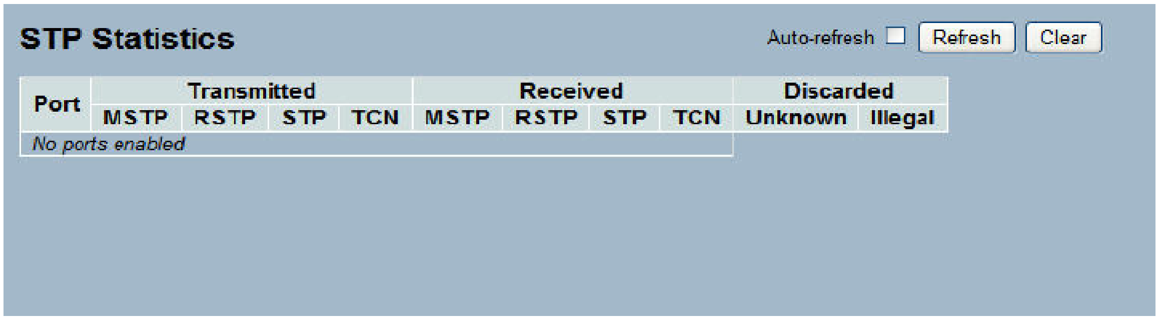
3-4.8 Port Statistics

After you complete the STP configuration you can view the STP Statistics. This page displays the STP Statistics detail counters of bridge ports in the currently selected switch.

To display the STP Port status in the web UI:

1. Click Configuration, Spanning Tree, Port Statistics.
2. To automatically refresh the information check the “Auto-refresh” checkbox.
3. Click “ Refresh“ to refresh the STP Bridges.

Figure 3-4.8: STP Statistics



STP Statistics

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

Parameter descriptions:

Port : The switch port number of the logical STP port.

MSTP : The number of MSTP Configuration BPDU's received/transmitted on the port.

RSTP : The number of RSTP Configuration BPDU's received/transmitted on the port.

STP : The number of legacy STP Configuration BPDU's received/transmitted on the port.

TCN : The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.

Discarded Unknown : The number of unknown Spanning Tree BPDU's received (and discarded) on the port.

Discarded Illegal : The number of illegal Spanning Tree BPDU's received (and discarded) on the port.

Buttons:

Auto-refresh: Click to automatically refresh the information.

Refresh : Click to refresh the STP Statistics information manually.

Clear: Click to refresh the STP Statistics information or clear by manually.

3-5 IGMP Snooping

This function is used to establish the multicast groups to forward the multicast packet to the member ports, and, in nature, avoids wasting the bandwidth while IP multicast packets are running over the network. This is because a switch that does not support IGMP or IGMP Snooping cannot tell the multicast packet from the broadcast packet, so it can only treat them all as the broadcast packet. Without IGMP Snooping, the multicast packet forwarding function is plain and nothing is different from broadcast packet.

A switch supported IGMP Snooping with the functions of query, report and leave, a type of 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. With this function, 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 must be running IGMP.

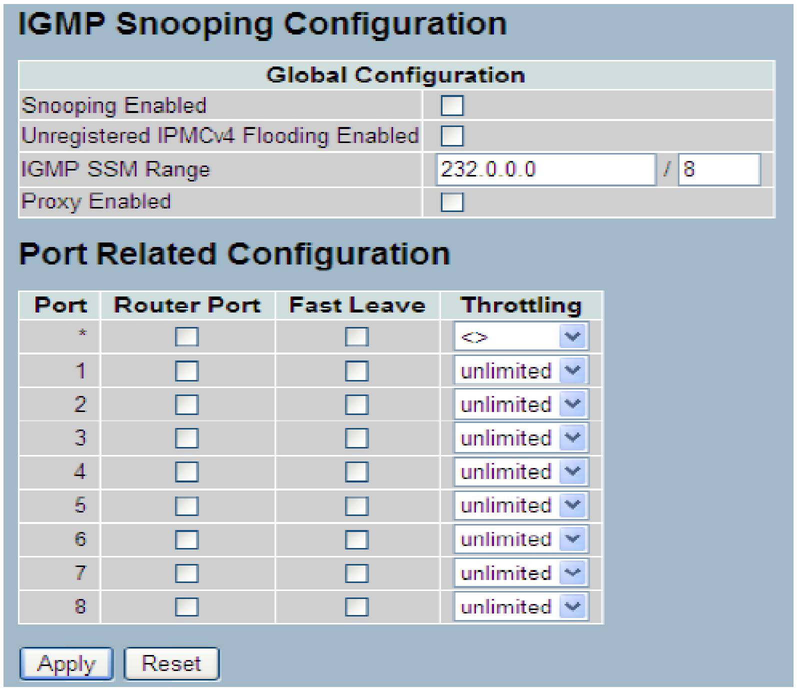
3-5.1 Basic Configuration

This page lets you set 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 must be running IGMP.

To configure IGMP Snooping parameters in the web UI:

1. Click Configuration, IGMP Snooping, Basic Configuration.
2. Evoke to select enable or disable which Global configuration
3. Evoke which port wants to become a Router Port or enable/ disable the Fast Leave function..
4. Scroll to set the Throttling parameter.
5. Click the Save button to save the settings.
6. To cancel the settings click the Reset button to revert to previously saved values.

Figure 3-5.1: IGMP Snooping Configuration



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

Parameter descriptions:

Snooping Enabled: Enable the Global IGMP Snooping.

Unregistered IPMCv4 Flooding enabled : Enable 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 :Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Port : Shows the physical Port index of switch.

Router Port : Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave : Enable the fast leave on the port.

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

Buttons

Save : Click to save changes.

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

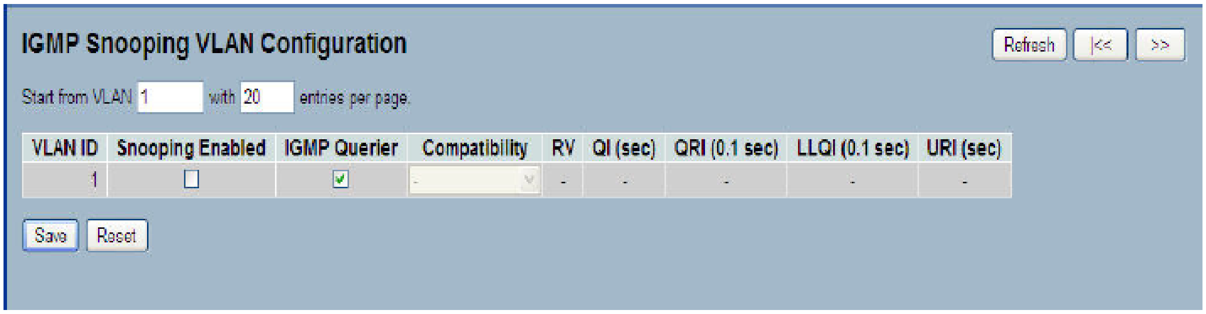
3-5.2 VLAN Configuration

The section describes the VLAN configuration setting process integrated with IGMP Snooping function. For Each setting page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table. The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the Refresh button will update the displayed table starting from that or the next closest VLAN Table match.

To configure IGMP Snooping VLAN parameters in the web UI:

1. Click Configuration, IGMP Snooping, VLAN Configuration
2. Evoke to select enable or disable Snooping , IGMP Querier Specify the parameters in the blank field.
3. Click the refresh to update the data or click << or >> to display previous entry or next entry.
4. Click the save to save the setting
5. To cancel the settings click the Reset button to revert to previously saved values.

Figure 3-5.2: IGMP Snooping VLAN Configuration.



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	□	☑	-	-	-	-	-	-

Parameter descriptions:

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

Snooping Enabled : Enable 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 taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selections are IGMP-Auto, Forced IGMPv1, Forced IGMPv2, and Forced IGMPv3. The default compatibility value is IGMP-Auto.

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

QI : Query Interval. The QI is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds; default query interval is 125 seconds.

QRI : Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of a second; default query response interval is 100 in tenths of seconds (10 seconds).

LLQI (LMQI for IGMP) : Last Member Query Interval. The LLQI is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds; default last member query interval is 10 in tenths of a second (1 second).

URI : Unsolicited Report Interval. The URI is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.

Buttons :

Save : Click to save changes.

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

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

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

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

3-5.3 Port Group Filtering

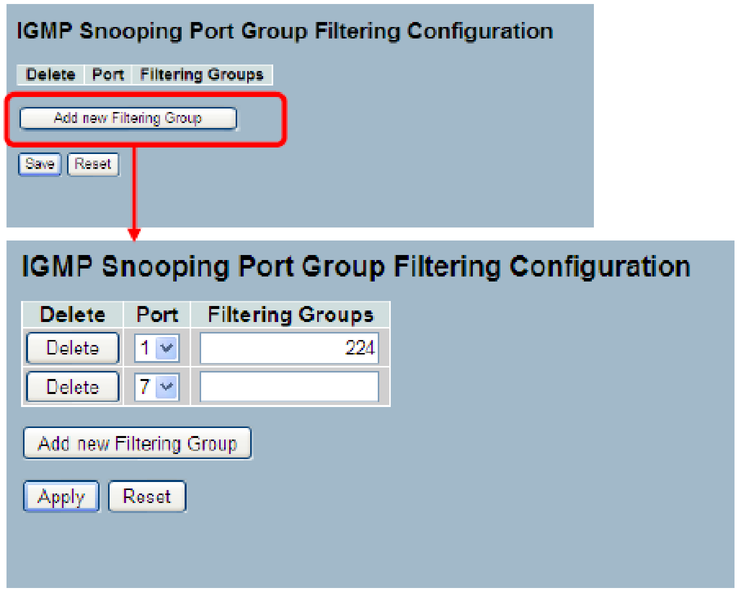
This section lets you set the IGMP Port Group Filtering parameters. With the IGMP filtering feature, you can exert this type of control. In some network application environments, such as the metropolitan or multiple-dwelling unit (MDU) installations, you may want to control the multicast groups to which a user on a switch port can belong. This lets you control the distribution of multicast services, such as IP/TV, based on some type of subscription or service plan.

With this feature you can filter multicast joins on a per-port basis by configuring 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 denying access to a multicast group is applied to a switch port, 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.

To configure IGMP Snooping Port Group parameters in the web UI:

1. Click Configuration, IGMP Snooping, Port Group Filtering
2. Click Add new Filtering Group
3. Scroll the Port to enable the Port Group Filtering.
4. Specify the Filtering Groups in the blank field.
5. Click the save to save the setting
6. To cancel the setting click the Reset button to revert to previously saved values.

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



IGMP Snooping Port Group Filtering Configuration

Delete	Port	Filtering Groups
Delete	1	224
Delete	7	

Parameter descriptions:

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

Port : To evoke the port enable the IGMP Snooping Port Group Filtering function.

Filtering Groups : The IP Multicast Group that will be filtered.

Buttons:

Save : Click to save changes.

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

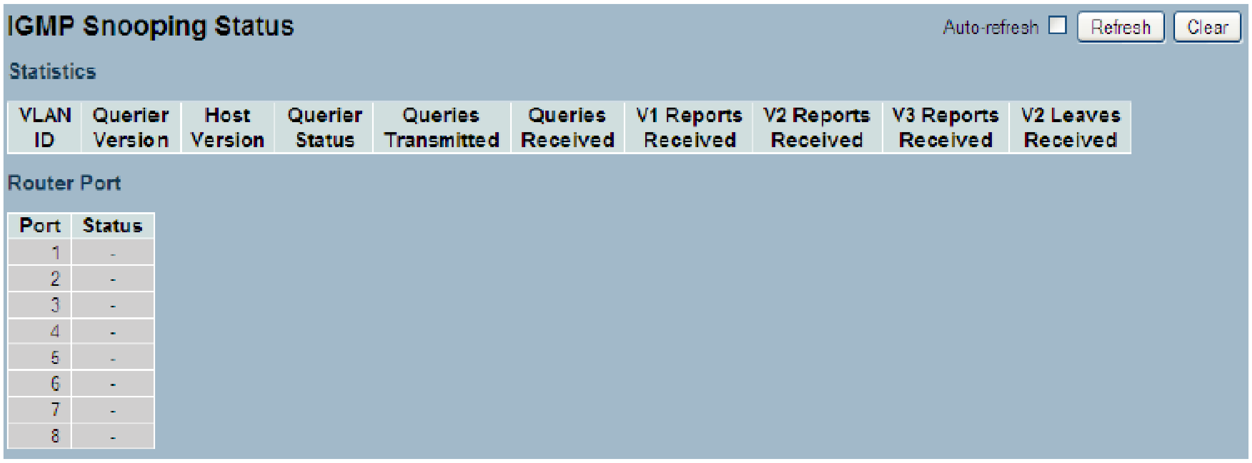
3-5.4 Status

After you complete the IGMP Snooping configuration, then you can view the IGMP Snooping status. This page displays the IGMP Snooping detail status.

To display the IGMP Snooping status in the web UI:

1. Click Configuration, IGMP Snooping, Status.
2. To automatically refresh the information check the “Auto-refresh” box.
3. Click “ Refresh“ to refresh the IGMP Snooping Status.
4. Click “ Clear“ to clear the IGMP Snooping Status.

Figure 3-5.4: 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	-

Parameter descriptions:

VLAN ID : The VLAN ID of the entry.

Querier Version : Working Querier Version currently.

Host Version : Working Host Version currently.

Querier Status : Shows the Querier status as "ACTIVE" or "IDLE".

Queries Transmitted : The number of Transmitted Queries.

Queries Received : The number of Received Queries.

V1 Reports Received : The number of Received V1 Reports.

V2 Reports Received : The number of Received V2 Reports.

V3 Reports Received : The number of Received V3 Reports.

V2 Leaves Received : The number of Received V2 Leaves.

Buttons:

Auto-refresh : Check to automatically refresh the log automatically.

Refresh : Click to refresh the Status manually.

Clear : Click to clear the Status manually.

3-5.5 Group Information

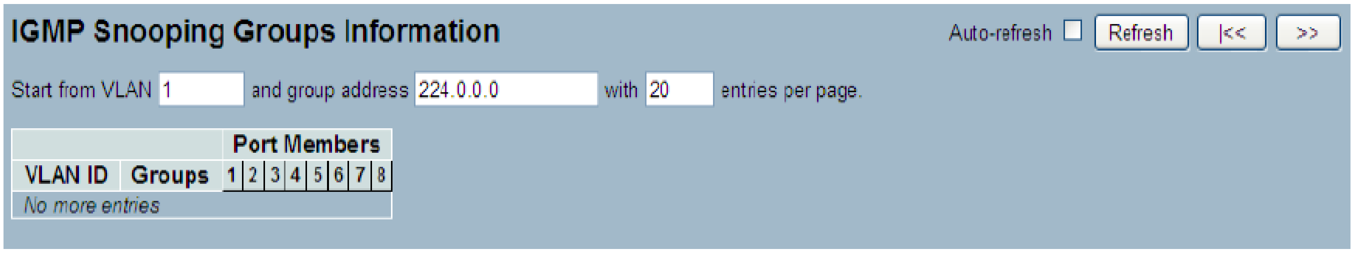
After you complete to set the IGMP Snooping function you can view the IGMP Snooping Group Information. Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group. The will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the IGMP Group Table. The will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table.

To display the IGMP Snooping Group Information in the web UI:

1. Click Configuration, IGMP Snooping, Group Information
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “ Refresh“ to refresh a entry of the IGMP Snooping Groups Information.
4. Click “<<” or “>> “ to move to previous or next entry.

Figure 3-5.5: IGMP Snooping Groups Information.



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
No more entries									

Parameter descriptions:

VLAN ID : VLAN ID of the group.

Groups : Group address of the group displayed.

Port Members : Ports under this group.

Buttons:

Auto-refresh : Check to refresh the log automatically.

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

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

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

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 is indicating 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.

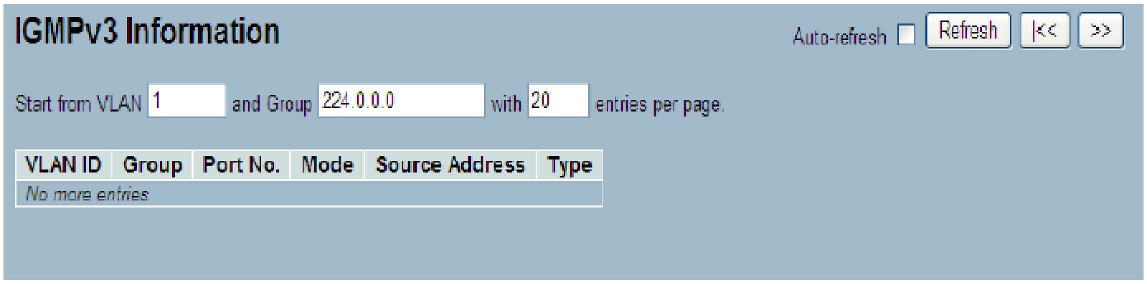
Addresses in the range 232.0.0.0/8 (232.0.0.0 to 232.255.255.255) are reserved for SSM by IANA. In the switch, you can configure SSM for arbitrary IP multicast addresses also.

Each page shows up to 99 entries from the IGMPv3 SSM (Source Specific Multicast) Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMPv3 Information table. The "Start from VLAN", and "Group" input fields let you select the starting point in the IGMPv3 Information Table. Clicking the 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 |<< button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address. The >> button will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "*No more entries*" is shown in the displayed table. Use the |<< button to start over.

To display IGMPv3 IPv4 SSM Information in the web UI:

1. Click Configuration, IGMP Snooping, IPv4 SSM Information.
2. To auto-refresh the information check “Auto-refresh”.
3. Click “ Refresh“ to refresh an entry of the IGMPv3 IPv4 SSM Information.
4. Click “<<” or “>> “ to move to the previous or next entry.

Figure 3-6.6: IGMPv3 IPv4 SSM Information.



IGMPv3 Information

Auto-refresh □ Refresh |<< >>

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

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

Parameter descriptions:

VLAN ID : VLAN ID of the group.

Group : Group address of the group displayed.

Port : Switch port number.

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

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

Type : Indicates the Type. It can be either Allow or Deny.

Buttons:

Auto-refresh : Check to refresh the log automatically.

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

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

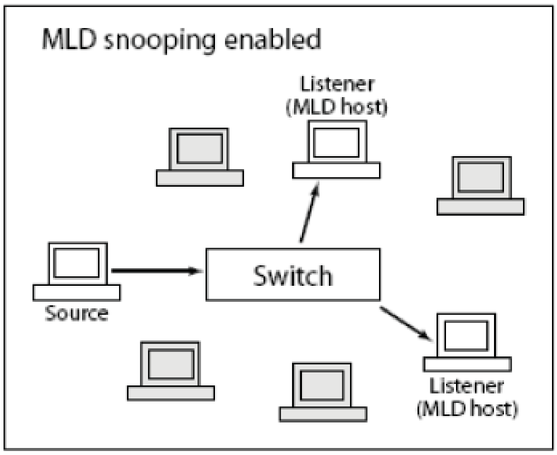
>> : Update the table, starting with the entry after the last entry currently displayed.

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, that 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 (that is, "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 that 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.

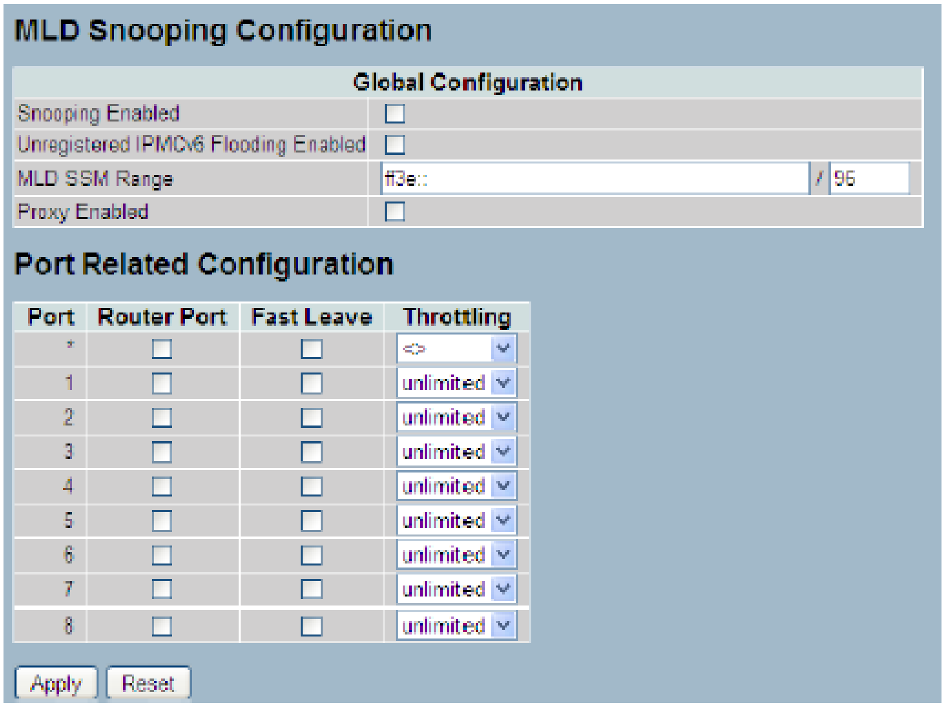


3-6.1 Basic Configuration

This page lets you configure basic MLD Snooping parameters. To configure MLD Snooping in the web UI:

1. Click Configuration, MLD Snooping, Basic Configuration.
2. Enable or disable the Global configuration parameters.
3. Evoke the port to join Router port and Fast Leave.
4. Scroll to select the Throttling mode with unlimited or 1 to 10.
5. Click the Save button to save the settings.
6. To cancel the settings click the Reset button to revert to previously saved values.

Figure 3-6.1: MLD Snooping Configuration.



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

Parameter descriptions:

Snooping Enabled : Enable the Global MLD Snooping.

Unregistered IPMCv6 Flooding enabled : Enable 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 : Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Port: The Port index what you enable or disable the MLD Snooping function.

Fast Leave : To evoke to enable the fast leave on the port.

Router Port : Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

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

Buttons:

Save : Click to save changes.

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

3-6.2 VLAN Configuration

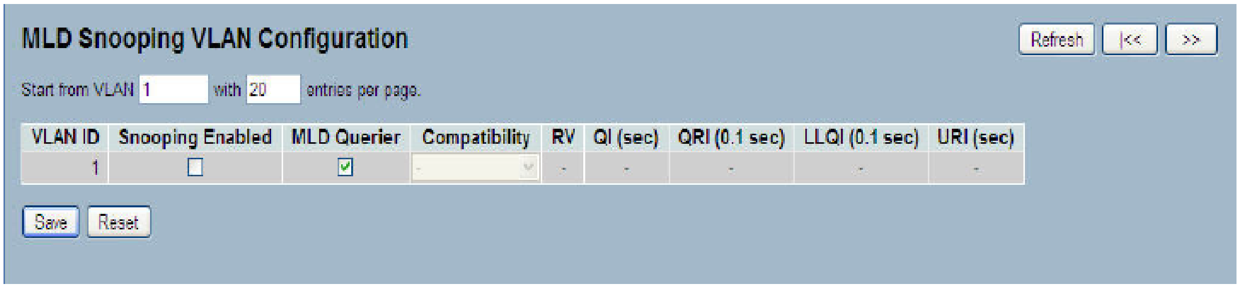
When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports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

The will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

To configure MLD Snooping VLAN in the web UI:

1. Click Configuration, MLD Snooping, VLAN Configuration.
2. Specify the VLAN ID and entries per page.
3. Click " Refresh" to refresh an entry.
4. Click "<<" or ">>" to move to the previous or next entry.

Figure 3-7.2: MLD Snooping VLAN Configuration.



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	□	☑	-	-	-	-	-	-

Parameter descriptions:

VLAN ID : The VLAN ID of the entry.

Snooping Enabled : Enable 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 taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The allowed selections are MLD-Auto, Forced MLDv1, and Forced MLDv2. The default compatibility value is MLD-Auto.

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

QI : Query Interval. The QI is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds; default query interval is 125 seconds.

QRI : Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds; default query response interval is 100 in tenths of seconds (10 seconds). .

LLQI (LMQI for IGMP) : Last Listener Query Interval. The LLQI is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address. Specific Queries sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages. The allowed range is 0 to 31744 in tenths of seconds, default last listener query interval is 10 in tenths of seconds (1 second).

URI : Unsolicited Report Interval. The URI is the time between repetitions of a node's initial report of interest in a multicast address. The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.

Buttons:

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

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

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

Save : Click to save changes.

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

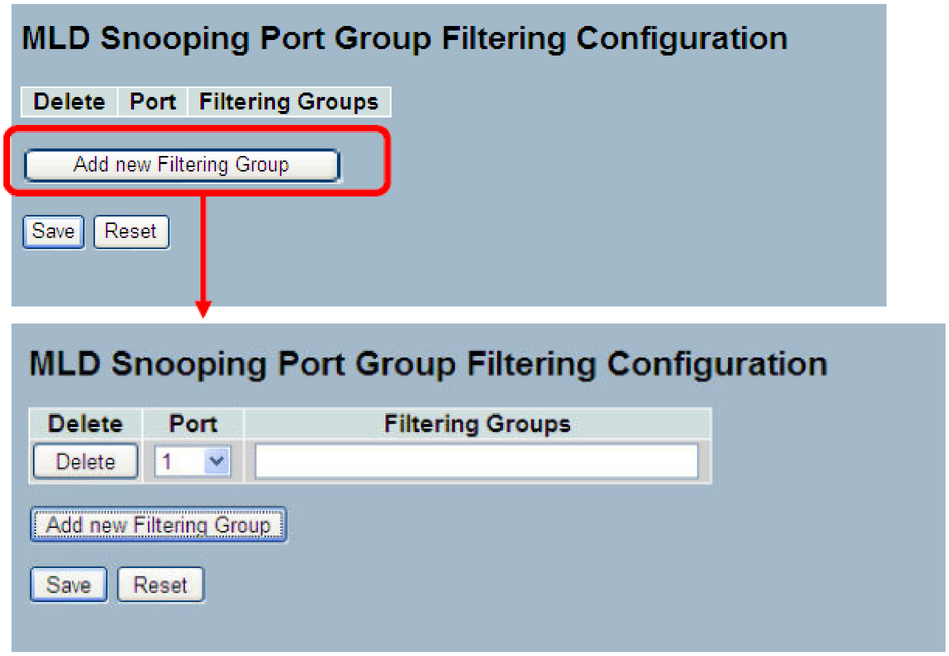
3-6.3 Port Group Filtering

This page lets you set the Port Group Filtering in the MLD Snooping function, and add new filtering group and safety policy.

To configure the MLD Snooping Port Group parameters in the web UI:

1. Click Configuration, MLD Snooping, Port Group Filtering Configuration.
2. Click the Add New Filtering Group button.
3. Specify the Filtering Groups and entries per page.
4. Click the Save button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

Figure 3-7.3: MLD Snooping Port Group Filtering Configuration



MLD Snooping Port Group Filtering Configuration

Delete	Port	Filtering Groups

MLD Snooping Port Group Filtering Configuration

Delete	Port	Filtering Groups
Delete	1	

Parameter descriptions:

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

Port : The logical port for the settings. You can evoke to enable the port to join filtering Group.

Filtering Groups : The IP Multicast Group that will be filtered.

Buttons:

Save : Click to save changes.

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

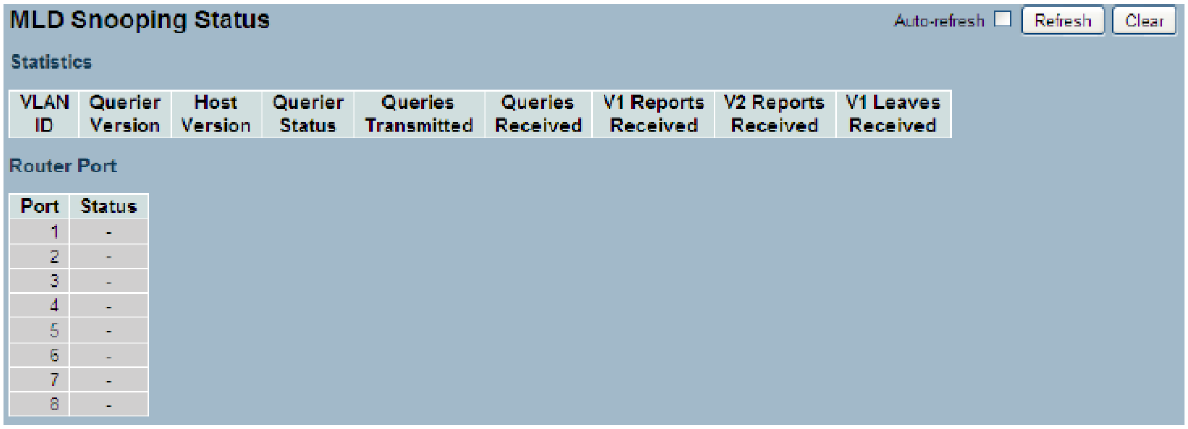
3-6.4 Status

This page lets you set and view MLD Snooping and MLD Snooping Status and detail information.

To display MLD Snooping Status in the web UI:

1. Click Configuration, MLD Snooping, Status.
2. To auto-refresh the information check "Auto-refresh".
3. Click " Refresh" to refresh an entry of the MLD Snooping Status Information.
4. Click " Clear" to clear the MLD Snooping Status.

Figure 3-6.4: 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	-

Parameter descriptions:

VLAN ID : The VLAN ID of the entry.

Querier Version : Working Querier Version currently.

Host Version : Working Host Version currently.

Querier Status : Show the Querier status is "ACTIVE" or "IDLE".

Queries Transmitted : The number of Transmitted Queries.

Queries Received : The number of Received Queries.

V1 Reports Received : The number of Received V1 Reports.

V2 Reports Received : The number of Received V2 Reports.

V1 Leaves Received : The number of Received V1 Leaves.

Buttons:

Auto-refresh : Click the icon then the device will refresh the log automatically.

Refresh : Click to manually refresh the page immediately.

3-6.5 Group Information

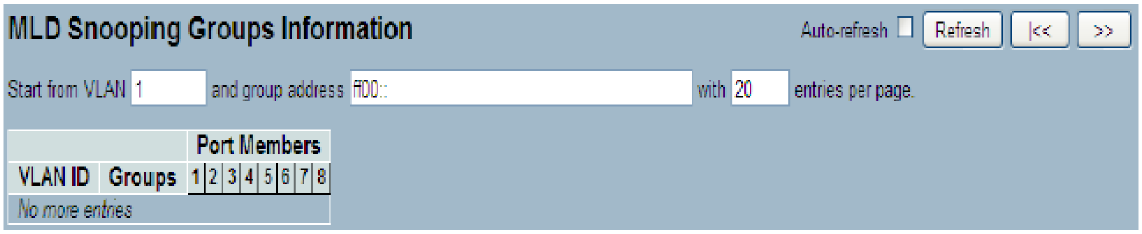
This page lets you set the MLD Snooping Groups Information. The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD Group table. Each page shows up to 99 entries from the MLD Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD Group Table.

Each page shows up to 99 entries from the MLD Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD Group Table. The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD Group Table.

To display the MLD Snooping Group information in the web UI:

1. Click Configuration, MLD Snooping, Group Information.
2. To auto-refresh the information check "Auto-refresh".
3. Click " Refresh" to refresh an entry.
4. Click " Clear" to clear the MLD Snooping Groups information.

Figure 3-6.5: 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
No more entries									

Parameter descriptions:

VLAN ID : VLAN ID of the group.

Groups : Group address of the group displayed.

Port Members : Ports under this group.

Buttons:

Auto-refresh : Click the icon then the device will refresh the page automatically.

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

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

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

3-6.6 IPv6 SSM Information

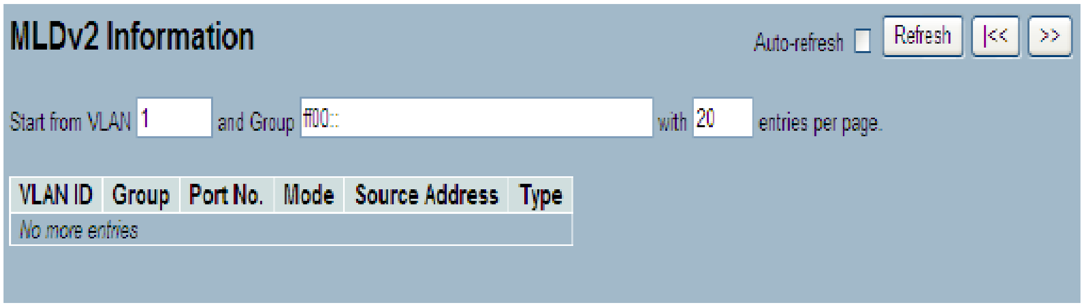
This page lets you configure the entries in the MLDv2 Information Table. The MLDv2 Information Table is sorted first by VLAN ID, then by group, and then by Port Number. Different source addresses belong to the same group are treated as single entry.

Each page shows up to 64 entries from the MLDv2 SSM (Source Specific Multicast) Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLDv2 Information Table. The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLDv2 Information Table.

To display the MLDv2 IPv6 SSM Information in the web UI:

1. Click Configuration, MLD Snooping, IPv6 SSM Information.
2. To auto-refresh the information check “Auto-refresh”.
3. Click “ Refresh“ to refresh an entry.
4. Click “<<” or “>>“ to move to previous or next entry.

Figure 3-6.6: IPv6 SSM Information



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					

Parameter descriptions:

VLAN ID : VLAN ID of the group.

Group : Group address of the group displayed.

Port : Switch port number.

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

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

Type : Indicates the Type. It can be either Allow or Deny.

Buttons:

Auto-refresh : Click the icon then the device will refresh the page automatically.

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

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

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

3-7 MVR

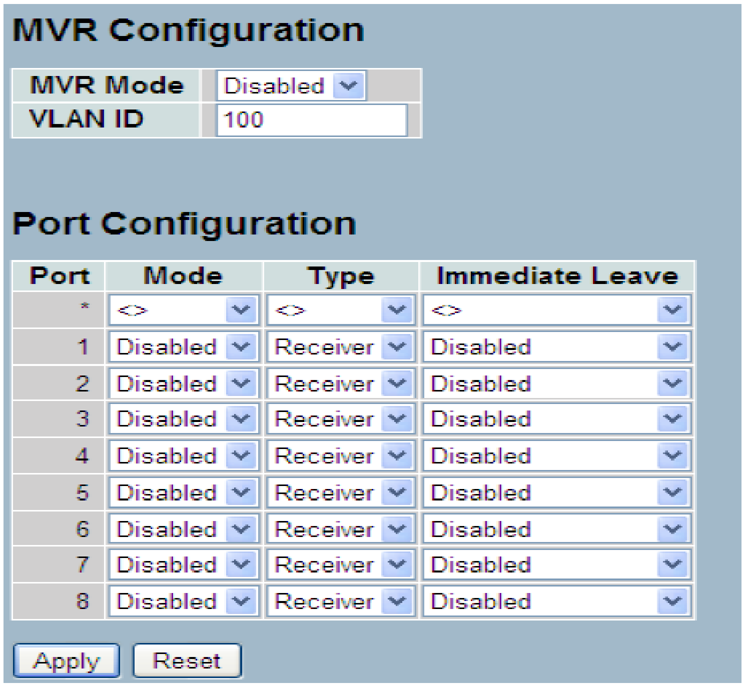
The MVR feature enables multicast traffic forwarding on the Multicast VLAN. In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR 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

This page lets you set MVR basic configuration parameters in the switch. To configure the MLD Snooping Port Group Configuration in the web UI:

1. Click Configuration, MVR, Configuration.
2. Set the MVR mode to enable or disable and set all parameters.
3. Click the Save button to save the settings
4. To cancel the settings click the Reset button to revert to previously saved values.

Figure 3-7.1: MVR Configuration



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

Parameter descriptions:

MVR Mode : Enable/Disable the Global MVR.

VLAN ID : Specify the Multicast VLAN ID.

Mode : Enable MVR on the port.

Type : Specify the MVR port type on the port.

Immediate Leave : Enable the fast leave on the port.

Buttons:

Save : Click to save changes.

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

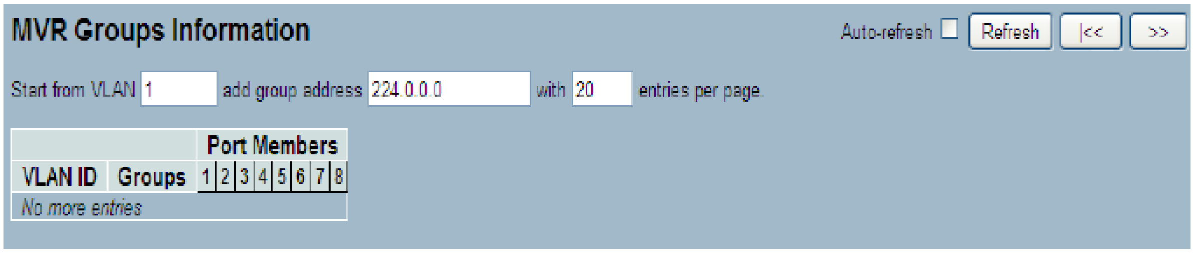
3-7.2 Groups Information

This page displays the MVR Groups detail information on the switch. Entries in the MVR Group Table are shown on this page. The MVR Group Table is sorted first by VLAN ID, and then by group

To display the MVR Groups Information in the web UI:

1. Click Configuration, MVR, Groups Information.
2. To auto-refresh the information check “Auto-refresh”.
3. Click the “ Refresh“ button to refresh the page information.
4. Click “<< “or “>>“ to move to previous or next entry.

Figure 3-7.2: MVR Groups Information



MVR Groups Information

Auto-refresh □ Refresh |<< >>

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
No more entries									

Parameter descriptions:

VLAN ID : VLAN ID of the group.

Groups : Group ID of the group displayed.

Port Members : Ports under this group.

Buttons:

Auto-refresh : Click the icon then the device will refresh the page automatically.

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

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

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

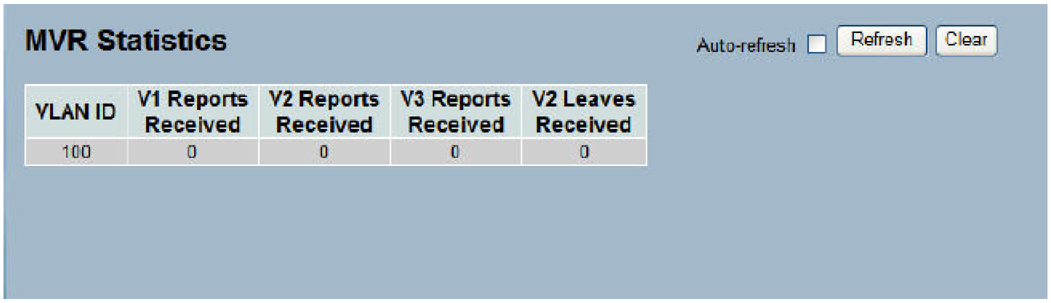
3-7.3 Statistics

This page displays the MVR detail Statistics that you have configured on the switch. It provides detailed MVR Statistics Information.

To display the MVR Statistics Information in the web UI:

1. Click Configuration, MVR, Statistics.
2. To auto-refresh the information check “Auto-refresh”.
1. Click the “Refresh“ button to refresh an entry.
3. Click “<<” or “>>“ to move to previous or next entry.

Figure 3-7.3: MVR Statistics Information



MVR Statistics

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

Parameter descriptions:

VLAN ID : The Multicast VLAN ID.

V1 Reports Received : The number of Received V1 Reports.

V2 Reports Received : The number of Received V2 Reports.

V3 Reports Received : The number of Received V3 Reports.

V2 Leaves Received : The number of Received V2 Leaves.

Buttons:

Auto-refresh : Click the icon to refresh the page automatically.

Refresh : Click to refresh the displayed statistics.

Clear: Click to clear the displayed statistics.

3-8 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. 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.

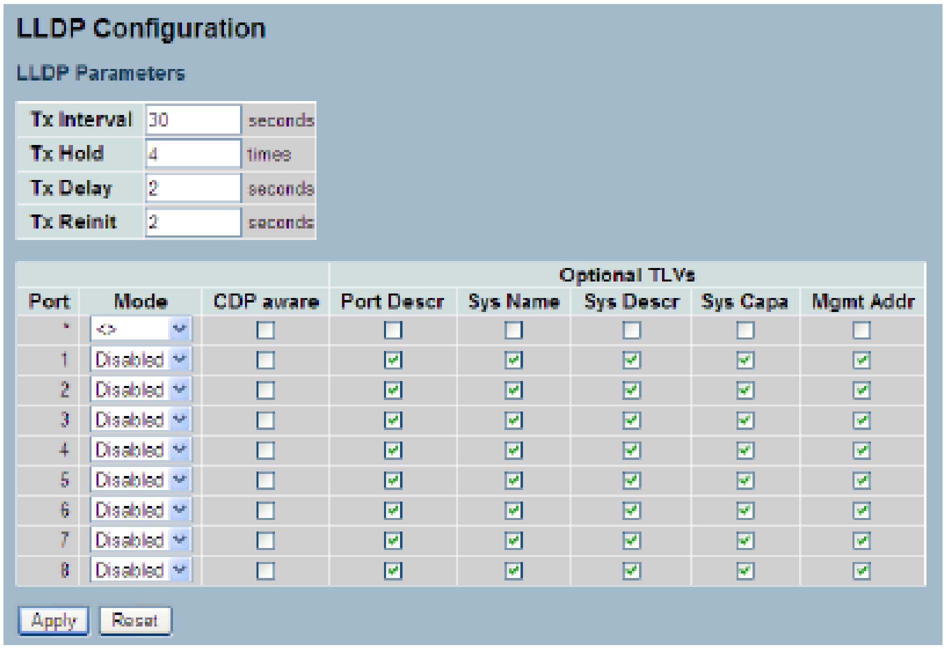
3-8.1 LLDP Configuration

You can set the LLDP configuration and detailed parameters on a per-port basis; the settings will take effect immediately. This page lets you view and configure current LLDP port settings.

To configure LLDP:

1. Click LLDP Configuration.
2. Modify 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.

Figure 3-8.1: LLDP Configuration



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	□	☑	☑	☑	☑	☑

Parameter descriptions:

LLDP Parameters

Tx Interval : The switch periodically transmits LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are 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 a 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 1 - 8192 seconds.

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

LLDP Port Configuration

Port : The switch port number of the logical LLDP port.

Mode : Select LLDP mode.

Rx only: The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.

Tx only: The switch will drop LLDP information received from neighbors, but will send out LLDP information.

Disabled : The switch will not send out LLDP information, and will drop LLDP information received from neighbors.

Enabled The switch will send out LLDP information, and will analyze LLDP information received from neighbors.

CDP Aware : Select CDP awareness. The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the port is enabled.

Only CDP TLVs that can be mapped to a corresponding field in the LLDP 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 enabled all CDP frames are terminated by the switch.

Note: When CDP awareness on a port is disabled the CDP information isn't removed immediately, but gets 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 undo any changes made locally and revert to previously saved values.

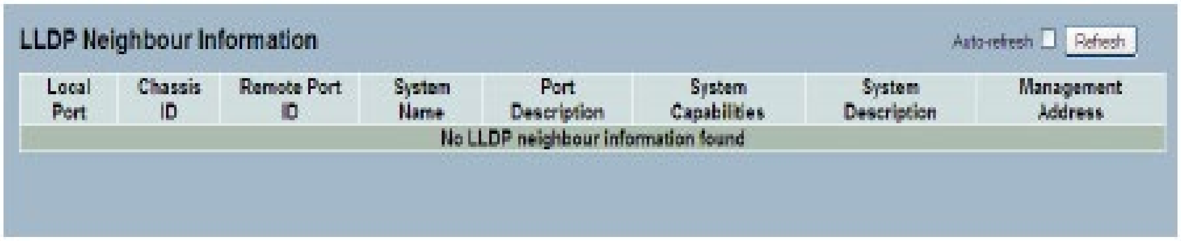
3-8.2 LLDP Neighbors

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected.

To show LLDP neighbors:

1. Click LLDP Neighbors.
2. Click Refresh for manual update web screen.
3. Click Auto-refresh for auto-update web screen.

Figure 3-8.2: LLDP Neighbors Information



LLDP Neighbour Information

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

Note: If a network with no devices supports LLDP the table shows "*No LLDP neighbor information found*".

Parameter descriptions:

Local Port : The port on which the LLDP frame was received.

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

Remote Port ID : The Remote Port ID is the identification of the neighbor port.

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

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

System Capabilities : System Capabilities describes the neighbor unit's capabilities. 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 neighbor unit.

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

Buttons:

Auto-refresh : Check the box to automatically refresh the information every 3 seconds.

Refresh : Click to refresh the displayed statistics.

3-8.3 LLDP-MED Configuration

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

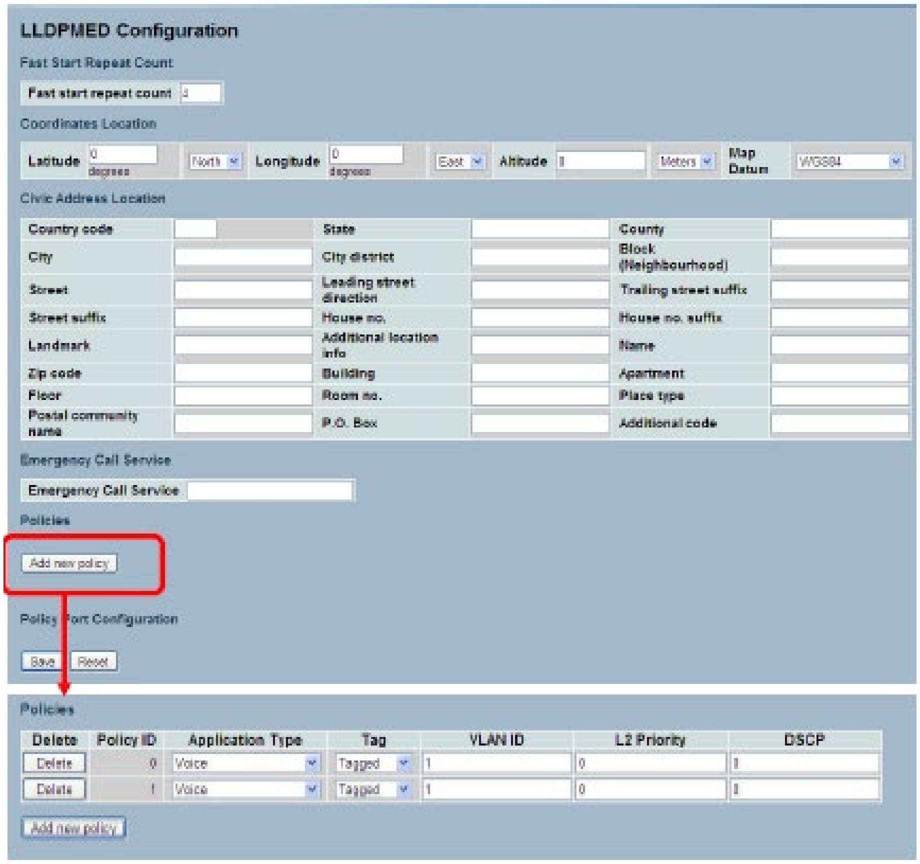
- Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority and Differentiated services (Diffserv) settings) enabling plug and play networking.
- Device location discovery to allow creation of location databases and, in the case of Voice over Internet Protocol (VoIP), Enhanced 911 services.
- Extended and automated power management of Power over Ethernet (PoE) end points.
- Inventory management, allowing network administrators to track their network devices, and determine their characteristics (manufacturer, software and hardware versions, serial or asset number).

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

To configure LLDP-MED:

1. Click LLDP-MED Configuration.
2. Modify Fast start repeat count parameter; the default is 4.
3. Modify Coordinates Location parameters.
4. Enter Civic Address Location parameters.
5. Add a new policy.
6. Click Save, will show following Policy Port Configuration.
7. Select Policy ID for each port.
8. Click Save.

Figure 3-8.3: LLDP-MED Configuration



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
Delete	1	Voice	Tagged	1	0	0

Parameter descriptions:

Fast start repeat count : Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy.

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

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

Note that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including Network Connectivity Devices, or other types of links.

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: Representing meters of Altitude defined by the vertical datum specified.

Floors: Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.

Map Datum : The Map Datum is used for the coordinates given in these options:

WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.

NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).

NAD83/MLLW: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

Civic Address Location : IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI).

Country code : The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.

State : National subdivisions (state, canton, region, province, prefecture).

County : County, parish, gun (Japan), district.

City : City, township, shi (Japan) - Example: Copenhagen.

City district : City division, borough, city district, ward, chou (Japan).

Block (Neighbourhood) : Neighbourhood, block.

Street : Street - Example: Poppelvej.

Leading street direction : Leading street direction - Example: N.

Trailing street suffix : Trailing street suffix - Example: SW.

Street suffix : Street suffix - Example: Ave, Platz.

House no. : House number - Example: 21.

House no. suffix : House number suffix - Example: A, 1/2.

Landmark : Landmark or vanity address - Example: Columbia University.

Additional location info : Additional location info - Example: South Wing.

Name : Name (residence and office occupant) - Example: Flemming Jahn.

Zip code : Postal/zip code - Example: 2791.

Building : Building (structure) - Example: Low Library.

Apartment : Unit (Apartment, suite) - Example: Apt 42.

Floor : Floor - Example: 4.

Room no. : Room number - Example: 450F.

Place type : Place type - Example: Office.

Postal community name : Postal community name - Example: Leonia.

P.O. Box : Post office box (P.O. BOX) - Example: 12345.

Additional code : Additional code - Example: 1320300003.

Emergency Call Service: Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

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

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

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

The network policy attributes advertised are:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)
2. Layer 2 priority value (IEEE 802.1D-2004)
3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

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

1. Voice
2. Guest Voice
3. Softphone Voice
4. Video Conferencing
5. Streaming Video
6. Control / Signaling (conditionally support a separate network policy for the media types above)

A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration.

It should be noted that LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

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

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

Application Type : Intended use of the application types:

1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
2. Voice Signaling (conditional) - for use in network topologies that require a different policy for the voice signaling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy.
3. Guest Voice - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.
4. Guest Voice Signaling (conditional) - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy.
5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance.
6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
8. Video Signaling (conditional) - for use in network topologies that require a separate policy for the video signaling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.

Tag : Tag indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN.

Untagged indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance.

Tagged indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.

VLAN ID : VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003.

L2 Priority : L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.

DSCP : DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 - 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. Click "Save".

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 :The port number to which the configuration applies.

Policy Id : The set of policies that shall apply to a given port. The set of policies is selected by checking the checkboxes that corresponds to the policies.

Buttons:

Save : Click to save changes.

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

3-8.4 LLDP-MED Neighbours

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

To show LLDP-MED neighbor:

1. Click LLDP-MED Neighbor.
2. Click Refresh for manual update web screen.
3. Click Auto-refresh for auto-update web screen.

Figure 3-9.4: LLDP-MED Neighbours information

LLDP-MED Neighbour Information

No LLDP-MED neighbour information found

Note: If your network without any device supports LLDPMED then the table will show "*No LLDP-MED neighbour information found*".

Parameter descriptions:

Port : The port on which the LLDP frame was received.

Device Type : LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices.

LLDP-MED Network Connectivity Device Definition: LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:

1. LAN Switch/Router
2. IEEE 802.1 Bridge
3. IEEE 802.3 Repeater (included for historical reasons)
4. IEEE 802.11 Wireless Access Point
5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method.

LLDP-MED Endpoint Device Definition : LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework. Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following.

Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).

LLDP-MED Generic Endpoint (Class I) : The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057.

Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.

LLDP-MED Media Endpoint (Class II) : The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming.

Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar.

Discovery services defined in this class include media-type-specific network layer policy discovery.

LLDP-MED Communication Endpoint (Class III) : The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.

Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management.

LLDP-MED Capabilities : LLDP-MED Capabilities describes the neighborhood unit's LLDP-MED capabilities. The possible capabilities are:

1. LLDP-MED capabilities
2. Network Policy
3. Location Identification
4. Extended Power via MDI - PSE
5. Extended Power via MDI - PD
6. Inventory
7. Reserved

Application Type : Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below.

1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
2. Voice Signaling - for use in network topologies that require a different policy for the voice signaling than for the voice media.
3. Guest Voice - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.
4. Guest Voice Signaling - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media.
5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops.
6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
8. Video Signalling - for use 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. Can be either Defined or Unknown

> ***Unknown***: The network policy for the specified application type is currently unknown.
>
> ***Defined***: The network policy is defined.

TAG : TAG is indicative of whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged or Untagged.

> ***Untagged***: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003.
>
> ***Tagged***: The device is using the IEEE 802.1Q tagged frame format.

VLAN ID : VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.

Priority : Priority is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 - 7).

DSCP : DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 - 63).

3-8.5 EEE

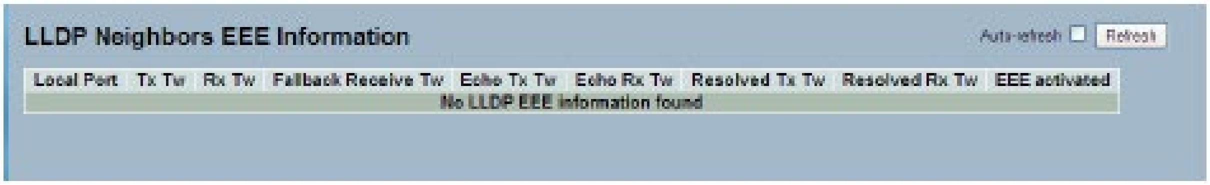
By using EEE power savings can be achieved at the expense of traffic latency. This latency occurs due to that the circuits EEE turn off to save power, need time to boot up before sending traffic over the link. This time is called "wakeup time". To achieve minimal latency, devices can use LLDP to exchange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

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

To show LLDP EEE neighbors:

1. Click LLDP, then click EEE to show discover EEE devices.
2. Click Refresh for manual update web screen.
3. Click Auto-refresh for auto-update web screen.

Figure 3-8.5: Neighbors EEE information



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								

Note: If your network without any devices which enables EEE function then the table will show “No LLDP EEE information found”.

Parameter descriptions:

Local Port : The port on which LLDP frames are received or transmitted.

Tx Tw : The link partner’s maximum time that transmit path can hold off sending data after reassertion of LPI.

Rx Tw : The link partner’s time that receiver would like the transmitter to holdoff to allow time for the receiver to wake from sleep.

Fallback Receive Tw : 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 it may use for a more efficient allocation. Systems that do not implement this option default the value to be the same as that of the Receive Tw_sys_tx.

Echo Tx Tw : The link partner's 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 : The link partner's Echo Rx Tw value.

Resolved Tx Tw : The resolved Tx Tw for this link. **Note**: NOT the link partner. The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).

Resolved Rx Tw : The resolved Rx Tw for this link. **Note**: NOT the link partner. The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).

Buttons:

Auto-refresh : Check to automatically refresh the device every 3 seconds.

Refresh : Click to manually refresh page information immediately.

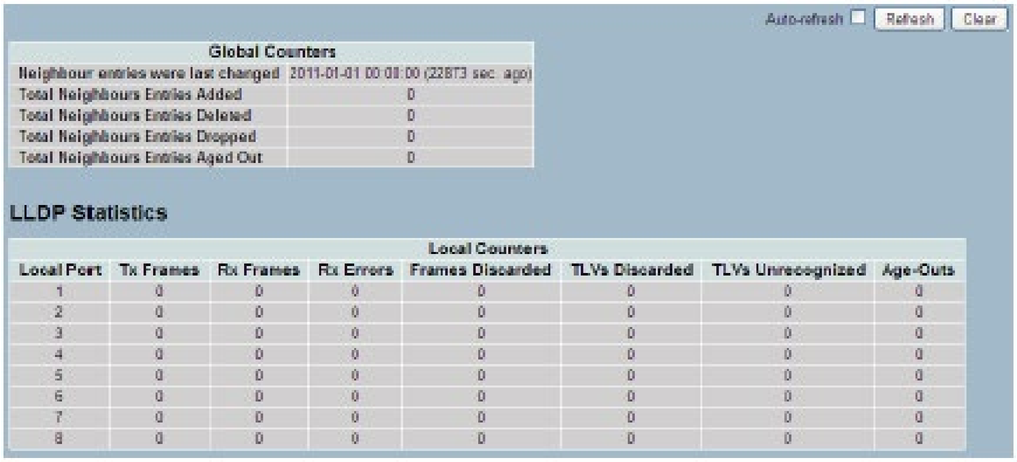
3-8.6 Port Statistics

Two types of counters are shown. Global counters are counters that refer to the whole switch, while local counters refer to per port counters for the currently selected switch

To show LLDP Statistics:

1. Click LLDP, then click Port Statistics to show LLDP counters.
2. Click Refresh for manual update web screen.
3. Click Auto-refresh for auto-update web screen.
4. Click Clear to clear all counters.

Figure 3-8.6: LLDP Port Statistics information



Global Counters	
Neighbour entries were last changed	2011-01-01 00:08:00 (22873 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

Parameter descriptions:

Global Counters

Neighbour entries were last changed at : It also shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.

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

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

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

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

Local Counters

Local Port : The port on which LLDP frames are received or transmitted.

Tx Frames : The number of LLDP frames transmitted on the port.

Rx Frames : The number of LLDP frames received on the port.

Rx Errors : The number of received LLDP frames containing some kind of error.

Frames Discarded : If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many 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 can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.

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

Org. Discarded : The number of organizationally received TLVs.

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

Buttons:

Auto-refresh : Check to automatically refresh the device every 3 seconds.

Refresh : Click to refresh the displayed statistics.

Clear : Click to clear the entries.

3- 9 Filtering Data Base

Filtering Data Base Configuration gathers many functions, including MAC Table Information, Static MAC Learning, which cannot be categorized to some function type.

MAC table: Switching of frames is based on 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 has been seen after a configurable age time

3-9.1 Configuration

The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here.

To configure MAC Address Table in the web UI:

Aging Configuration

1. Click configuration.
2. Specify the Disable Automatic Aging and Aging Time.
3. Click Save.

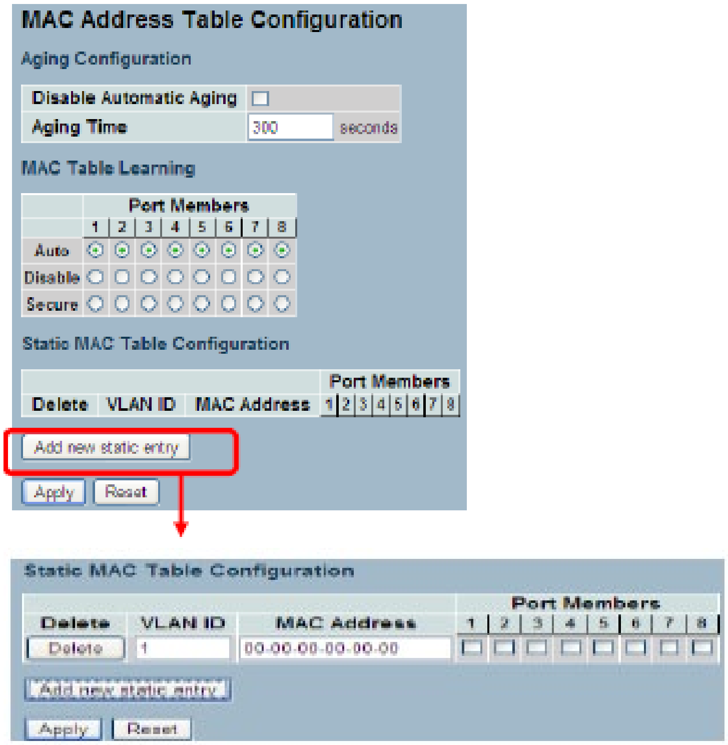
MAC Table Learning

1. Click configuration.
2. Specify the Port Members (Auto, Disable, 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.

Figure 3- 9.1: MAC Address Table Configuration



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
Auto	●	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○

Static MAC Table Configuration

			Port Members							
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8

Static MAC Table Configuration

			Port Members							
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8
Delete	1	00-00-00-00-00-00	□	□	□	□	□	□	□	□

Parameter descriptions:

Aging Configuration : By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging. Configure aging time by entering a value here 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, so that it 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 as soon as a frame with unknown SMAC is received.

Disable : No learning is done.

Secure : Only static MAC entries are learned; all other frames are dropped.

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

Static MAC Table Configuration: The static entries in the MAC table are shown in this table. The static MAC table can contain up to 64 entries. The MAC table is sorted first by VLAN ID and then by MAC address.

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

VLAN ID : The VLAN ID of the entry.

MAC Address : The MAC address of the entry.

Port Members : Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

Adding a New Static Entry : Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save".

Buttons:

Apply: Click to save changes.

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

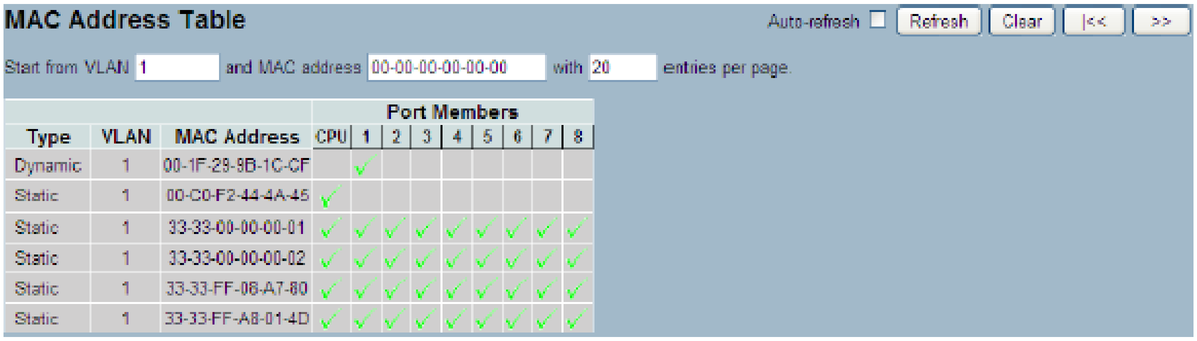
3- 9.2 Dynamic MAC Table

Entries in the MAC Table are shown on this page. The MAC Address Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

To display the MAC Address Table in the web UI:

1. Click Dynamic MAC Table .
2. Specify the VLAN and MAC Address.
3. Display MAC Address Table.

Figure 3- 9.2: Dynamic MAC Address Table information



MAC Address Table

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
Dynamic	1	00-1F-29-9B-1C-CF		✓							
Static	1	00-C0-F2-44-4A-45	✓								
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-06-A7-80	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-A8-01-4D	✓	✓	✓	✓	✓	✓	✓	✓	✓

Parameter descriptions:

Type : Indicates whether the entry is a static or a dynamic entry.

VLAN : The VLAN ID of the entry.

MAC address : The MAC address of the entry.

Port Members : The ports that are members of the entry.

Buttons:

Auto-refresh : Check Auto-refresh box then the device will refresh the log automatically.

Refresh: Click to refresh the system log page.

Clear : Click to clear the page information manually.

|<< : Go to Starting page.

<< : Go to Previous page.

>> : Go to Next page.

>>| : Go to Last page.

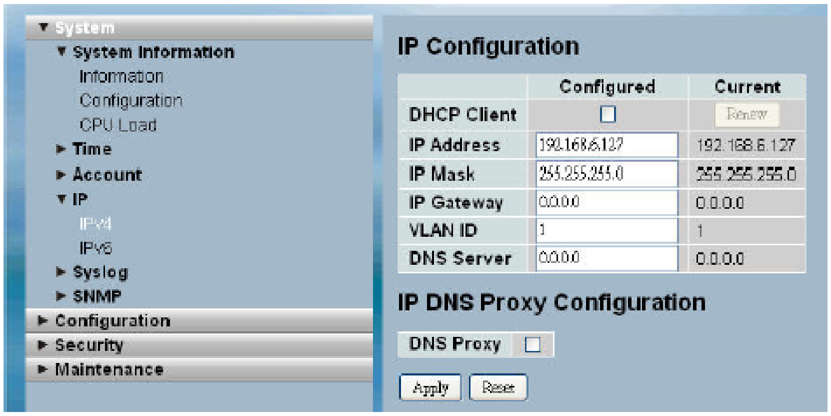
Note:

00-40-C7-73-01-29 : your 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: your switch MAC address (for IPv6 global IP).
FF-FF-FF-FF-FF-FF : for Broadcast.

3-10 VLAN

This section lets you assign a specific VLAN for management purposes. 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.

Figure 3-10.1.1: IP Configuration for management VLAN



IP Configuration

	Configured	Current
DHCP Client	□	Renew
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 □

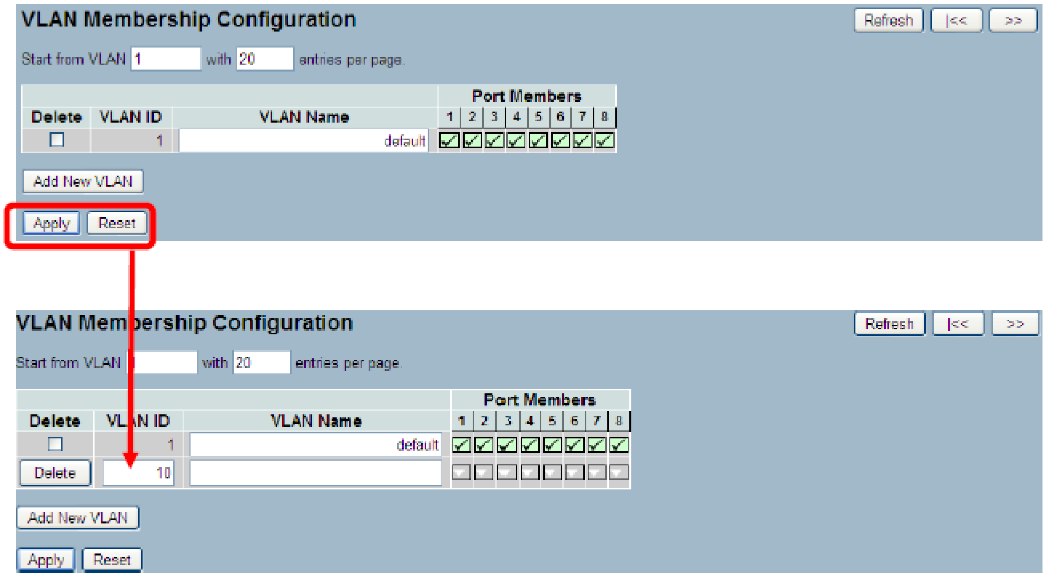
When you specify a new management VLAN, your HTTP connection to the old management VLAN is lost. For this reason, you should have a connection between your management station and a port in the new management VLAN or connect to the new management VLAN through a multi-VLAN route.

3-10.1 VLAN Membership

The VLAN membership configuration for the selected switch can be monitored and modified here. Up to 4094 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN. To configure VLAN membership in the web UI:

1. Click VLAN membership Configuration.
2. Specify Management VLAN ID from 1- 4094.
3. Click Save.

Figure 3-10.1.2: VLAN Membership Configuration



VLAN Membership Configuration

Start from VLAN 1 with 20 entries per page

Delete	VLAN ID	VLAN Name	Port Members 1	2	3	4	5	6	7	8
□	1	default	☑	☑	☑	☑	☑	☑	☑	☑

VLAN Membership Configuration

Start from VLAN with 20 entries per page

Delete	VLAN ID	VLAN Name	Port Members 1	2	3	4	5	6	7	8
□	1	default	☑	☑	☑	☑	☑	☑	☑	☑
Delete	10		□	□	□	□	□	□	□	□

Parameter descriptions:

Delete : To delete a VLAN entry, check this box and the entry will be deleted on the selected switch.
Warning: the default VLAN 1 can be deleted. But if deleting the default VLAN 1, the connection to the switch would lost and some errors would occur.

VLAN ID : Indicates the ID of every single VLAN. Legal values for a VLAN ID are 1 to 4094.

VLAN Name : Indicates the name of VLAN. VLAN Name can contain alphabets, numbers, and mix of alphabets and numbers, but exclude special characters. VLAN Name can leave blanks. The length of VLAN name supports up to 32 characters. VLAN name can be edited for the existing VLAN entries.

Port Members : A row of check boxes for each port display port members of each VLAN. To include a port in a VLAN, tick the box. To remove or exclude the port from the VLAN, make sure the box is unchecked.

Adding a New VLAN : Click to add a new VLAN group. An empty row, no port is member and all boxes are unchecked, is added to the table to configure. A VLAN without any port members cannot be set up.

Buttons:

Apply : Click to save changes.

Reset : Click to undo any change which is made before pressing Apply button. Go back to the previous group configuration.

Refresh: Click to refresh the system log page.

Clear : Click to clear the page information manually.

|<< : Go to Starting page.

<< : Go to Previous page.

>> : Go to Next page.

>>| : Go to Last page.

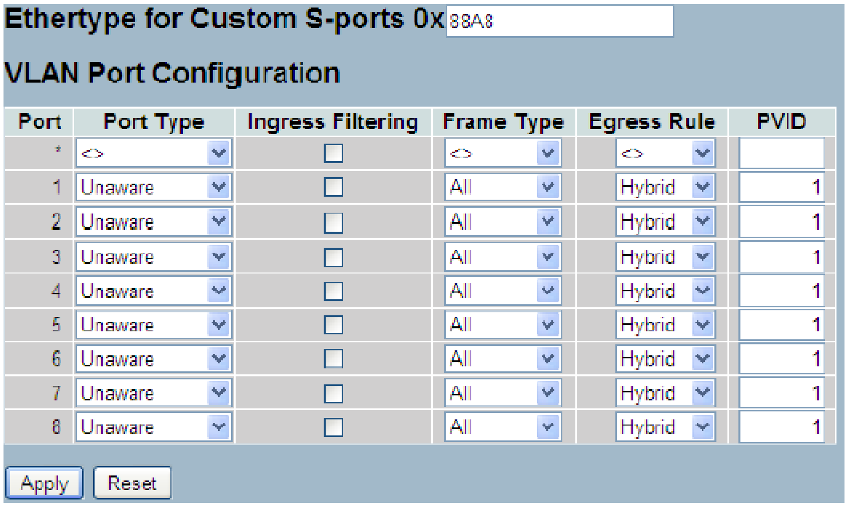
3-10.2 Ports

You can configure all parameters on each port in VLAN Port Setting. These parameters involved two parts: Ingress rule and Egress rule. The function of Port Type, Ingress Filtering, Frame Type, and PVID affect Ingress process. Furthermore, Port Type, Egress Rule, and PVID affect Egress process.

To configure VLAN Port configuration in the web UI:

1. Click VLAN Port Configuration.
2. Specify the VLAN Port Configuration parameters.
3. Click Save.

Figure 3-10.2: VLAN Port Configuration



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

Parameter descriptions:

Ethertype for Custom S-ports : This field specifies the ether type used for Custom S-ports while s-custom-port enabled. This is a global setting for all the Custom S-ports. Custom Ethertype lets you 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 802.1ptagged frames.

Port : Indicate the port number of each port.

Port Type : Port can be one of the following types: Unaware, C-port, S-port, and S-custom-port.

Port Type	Ingress action	Egress action
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 receives tagged frames: 1. if the tagged frame with 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 receives untagged frames, an untagged frame obtain a tag (based on PVID) and is forwarded. When the port receives tagged frames: 1. if a tagged frame with 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 receives tagged frames: 1. if a tagged frame with 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 receives tagged frames: 1. if a tagged frame with 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 an s-custom-port will be set to a self-customized value, which can be set by using the column of Ethertype for Custom S-ports.

Ingress Filtering :

Enable ingress filtering on a port by ticking the box. 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 (Do not forward). If ingress filtering is disabled and the ingress port is not a member of the classified VLAN group of the frame, however, the frame is still forwarded. By default, ingress filtering is disabled (untick).

Frame Type : 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 : Determines what device the port connect to. If the port connect to VLAN-unaware devices, such as terminal/work station, Access link should be used. If the port connect to VLAN aware devices, for example, 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 : Configures the Port VLAN identifier. The allowed values are 1 - 4094. The default value is 1. When the port received a untagged frame, the port will give a tag to it based on the value of PVID, and the frame become tagged frame.

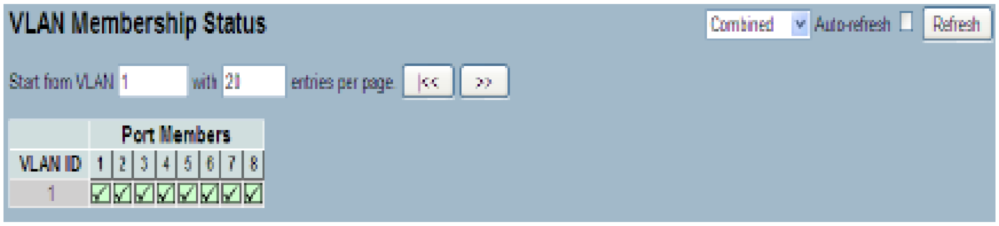
Note: The port must be a member of the same VLAN as the Port VLAN ID.

3-10.3 Switch Status

The Switch Status function gathers the information of all VLAN status and reports it by the order of Static, NAS, MVRP, MVP, Voice, VLAN, MSTP, GVRP, Combined. To display VLAN membership status in the web UI:

1. Click VLAN Membership.
2. Select the VLAN user type.
3. Select the Start from VLAN and entries per page.
4. View the VLAN membership information.

Figure 3-10.3: VLAN Membership Status



VLAN Membership Status

Combined ▾ Auto-refresh □ Refresh

Start from VLAN 1 with 20 entries per page. |<< >>

	Port Members							
VLAN ID	1	2	3	4	5	6	7	8
1	☑	☑	☑	☑	☑	☑	☑	☑

Parameter descriptions:

VLAN User select box: At the dropdown select one of the VLAN user types listed below. The VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configurations such as PVID and UVID. The following VLAN user types are currently supported:

Web/SNMP : These are referred to as static.

NAS : NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

MVRP : Multiple VLAN Registration Protocol (MVRP) allows dynamic registration and deregistration of VLANs on ports on a VLAN bridged network.

GVRP : GARP VLAN Registration Protocol (GVRP) allows dynamic registration and deregistration of VLANs on ports on a VLAN bridged network.

Voice VLAN : Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones.

MVR : MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.

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 : Indicates the ID of this particular VLAN.

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

Buttons:

|<< : Go to Starting page.

<< : Go to Previous page.

>> : Go to Next page.

>>| : Go to Last page.

Auto-refresh : Check the box to automatically refresh the information every 3 seconds.

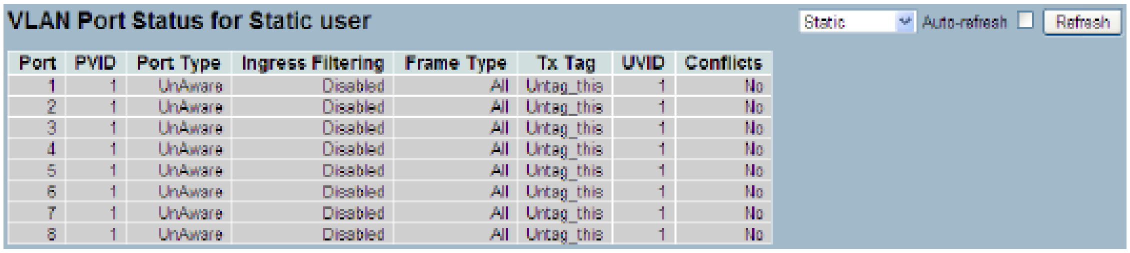
Refresh : Click to manually refresh the webpage immediately.

3-10.4 Port Status

The function Port Status gathers the information of all VLAN status and reports it in the order of Static, NAS, MVRP, MVP, Voice VLAN, MSTP, GVRP, Combined. To display VLAN Port Status in the web UI:

1. Click VLAN Port Status.
2. Specify the Static NAS MVRP MVP Voice VLAN MSTP GVRP, Combined.
3. Display Port Status information.

Figure 3-10.4: VLAN Port Status for Static user:



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

Parameter descriptions:

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

PVID : Shows the VLAN identifier for that port. Valid values are 1 - 4095. The default value is 1.

Port Type : Shows the Port Type. Port type can be any of Unaware, C-port, S-port, 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 : 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 : 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 : Shows egress filtering frame status whether tagged or untagged.

UVID : Shows UVID (untagged VLAN ID). A port's UVID determines the packet's behavior at the egress side.

Conflicts : Shows status of Conflicts whether exists or not. When a Volatile VLAN User requests to set VLAN membership or VLAN port configuration, the following conflicts can occur:

- Functional Conflicts between features.
- Conflicts due to hardware limitation.
- Direct conflict between user modules.

Buttons:

Auto-refresh : Check the box to automatically refresh the information every 3 seconds.

Refresh : Click to manually refresh the webpage immediately.

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

The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here. Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

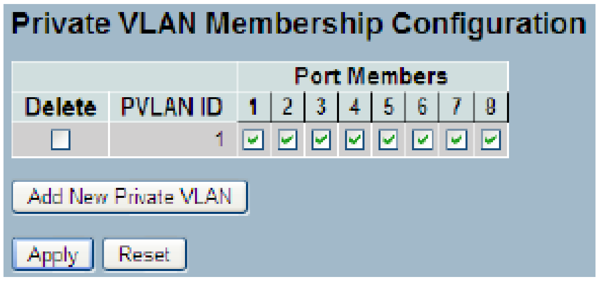
A port must be a member of both a VLAN and a Private VLAN to be able to forward packets.

By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1. A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

To configure a Private VLAN in the web UI:

1. Click add new Private VLAN configuration.
2. Specify the Private VLAN ID and Port Members.
3. Click Save.

Figure 3-10.5.1: Private VLAN Membership Configuration



Private VLAN Membership Configuration

		Port Members							
Delete	PVLAN ID	1	2	3	4	5	6	7	8
☐	1	☑	☑	☑	☑	☑	☑	☑	☑

Parameter descriptions:

Delete : Check this box to delete a private VLAN entry. The entry will be deleted during the next save.

Private VLAN ID : Indicates the ID of this particular private VLAN.

Port Members : A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Adding a New Private VLAN : Click to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed.

Buttons:

Save : Click to save changes.

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

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 generates 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.

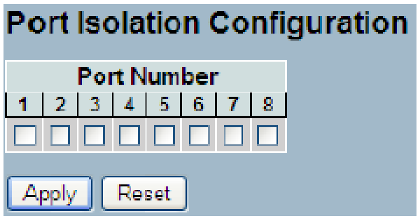
A destination address on a data packet is matched with a physical address on said layer 2 switch and a forwarding map is generated for the data packet based upon the destination address on the data packet. The data packet is then sent to the plurality of ports pursuant to the forwarding map generated based upon whether the ingress port was configured as a protected or non-protected port.

This page is used for enabling or disabling port isolation on ports in a Private VLAN.A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.

To configure Port Isolation configuration in the web UI:

1. Click VLAN, Port Isolation.
2. Evoke which port want to enable Port Isolation
3. Click Save.

Figure 3-10.5.2: Port Isolation Configuration



Port Isolation Configuration

Port Number							
1	2	3	4	5	6	7	8
□	□	□	□	□	□	□	□

Parameter descriptions:

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

Buttons:

Save – Click to save changes.

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

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. On the other hand, 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, which brings security issues. To provide user access and ensure data security in the meantime, 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, flexible network access for terminal devices.

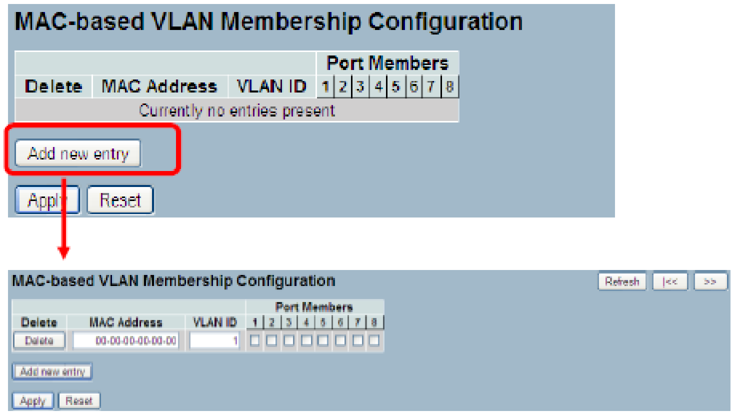
3-10.6.1 Configuration

The MAC-based VLAN entries can be configured here. This page allows for adding and deleting MAC-based VLAN entries and assigning the entries to different ports. This page shows only static entries.

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.

Figure 3-10.6.1: MAC-based VLAN Membership Configuration



MAC-based VLAN Membership Configuration

			Port Members							
Delete	MAC Address	VLAN ID	1	2	3	4	5	6	7	8
Currently no entries present										

MAC-based VLAN Membership Configuration

			Port Members							
Delete	MAC Address	VLAN ID	1	2	3	4	5	6	7	8
Delete	00-00-00-00-00-00	1	□	□	□	□	□	□	□	□

Parameter descriptions:

Delete : To delete a MAC-based VLAN entry, check this box and press save. The entry will be deleted on the selected switch.

MAC Address : Indicates the MAC address.

VLAN ID : Indicates the VLAN ID.

Port Members : A row of check boxes for each port is displayed for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, check the box. To remove or exclude the port from the MAC-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Adding a New MAC-based VLAN : Click to add a new MAC-based VLAN entry. An empty row is added to the table, and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 through 4095.

The MAC-based VLAN entry is enabled 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 "Save".

Buttons:

Save : Click to save changes.

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

3-10.6.2 Status

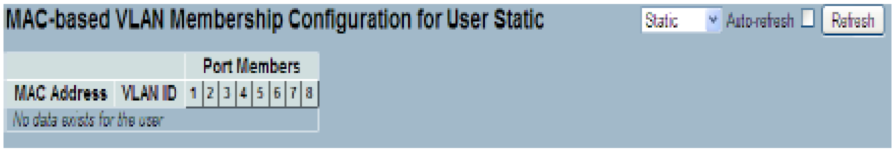
This section shows MAC-based VLAN entries configured by various MAC-based VLAN users. The following VLAN User types are currently supported:

NAS : NAS provides port-based authentication, which involves communications between a Supplicant, an Authenticator, and an Authentication Server.

To Display MAC-based VLAN configured in the web UI:

1. Click MAC-based VLAN Status.
2. Specify the User type.
3. Display MAC-based information.

Figure 3-10.6.2: MAC-based VLAN Membership Status for User Static



MAC-based VLAN Membership Configuration for User Static

Static ▾ Auto-refresh □ Refresh

		Port Members							
MAC Address	VLAN ID	1	2	3	4	5	6	7	8
No data exists for the user									

Parameter descriptions:

MAC Address : Indicates the MAC address.

VLAN ID : Indicates the VLAN ID.

Port Members : Port members of the MAC-based VLAN entry.

Buttons:

Auto-refresh : To evoke the auto-refresh icon then the device will refresh the information automatically.

Refresh: Check the box to immediately refresh page information manually.

3-10.7 Protocol -based VLAN

This section lets you set Protocol -based VLAN functions. Switch protocol supports includes Ethernet, LLC, SNAP, and LLC.

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, and can also provide flow control and automatic repeat request (ARQ) error management mechanisms.

SNAP: The Sub network 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 spaces. It is used with IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.11 and other IEEE 802 physical network layers, as well as with non-IEEE 802 physical network layers such as FDDI that use 802.2 LLC.

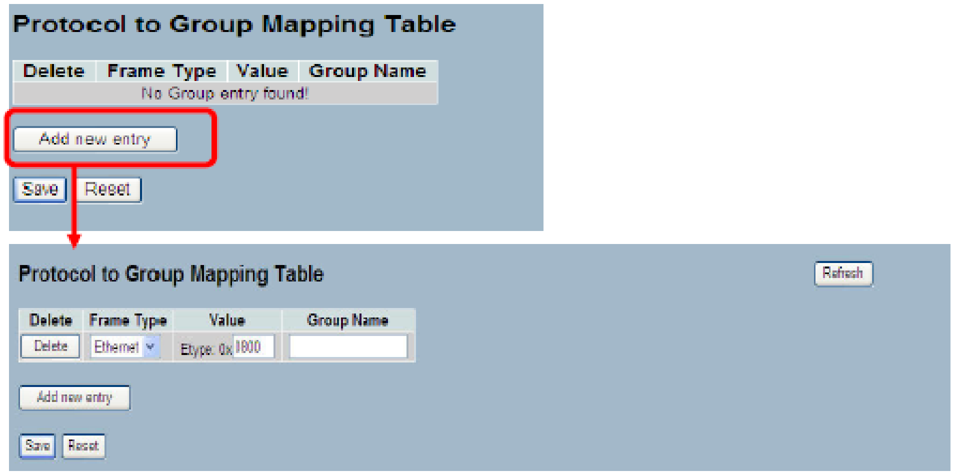
3-10.7.1 Protocol to Group

This page allows you to add new protocols to Group Name (unique for each Group) mapping entries as well as allow you to see and delete already mapped entries for the selected switch.

To configure Protocol -based VLAN in the web UI:

1. Click Protocol -based VLAN configuration and add new entry.
2. Specify the Ethernet LLC SNAP Protocol and Group Name.
3. Click Save.

Figure 3-10.7.1: Protocol to Group Mapping Table



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 1800	

Parameter descriptions:

Delete : To delete a Protocol to Group Name map entry, check this box. The entry will be deleted on the switch during the next Save.

Frame Type : Frame Type can have one of the following values:

1. Ethernet
2. LLC
3. SNAP

Note: On changing the Frame type field, valid value of the following text field will vary depending on the new frame type you selected.

Value : Valid value that can be entered in this text field depends on the option selected from the the preceding Frame Type selection menu. Below is the Value criteria for three different Frame Types:

1. **For Etherne**t: Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff.
2. **For LLC**: Valid value in this case is comprised of two different sub-values.
    a. **DSAP**: 1-byte long string (0x00-0xff)
    b. **SSAP**: 1-byte long string (0x00-0xff)
3. **For SNAP**: Valid value in this case also is comprised of two different sub-values.
    a. ***OUI***: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff.
    b. ***PID***: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.

Group Name : A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers(0-9). **Note**: Special characters and underscore (_) are not allowed.

Adding a New Group to VLAN mapping entry : Click the Add new entry button to add a new entry in mapping table. An empty row is added to the table; Frame Type, Value and the Group Name can be configured as needed.

Buttons:

Save – Click to save changes.

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

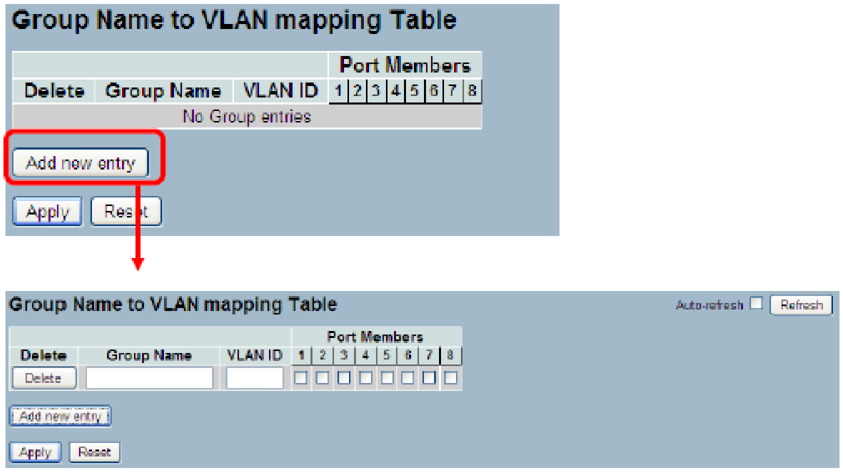
Refresh : Click to refresh the webpage information manually.

3-10.7.2 Group to VLAN

This section allows you to map a already configured Group Name to a VLAN for the selected switch. To display Group Name to VLAN mapping table configured in the web UI:

1. Click Group Name VLAN configuration and add new entry.
2. Specify the Group Name and VLAN ID.
3. Click Save.

Figure 3-12.7.2: Group Name to VLAN Mapping Table



Group Name to VLAN mapping Table

			Port Members							
Delete	Group Name	VLAN ID	1	2	3	4	5	6	7	8
No Group entries										

Add new entry

Apply Reset

Group Name to VLAN mapping Table Auto-refresh □ Refresh

			Port Members							
Delete	Group Name	VLAN ID	1	2	3	4	5	6	7	8
Delete			□	□	□	□	□	□	□	□

Add new entry

Apply Reset

Parameter descriptions:

Delete : To delete a Group Name to VLAN map entry, check this box. The entry will be deleted on the switch during the next Save

Group Name : A valid Group Name is a string of at most 16 characters which consists of a combination of alphabets (a-z or A-Z) and integers(0-9), no special character is allowed. Whichever Group name you try map to a VLAN must be present in Protocol to Group mapping table and must not be reused by any other existing mapping entry on this page.

VLAN ID : Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1- 4095.

Port Members : A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Adding a New Group to VLAN mapping entry : Click 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. Valid values for a VLAN ID are 1 through 4095. The button can be used to undo the addition of new entry.

Buttons:

Save : Click to save changes.

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

Auto-refresh : To evoke the auto-refresh icon then the device will refresh the information automatically.

Refresh : Click to refresh the Protocol Group Mapping information manually.

3-10.8 IEEE 802.1QinQ (double-tag) configuration

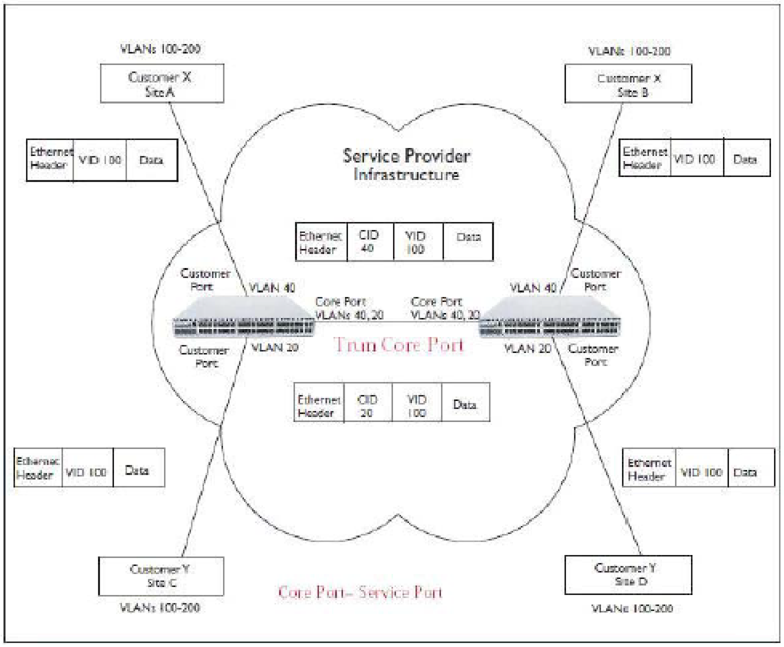
Service providers can use Q-in-Q to transparently pass Layer 2 VLAN traffic from a customer site, through the service provider network, to another customer site without removing or changing the customer VLAN tags.

The double Q-in-Q tags can indicate different information, the inner tag indicates the user, 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.

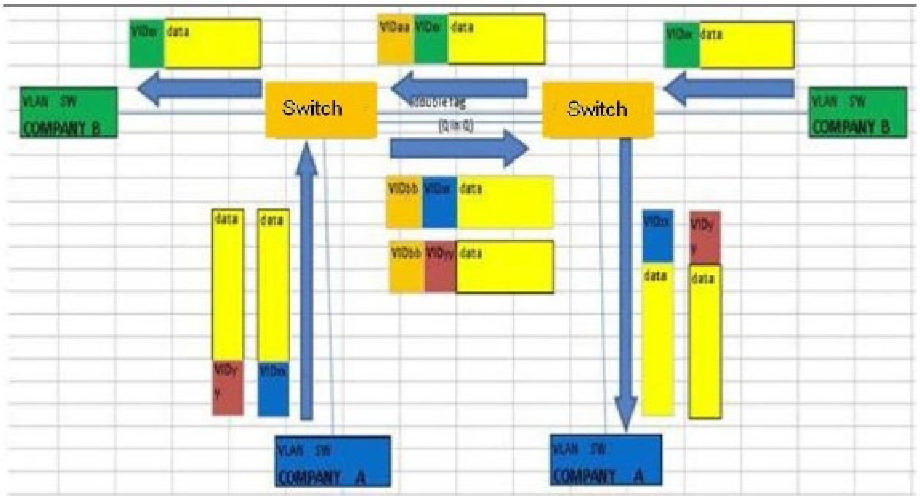
Scenario :

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 the existing VLAN.

Typical Application:



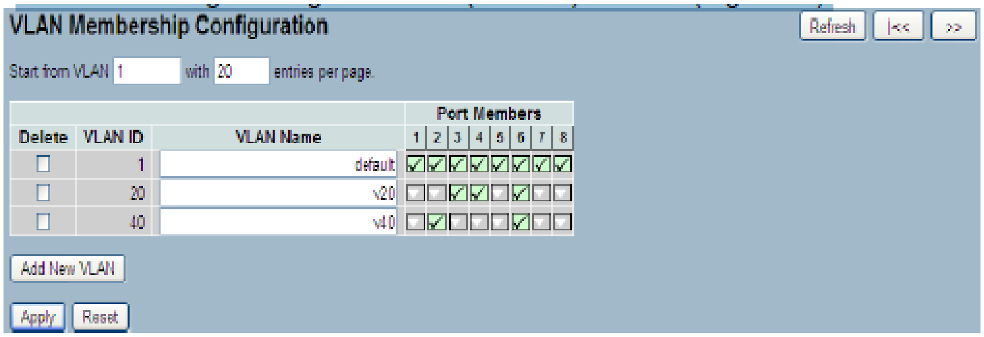
An abstract illustration to above application:



Configure Steps:

1. Create VLAN 20 and VLAN 40:
   a. Configure Port 3. Port 4 and Port 6 belong to VLAN 20.
   b. Configure Port 2 and Port 6 belong to VLAN 40.
   c. Port 6 is uplink port.

   The above setting is configured at SW1 (Left side) and SW2 (Right side).



Start from VLAN 1 with 20 entries per page.

			Port Members							
Delete	VLAN ID	VLAN Name	1	2	3	4	5	6	7	8
□	1	default	☑	☑	☑	☑	☑	☑	☑	☑
□	20	v20	□	□	☑	☑	□	☑	□	□
□	40	v40	□	☑	□	□	□	☑	□	□

2. Configure PVID:
   a. Port2 is PVID=40 and its port role is VLAN Access mode.
   b. Port3 and Port4 are PVID=20 and their port role are VLAN Access mode.
   c. The port role of Port 6 is VLAN Trunk mode.
3. Configure Port Type to “Unaware“ at Port1 ~ Port 4.
4. Configure Port Type to “S-Port“ at Port 6.

The uplink port, port 8, can be set as C-Port or S-Port. The uplink port on both switches must be set to the same Type. Set S-Port to S-Port in the example.

Q in Q belongs to the Tag-based mode; however, it would treat all frames as untagged, which means that tag with PVID will be added into all packets. These packets will then be forwarded as Tag-based VLAN, so the incoming packets with tags will become double tagged.

3-11 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.

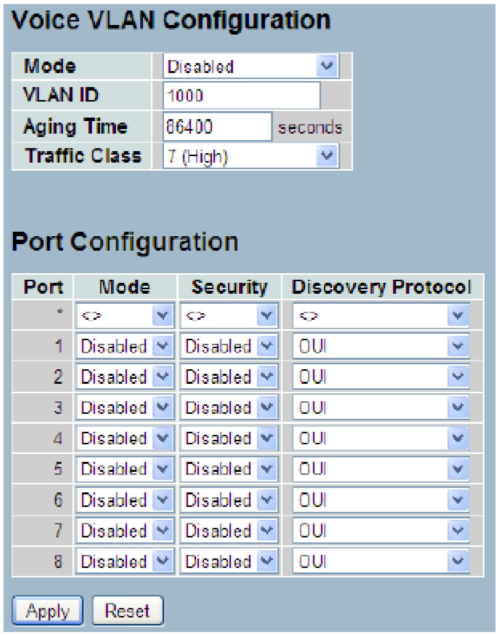
3-11.1 Configuration

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, 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.

To configure Voice VLAN in the web UI:

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
4. Click Save.

Figure 3-11.1: Voice VLAN Configuration



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

Parameter descriptions:

Mode : Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are:

Enabled: Enable Voice VLAN mode operation.

Disabled: Disable Voice VLAN mode operation.

VLAN ID : 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 : 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 : Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.

Port Mode : Indicates the Voice VLAN port mode. When the port mode isn't equal disabled, you must disable MSTP feature before you enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible port modes are:

Disabled: Disjoin from Voice VLAN.

Auto: Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically.

Forced: Force join to Voice VLAN.

Port Security : Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds. Possible port modes are:

Enabled: Enable Voice VLAN security mode operation.

Disabled: Disable Voice VLAN security mode operation.

Port Discovery Protocol :Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart auto detect process. Possible discovery protocols are:

OUI: Detect telephony device by OUI address.

LLDP: Detect telephony device by LLDP.

Both: Both OUI and LLDP.

Buttons:

Save : Click to save changes.

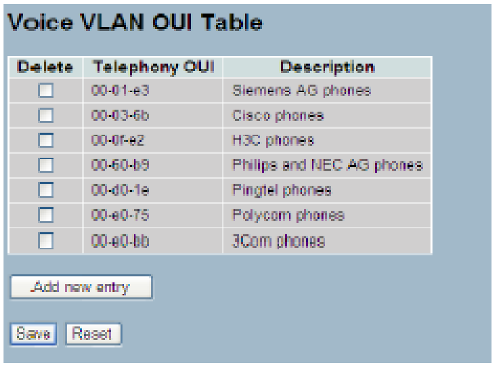
Reset : Click to undo any changes made locally and revert to previously saved values.

3-11.2 OUI

The section describes how to Configure VOICE VLAN OUI table . The maximum entry number is 16. Modifying the OUI table will restart auto detection of OUI process. To configure Voice VLAN OUI Table in the web interface:

1. Select “Add new entry”, “Delete” in the Voice VLAN OUI table.
2. Specify Telephony OUI, Description.
3. Click Save.

Figure 3-11.2: Voice VLAN OUI Table



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

Parameter descriptions:

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

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 : The description of OUI address. Normally, 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. An empty row is added to the table, the Telephony OUI, Description.

Buttons:

Save : Click to save changes.

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

Note: All non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds. For example: when Packets keep to enter the port, to add a new OUI entry, it can help this OUI match current packets, then it must be 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, e.g. end stations and switches, can register and de-register attribute values, such as VLAN Identifiers, with each other. 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.

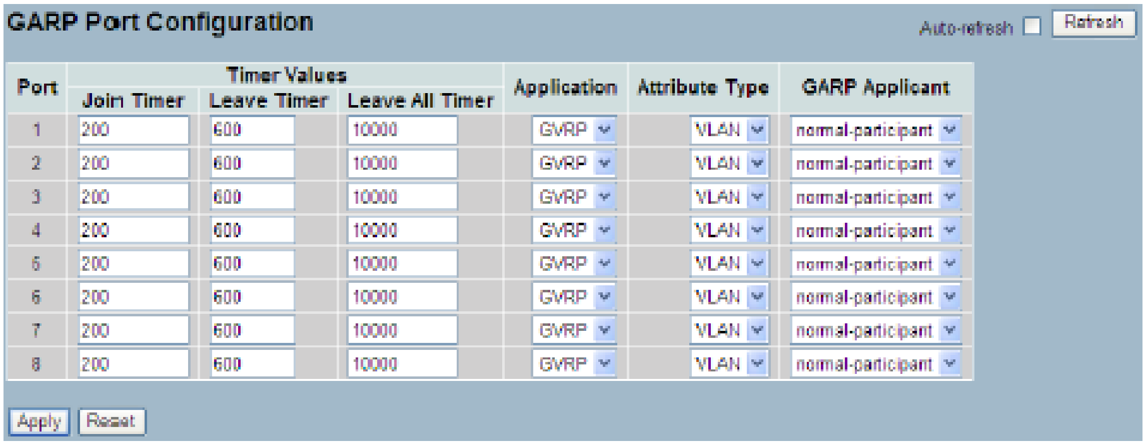
3-12.1 Configuration

This page allows you to configure the basic GARP Configuration settings for all switch ports. The settings relate to the currently selected unit, as reflected by the page header.

To configure GARP Port settings in the web UI:

1. Click GARP configure.
2. Specify GARP Configuration Parameters..
3. Click Save.

Figure 3-12.1: GARP Port Configuration



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

Parameter descriptions:

Port : The Port column shows the list of ports for which you can configure GARP settings. There are 2 types of configuration settings which can be configured on a per port bases.

Timer Values

- Application
- Attribute Type
- GARP Applicant

Timer Values : To set the GARP join timer, leave timer and .leave all timers, units is microseconds. 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 600-1000ms. The default value for Leave Timer is 600ms.

Leave All Timer : The default value for Leave All Timer is 10000ms

Application : Currently only supported application is GVRP.

Attribute Type : Currently only supported Attribute Type is VLAN.

GARP Applicant : This configuration is used to configure the Applicant state machine behavior for GARP on a particular port locally.

- ***normal-participant***: In this mode the Applicant state machine will operate normally in GARP protocol exchanges. The default configuration is normal participant.
- ***non-participant***: In this mode the Applicant state machine will not participate in the protocol operation.

Buttons:

Apply : Click to save changes.

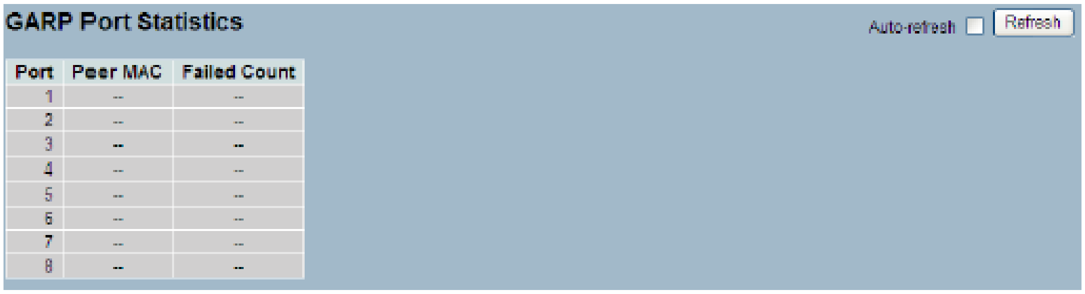
Reset : Click to undo any changes made locally and revert to previously saved values.

3-12.2 Statistics

This page shows GARP port statistics for all switch ports. To display GARP Port statistics in the web UI:

1. Click GARP statistics.
2. View the GARP Counter information.
3. Click Refresh to modify the GARP statistics information.

Figure 3-12.2: GARP Port Statistics



GARP Port Statistics

Port	Peer MAC	Failed Count
1	--	--
2	--	--
3	--	--
4	--	--
5	--	--
6	--	--
7	--	--
8	--	--

Parameter descriptions:

Port : The Port column shows the list of all ports for which per port GARP statistics are shown.

Peer MAC : Peer MAC is MAC address of the neighbor Switch from with GARP frame is received.

Failed Count : explain Failed count here.

Buttons

Auto-refresh : Click to auto-refresh the page automatically.

Refresh: Click to manually refresh the GARP Port Statistics information immediately.

3-13 GVRP

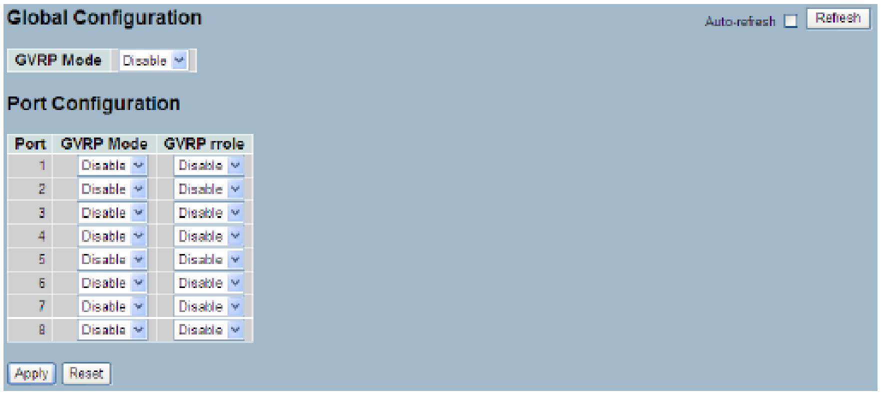
GVRP is an application based on Generic Attribute Registration Protocol (GARP), mainly used to automatically and dynamically maintain the group membership information of the VLANs. The GVRP offers the function providing the VLAN registration service through a GARP application. It makes use of GARP Information 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, 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 page allows you to configure the basic GVRP Configuration settings for all switch ports. To configure GVRP Port Configuration in the web UI:

1. Click GVRP configure.
2. Specify GVRP Configuration Parameters..
3. Click Save.

Figure 3-13.1: GVRP Global Configuration



Global Configuration

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

Parameter descriptions:

GVRP Mode : GVRP Mode is a global setting, to enable the GVRP globally select 'Enable' from menu and to disable GVRP globally select 'Disable'.

Port : The Port column shows the list of ports for which you can configure per port GVRP settings. The configuration settings which can be configured on per port basis are GVRP Mode and GVRP Role.

1. **GVRP Mode**: This configuration is to enable/disable GVRP Mode on particular port locally.

   Disable: Select to Disable GVRP mode on this port (default).

   Enable: Select to Enable GVRP mode on this port.

2. **GVRP role** : This configuration is used to configure restricted role on an interface.

   Disable: Select to Disable GVRP rrole on this port (default).

   Enable: Select to Enable GVRP rrole on this port.

Buttons:

Auto-refresh : Click to refresh the page information automatically.

Refresh : Click to immediately refresh page information manually.

Apply : Click to save changes.

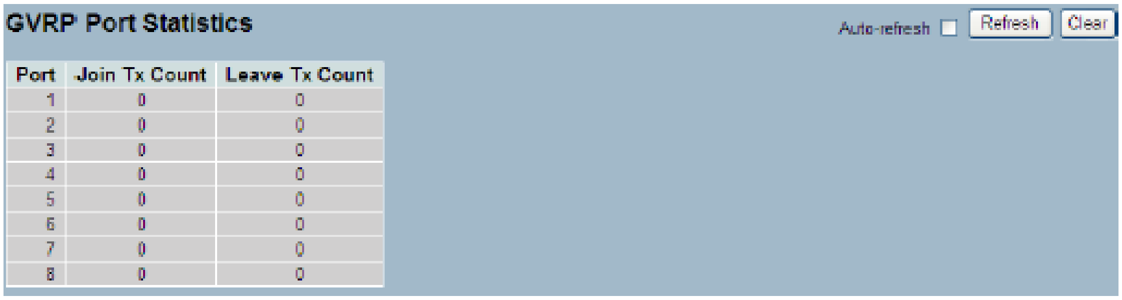
Reset : Click to undo any changes made locally and revert to previously saved values.

3-13.2 Statistics

The section describes how to shows the basic GVRP Port statistics for all switch ports. To display GVRP Port statistics in the web UI:

1. Click GVRP statistics.
2. Scroll which port you want to display the GVRP Counter information..
3. Click Refresh to modify the GVRP statistics information.

Figure 3-13.2: GVRP Port Statistics



GVRP Port Statistics

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

Parameter descriptions:

Port : The Port column shows the list of ports for which you can see port counters and statistics.

Join Tx Count : Displays the number of GVRP Join event packets received on the port.

Leave Tx Count : Displays the number of GVRP Leave packets received on the port.

Buttons:

Auto-refresh : Click to auto-refresh the information automatically every 3 seconds.

Refresh : Click to immediately refresh the GVRP Port Statistics information manually.

Clear : Click to reset the counters.

3-14 QoS

The switch supports 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.

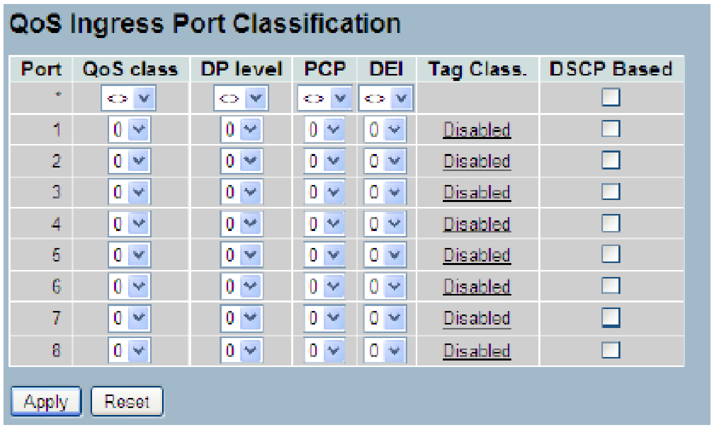
The switch support advanced memory control mechanisms providing excellent performance of all QoS classes under any traffic scenario, including jumbo frame. A super priority queue with dedicated memory and strict highest priority is in the arbitration. The ingress super priority queue allows traffic recognized 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

This page lets you configure the basic QoS Ingress Classification settings for all switch ports. To configure the QoS Port Classification parameters in the web UI:

1. Click Configuration, QoS, Port Classification.
2. Select QoS class, DP Level, PCP and DEI parameters.
3. Click the Apply button to save the setting.
4. To cancel the settings click the Reset button to revert to previously saved values.

Figure 3-14.1: QoS Configuration



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	□

Parameter descriptions:

Port : The port number for which the configuration below applies.

QoS class : Controls the default QoS class, i.e., 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 0 (zero) has the lowest priority.

DP level : Controls the default DP level, i.e., the DP level for frames not classified in any other way.

PCP : Control the default PCP for untagged frames.

DEI : Control the default DEI for untagged frames.

Tag Class. : Show 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 linked mode in order to configure the mode and/or mapping.

DSCP Based : Click to Enable DSCP Based QoS Ingress Port Classification.

Buttons:

Apply : Click to save changes.

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

Note: DP level : Every incoming frame is classified to a Drop Precedence Level (DP level), which is used throughout the device for providing congestion control guarantees to the frame according to what was configured for that specific DP level.

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 Pri column in Vlan tag packet, DEI is cfi column

PCP values from 0~7 can be used for priority definition .

DEI value is 0 or 1: it is settable, map to DP value is 0 or 1. When ingress Qos class value is the same, then DP level value is used to define the priority and larger DP values will be dropped first.

Example: From Port 1 input 1G Pkts , Egress Port 7 Rate be set with 500M . Port 1 Packets will includes two kinds of 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) Packet all past, and (b) packets all drop.

3-14.2 Port Policing

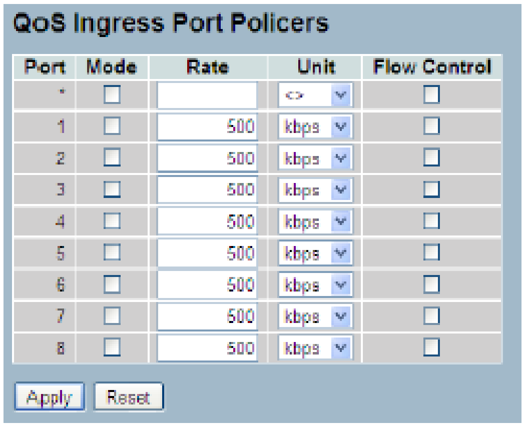
This section provides an overview of f QoS Ingress Port Policers for all switch ports The Port Policing is useful in constraining traffic flows and marking frames above specific rates.

Policing is primarily useful for data flows and voice or video flows because voice and video usually maintains a steady rate of traffic.

To display the QoS Port Schedulers in the web UI:

1. Click Configuration, QoS, Port Policing
2. Select which port (s) are to be enabled.
3. Set the Rate, Unit, and Flow Control parameters.
4. Click Apply to save the configuration.

Figure 3-14.2: QoS Ingress Port Policers Configuration



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	□

Parameter descriptions:

Port : The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.

Mode : Check the box for Port(s) you want to enable the QoS Ingress Port Policers function.

Rate : To set the Rate limit value for this port, the default is 500.

Unit : Scroll to select what unit of rate includes kbps, Mbps, fps and kfps. The default is kbps.

Flow Control : To evoke to enable or disable flow control on port.

Buttons:

Save – Click to save changes.

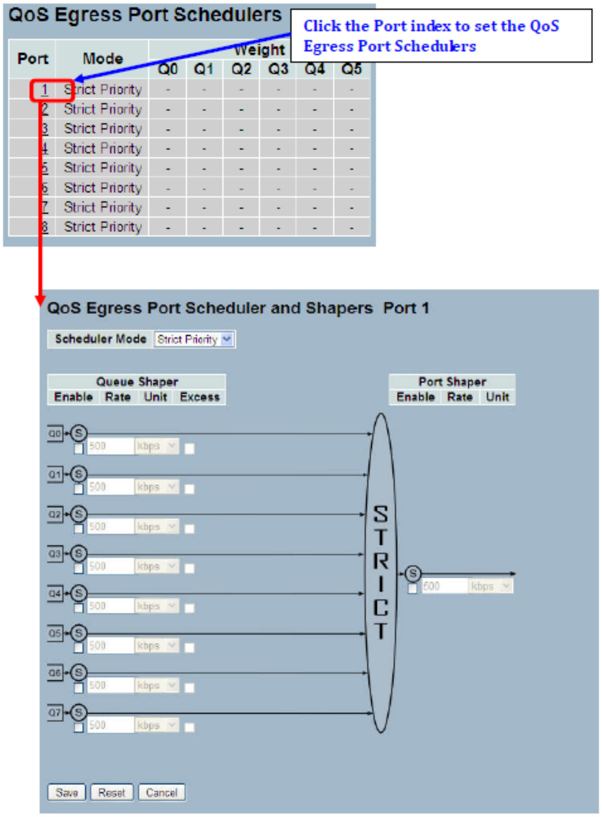
Reset- Click to undo any changes made locally and revert to previously saved values.

3-14.3 Port Scheduler

This section provides an overview of QoS Egress Port Schedulers for all switch ports. To display the QoS Port Schedulers in the web UI:

1. Click Configuration, QoS, Port Schedulers.
2. Display the QoS Egress Port Schedulers.

Figure 3-14.3: QoS Egress Port Schedules



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	-	-	-	-	-	-

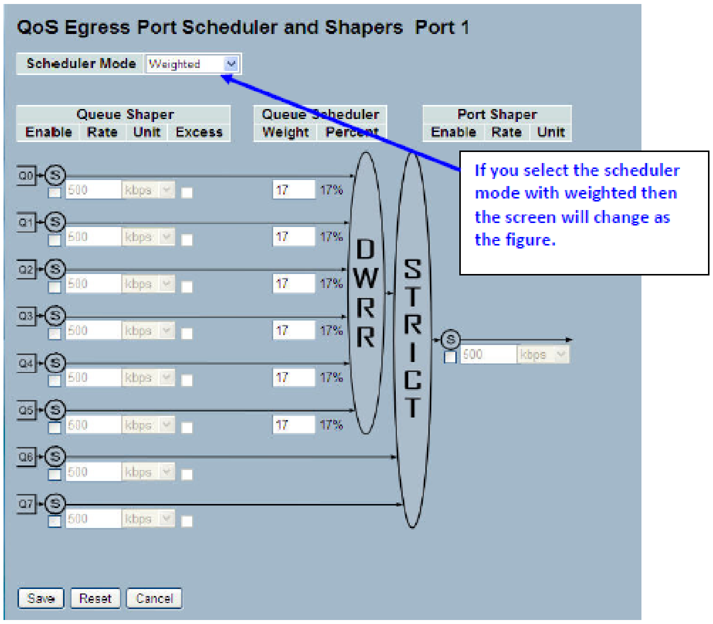
Click the Port index to set the QoS Egress Port Schedulers

QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: Strict Priority

Queue	Queue Shaper Enable	Rate	Unit	Excess
Q0	□	500	kbps	□
Q1	□	500	kbps	□
Q2	□	500	kbps	□
Q3	□	500	kbps	□
Q4	□	500	kbps	□
Q5	□	500	kbps	□
Q6	□	500	kbps	□
Q7	□	500	kbps	□

Port Shaper: Enable □ Rate 500 Unit kbps



QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: Weighted

Queue	Queue Shaper Enable	Rate	Unit	Excess	Queue Scheduler Weight	Percent
Q0	□	500	kbps	□	17	17%
Q1	□	500	kbps	□	17	17%
Q2	□	500	kbps	□	17	17%
Q3	□	500	kbps	□	17	17%
Q4	□	500	kbps	□	17	17%
Q5	□	500	kbps	□	17	17%
Q6	□	500	kbps	□		
Q7	□	500	kbps	□		

Port Shaper: Enable □ Rate 500 Unit kbps

If you select the scheduler mode with weighted then the screen will change as the figure.

Parameter descriptions:

Port : The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.

Mode : Shows the scheduling mode for this port

Weight (Qn) : Shows the weight for this queue and port.

Scheduler Mode : Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.

Queue Shaper Enable : Controls whether the queue shaper is enabled for this queue on this switch port.

Queue Shaper Rate : Controls the rate for the queue shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps".

Queue Shaper Unit : Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".

Queue Shaper Excess : Controls whether the queue is allowed to use excess bandwidth.

Queue Scheduler Weight : Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Queue Scheduler Percent : Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted"

Port Shaper Enable : Controls whether the port shaper is enabled for this switch port.

Port Shaper Rate : Controls the rate for the port shaper. The default value is ?. This value is restricted to 500-1000000 when the "Unit" is "kbps", and it is restricted to 1-100 when the "Unit" is "Mbps".

Port Shaper Unit : 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 undo any changes made locally and revert to previously saved values.

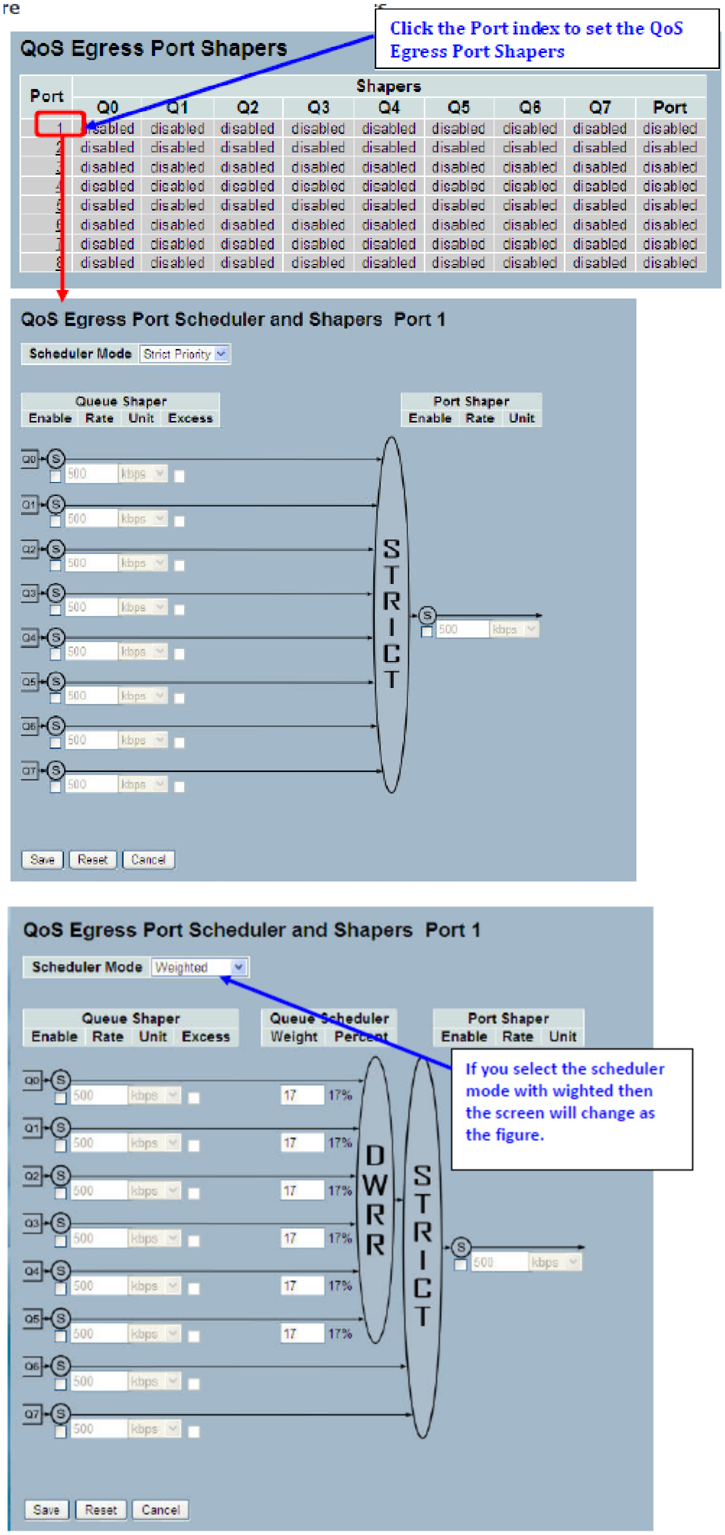
3-14.4 Port Shaping

This section provides an overview of QoS Egress Port Shaping for all switch ports. To display the QoS Port Shapers in the web UI:

1. Click Configuration, QoS, Port Shapers.
2. View the QoS Egress Port Shapers.

Figure 3-14.4: QoS Egress Port Shapers

re



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

QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: Strict Priority

Queue Shaper (Enable, Rate, Unit, Excess): Q0–Q7: □ 500 kbps □

Port Shaper (Enable, Rate, Unit): □ 500 kbps

QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: Weighted

Queue Shaper (Enable, Rate, Unit, Excess): Q0–Q7: □ 500 kbps □

Queue Scheduler (Weight, Percent): Q0–Q5: 17 17%

Port Shaper (Enable, Rate, Unit): □ 500 kbps

If you select the scheduler mode with wighted then the screen will change as the figure.

Parameter descriptions:

Port : The logical port for the settings contained in the same row. Click on the port number in order to configure the shapers.

Shapers (Qn) : Shows "disabled" or actual queue shaper rate - e.g. "800 Mbps".

Shapers (Port) : Shows "disabled" or actual port shaper rate - e.g. "800 Mbps".

Scheduler Mode : Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.

Queue Shaper Enable : Controls whether the queue shaper is enabled for this queue on this switch port.

Queue Shaper Rate : Controls the rate for the queue shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps".

Queue Shaper Unit : Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".

Queue Shaper Excess : Controls whether the queue is allowed to use excess bandwidth.

Queue Scheduler Weight : Controls the weight for this queue. The default value is "17". This value is restricted to 1- 100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Queue Scheduler Percent : Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted"

Port Shaper Enable : Controls whether the port shaper is enabled for this switch port.

Port Shaper Rate : Controls the rate for the port shaper. The default value is 500. This value is restricted to 500-1000000 when the "Unit" is "kbps", and it is restricted to 1-1000 when the "Unit" is "Mbps".

Port Shaper Unit : Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

Buttons:

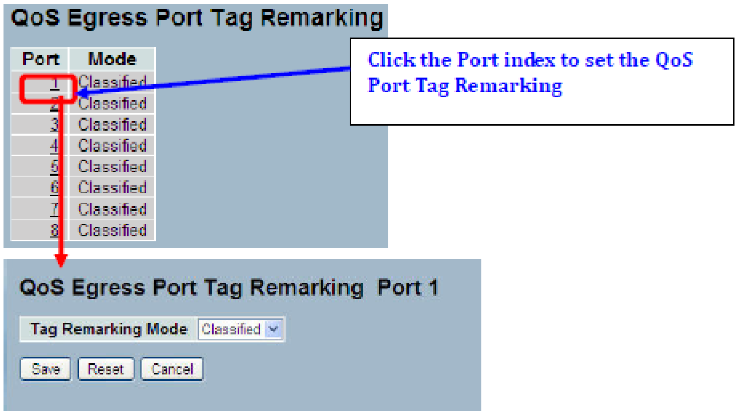
Save : Click to save changes.

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

3-14.5 Port Tag Remarking

This section provides an overview of QoS Egress Port Tag Remarking for all switch ports. To display the QoS Port Tag Remarking in the web UI:

1. Click Configuration, QoS, Port Tag Remarking.
2. Click the Port index to set the QoS Port Tag Remarking.
3. Click the Save, Reset or Cancel button as required.



QoS Egress Port Tag Remarking

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	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: Port Tag Remarking

Parameter descriptions:

Port : The logical port for the settings contained in the same row. Click on the port number in order to configure tag remarking.

Mode : Show the tag remarking mode for this port.

Classified: Use classified PCP/DEI values.

Default: Use default PCP/DEI values.

Mapped: Use mapped versions of QoS class and DP level.

Tag Remarking Mode : Scroll to select the tag remarking mode for this port.

Classified: Use classified PCP/DEI values.

Default: Use default PCP/DEI values.

Mapped: Use mapped versions of QoS class and DP level.

Buttons:

Save : Click to save changes.

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

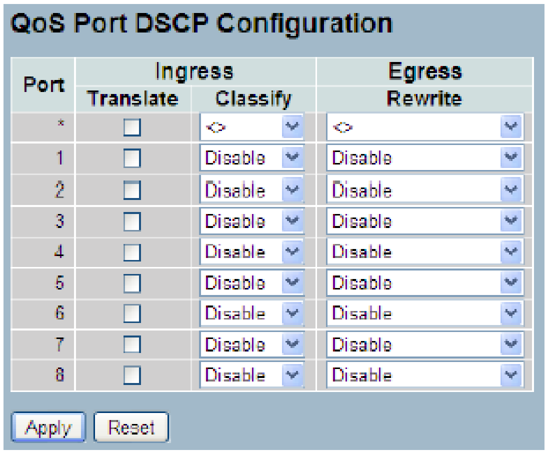
Cancel – Click to cancel the changes.

3-14.6 Port DSCP

This page lets you set the QoS Port DSCP parameters for all switch ports. To configure QoS Port DSCP in the web UI:

1. Click Configuration, QoS, Port DSCP
2. Enable or disable the Ingress Translate and select the Classify parameters.
3. Select Egress Rewrite parameters.
4. Click the Save button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

Figure 3-14.6: QoS Port DSCP Configuration



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

Parameter descriptions:

Port : The Port column shows the list of ports for which you can configure DSCP ingress and egress settings.

Ingress : In Ingress settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress:

1. **Translate** : To Enable the Ingress Translation click the checkbox.
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**: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.
   - **All**: Classify all DSCP.

Egress : Port Egress Rewriting can be one of these parameters:

- **Disable**: No Egress rewrite.
- **Enable**: Rewrite enable without remapped.
- **Remap**: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value.

Buttons:

Apply – Click to save changes.

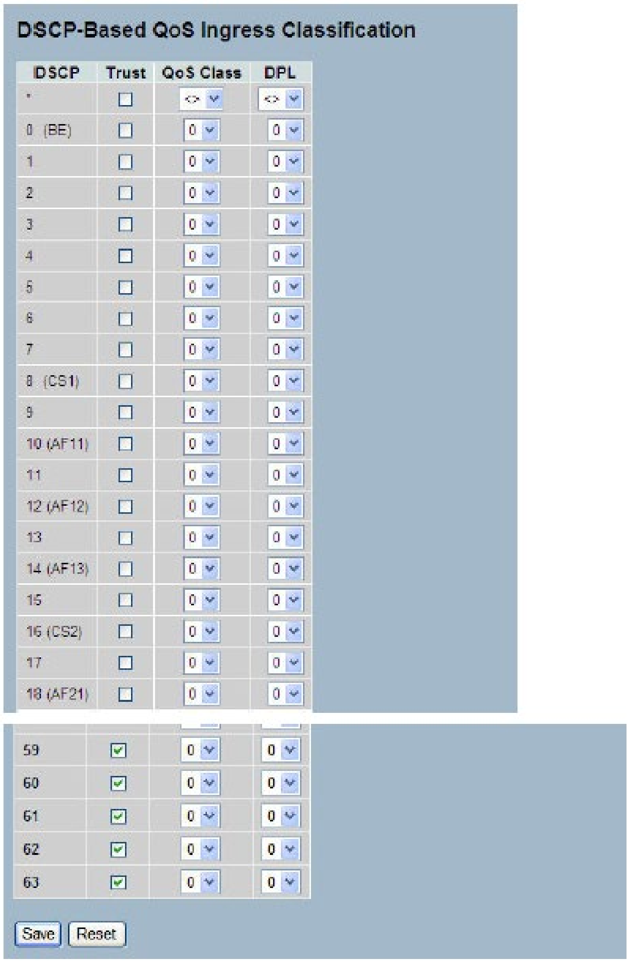
Reset- Click to undo any changes made locally and revert to previously saved values.

3-14.7 DSCP-Based QoS

This page lets you configure the DSCP-Based QoS mode. To configure the DSC-based QoS Ingress Classification parameters in the web UI:

1. Click Configuration, QoS, DSCP-Based QoS
2. Enable or disable the DSCP for Trust
3. Select QoS Class and DPL parameters
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values

Figure 3-14.7: DSCP-Based QoS Ingress Classification Configuration



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
17	□	0	0
18 (AF21)	□	0	0
59	☑	0	0
60	☑	0	0
61	☑	0	0
62	☑	0	0
63	☑	0	0

Parameter descriptions:

DSCP : Maximum number of support ed DSCP values are 64.

Trust : Click to check if the DSCP value is trusted.

QoS Class : QoS Class value can be any of (0-7).

DPL : Drop Precedence Level (0-3).

Buttons:

Save – Click to save changes.

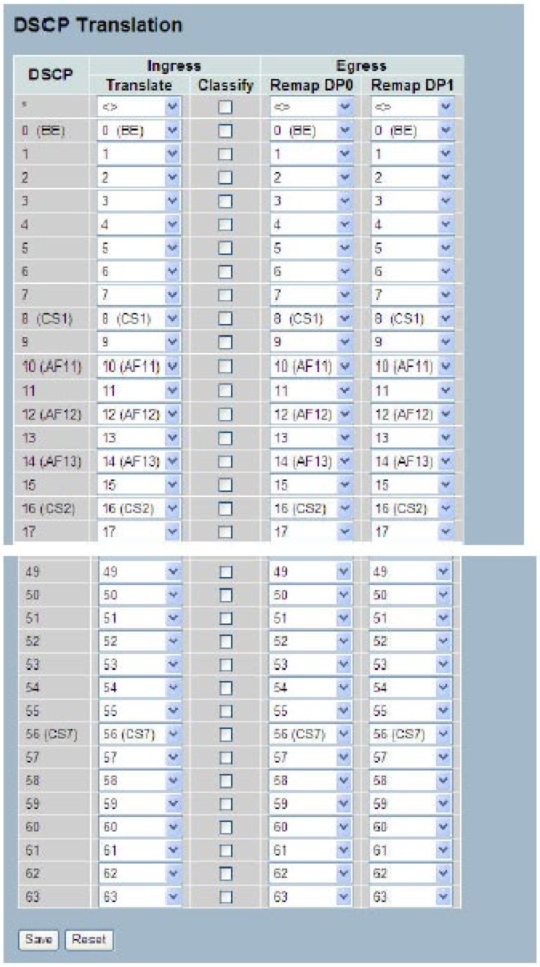
Reset- Click to undo any changes made locally and revert to previously saved values.

3-14.8 DSCP Translation

This page lets you configure basic QoS DSCP Translation settings in Ingress or Egress. To configure DSCP Translation parameters in the web UI:

1. Click Configuration, QoS, DSCP Translation,
2. Scroll to set the Ingress Translate and Egress Remap DP0 and Remap DP1 parameters.
3. Evoke to enable or disable Classify.
4. Click Save to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values

Figure 3-14.8: DSCP Translation Configuration



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
12 (AF12)	12 (AF12)	□	12 (AF12)	12 (AF12)
13	13	□	13	13
14 (AF13)	14 (AF13)	□	14 (AF13)	14 (AF13)
15	15	□	15	15
16 (CS2)	16 (CS2)	□	16 (CS2)	16 (CS2)
17	17	□	17	17
49	49	□	49	49
50	50	□	50	50
51	51	□	51	51
52	52	□	52	52
53	53	□	53	53
54	54	□	54	54
55	55	□	55	55
56 (CS7)	56 (CS7)	□	56 (CS7)	56 (CS7)
57	57	□	57	57
58	58	□	58	58
59	59	□	59	59
60	60	□	60	60
61	61	□	61	61
62	62	□	62	62
63	63	□	63	63

Parameter descriptions:

DSCP : Maximum number of supported DSCP values is 64 and valid DSCP values range from 0 to 63.

Ingress : Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. There are two configuration parameters for DSCP Translation:

Translate : DSCP at Ingress side can be translated to any of (0-63) DSCP values.

Classify : Click to enable Classification at Ingress side.

Egress : The following configurable parameters are for the Egress side:

1. **Remap DP0** : Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63

2. **Remap DP1** : Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.

Buttons:

Save : Click to save changes.

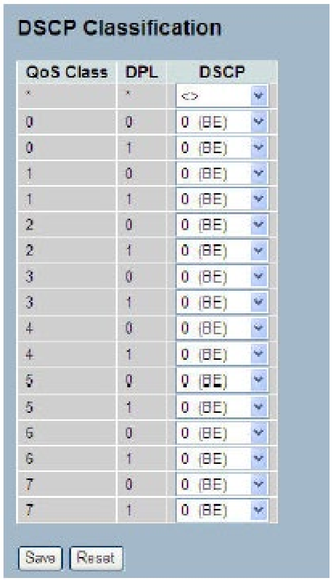
Reset : Click to undo any changes made locally and revert to previously saved values.

14.9 DSCP Classification

This page lets you configure and map DSCP value to a QoS Class and DPL value. To configure the DSCP Classification parameters in the web UI:

1. 1.Click Configuration, QoS, DSCP Translation.
2. Set the DSCP Parameters.
3. Click the Save button to save the settings.
4. To cancel the settings click the Reset button to revert to previously saved values.

Figure 3-14.9: DSCP Classification Configuration



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)

Parameter descriptions:

QoS Class : Available QoS Class value ranges from 0 to 7. QoS Class (0-7) can be mapped to the following parameters.

DPL : Drop Precedence Level (0-1) can be configured for all available QoS Classes.

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

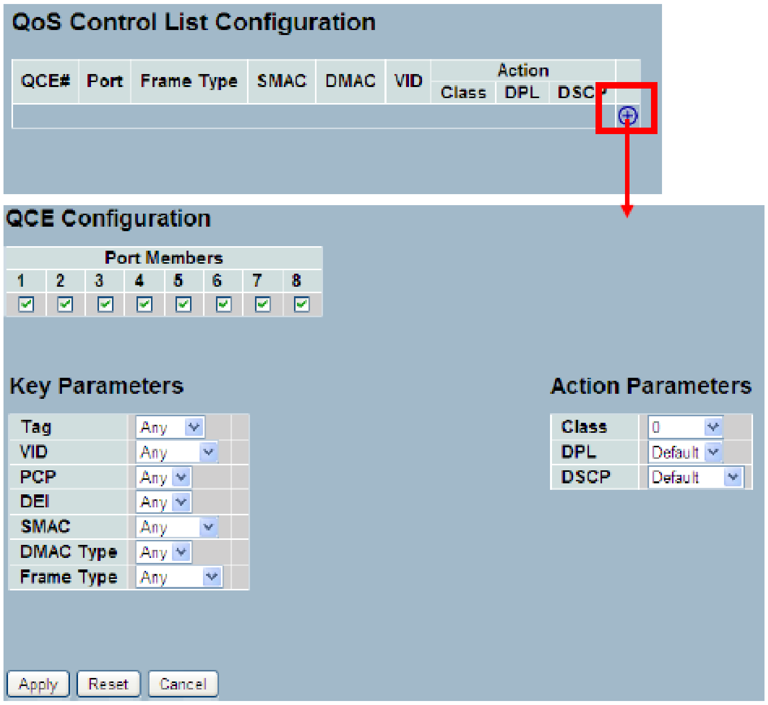
3-14.10 QoS Control List Configuration

This page shows the QoS Control List(QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is 256 per switch. Click on the lowest plus sign to add a new QCE to the list.

To configure QoS Control List parameters in the web UI:

1. Click Configuration, QoS, QoS Control List.
2. Click the to add a new QoS Control List.
3. Scroll all parameters and evoke the Port Member to join the QCE rules.
4. Click the Save button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

Figure 3-14.10: QoS Control List Configuration



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
☑	☑	☑	☑	☑	☑	☑	☑

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

Parameter descriptions:

QCE# : Indicate the index of QCE.

Port : Indicates the list of ports configured with the QCE.

Frame Type : Indicates the type of frame to look for incoming frames. Possible frame types are:

Any: The QCE will match all frame 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 : Display the OUI field of Source MAC address, i.e. first three octet (byte) of MAC address.

DMAC : Specify the type of Destination MAC addresses for incoming frame. Possible values are:

Any: All types of Destination MAC addresses are allowed (default).

Unicast: Only Unicast MAC addresses are allowed.

Multicast: Only Multicast MAC addresses are allowed.

Broadcast: Only Broadcast MAC addresses are allowed.

VID :Indicates VLAN ID, either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'.

Conflict : Displays QCE status. It may happen that resources required to add a QCE may not available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the resource required by the QCE and clicking the 'Refresh' button.

Action : Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. There are three action fields: Class, DPL and DSCP.

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 DPL column.

DSCP: If a frame matches the QCE then 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 row.

⬆ : Moves the QCE up the list.

⬇ : Moves the QCE down the list.

⊗ : Deletes the QCE.

⊕ : The lowest plus sign adds a new entry at the bottom of the QCE listings.

Port Members : Check the checkbox button in case you what to make any port member of the QCL entry. By default all ports will be checked.

Key Parameters : Key configuration is described as below:

Tag Value of Tag field can be 'Any', 'Untag' or 'Tag'

VID: Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; you can enter either a specific value or a range of VIDs

PCP Priority Code Point: Valid value PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

DEI Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any'

SMAC Source MAC address: 24 MS bits (OUI) or 'Any'

DMAC Type Destination MAC type: possible values are unicast (UC), multicast (MC), broadcast (BC) or 'Any'

Frame Type: can have any of these values: 1. Any, 2. Ethernet, 3. LLC, 4. SNAP, 5. IPv4, or 6. IPv6 as described below.

1. ***Any*** : Allow all types of frames.

2. ***Ethernet*** : Ethernet Type Valid Ethernet type can have value within 0x600-0xFFFF or 'Any', 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 Address 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 0x00-0xFFFF or 'Any', default value is 'Any'

5. ***IPv4*** : Protocol IP protocol number: (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(DSCP):
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: (0-255, TCP or UDP) or 'Any'.
Source IP IPv6 source address: (a.b.c.d) or 'Any', 32 LS bits.
DSCP Diffserv Code Point value (DSCP): can be a specific value, a range of values, 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 a 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.

Action Configuration :

Class QoS Class: "class (0-7)", default- basic classification.

DP Valid DP Level can be (0-3)", default- basic classification.

DSCP Valid dscp value can be (0-63, BE, CS1-CS7, EF or AF11-AF43).

Buttons:

Apply : Click to save changes.

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

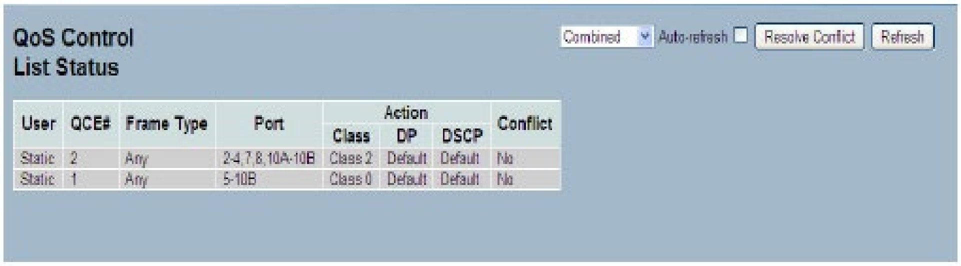
Cancel : Click to ignore changes.

3-14.11 QCL Status

This page lets you configure and view the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 per switch. To display QoS Control List Status in the web UI:

1. Click Configuration, QoS , QCL Status.
2. To auto-refresh the information click the “Auto-refresh” button.
3. Select the combined, static, Voice VLAN and conflict.
4. Click the “Refresh“ button to refresh an entry of the MVR Statistics Information.

Figure 3-14.11: QoS Control List Status



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

Parameter descriptions:

User : Indicates the QCL user. The default is ‘Combined’.

QCE# : Indicates the index of QCE.

Frame Type : Indicates the type of frame to look for incoming frames. Possible frame types are:

Any: The QCE will match all frame type.

Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.

LLC: Only (LLC) frames are allowed

LLC: Only (SNAP) frames are allowed.

IPv4: The QCE will match only IPV4 frames.

IPv6: The QCE will match only IPV6 frames.

Port : Indicates the list of ports configured with the QCE.

Action : Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. There are three action fields: Class, DPL and DSCP.

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 DPL column.

DSCP: If a frame matches the QCE then DSCP will be classified with the value displayed under the DSCP column.

Conflict : Display QCE status. It may happen that resources required to add a QCE may not available, in that case it shows conflict status as 'Yes', otherwise it is always 'No’. Please note that conflict can be resolved by releasing the resource required by the QCE and pressing the 'Refresh' button.

Buttons:

Auto-refresh : To evoke the auto-refresh icon then the device will refresh the information automatically.

Resolve Conflict : Click it to resolve the conflict issue.

Refresh : Click to refresh the QCL information manually.

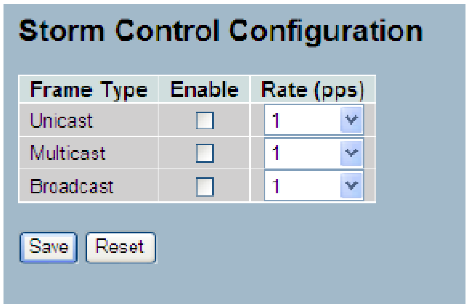
3-14.12 Storm Control

This page lets you configure Storm control for the switch. There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. 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.

To configure Storm Control parameters in the web UI:

1. Click Configuration, QoS, Storm Control Configuration.
2. Select the frame type to enable storm control.
3. Set the Rate parameters.
4. Click the Save button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

Figure 3-14.12: Storm Control Configuration



Storm Control Configuration

Frame Type	Enable	Rate (pps)
Unicast	□	1
Multicast	□	1
Broadcast	□	1

Parameter descriptions:

Frame Type : The settings in a particular row apply to the frame type listed here: Unicast, Multicast or Broadcast.

Enable : Enable or disable 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. , 1024K, 2048K, 4096K, 8192K, 16384K or 32768K. The 1 kpps is actually 1002.1 pps.

Buttons:

Save : Click to save changes.

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

3-15 Thermal Protection

This section lets you set and view current settings for controlling thermal protection. Thermal protection is used to protect the chip from getting overheated.

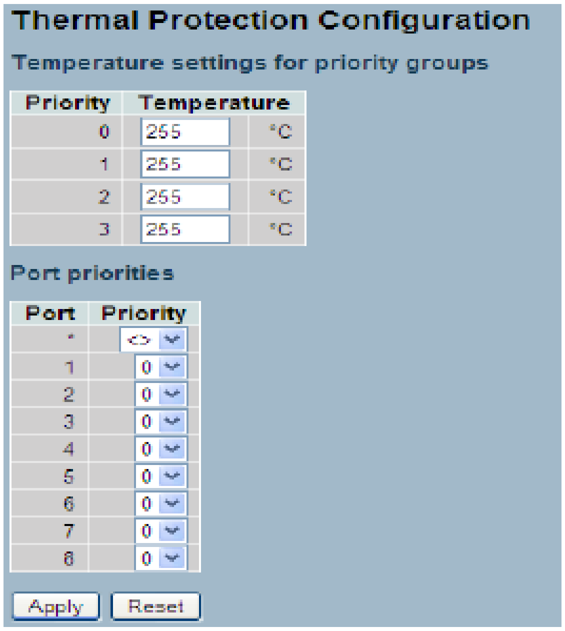
3-15.1 Configuration

This page lets you view and set current setting for controlling thermal protection. Thermal protection is used to protect the chip from getting overheated. When the temperature exceeds the configured thermal protection temperature, ports will be turned off in order to decrease the power consumption. It is possible to arrange the ports with different priorities. Each priority can be given a temperature at which the corresponding ports will be turned off

To configure Thermal Protection in the web UI:

1. Click Configuration, Thermal Protection, Configuration.
2. Specify the temperature priority (0 to 3).
3. Set the Priority
4. Click the save to save the settings
5. To cancel the settings click the Reset button to revert to previously saved values.

Figure 3-15.1: Thermal Protection Configuration



Thermal Protection Configuration

Temperature settings for priority groups

Priority	Temperature	
0	255	°C
1	255	°C
2	255	°C
3	255	°C

Port priorities

Port	Priority
*	<>
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0

Parameter descriptions: Temperature settings for priority groups. The temperature at which the ports with the corresponding priority will be turned off.

Priority : The criteria index for thermal protect trigger temperature, The index from 0 to 3.

Temperature : To set the temperature to trigger the thermal protect in degrees C. **Note**: The temperature means the MAC and PHY chipset's TA temperature, not PSU device temperature or environment temperature. Please don't set environment temperature limitation value.

Port priorities : The priority the port belongs to. It lets you set priority criterion to trigger whether each port is to be turned off via thermal protection.

Buttons:

Apply : Click to save changes.

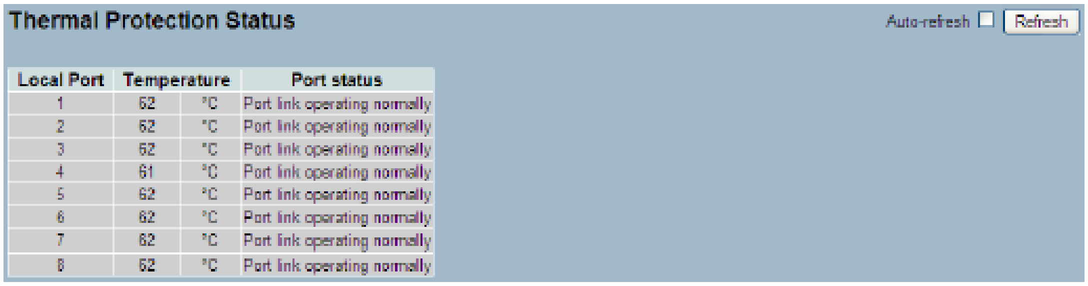
Reset : Click to undo any changes made locally and revert to previously saved values.

3-15.2 Status

This page lets you view thermal status information related to thermal protection when the Thermal Protection function is configured. To display Thermal Protection Status in the web UI:

1. Click Configuration, Thermal Protection, Status.
2. Use the Auto-refresh or Refresh button as required.

Figure 3-15.2: Thermal Protection Status



Thermal Protection Status

Local Port	Temperature		Port status
1	62	°C	Port link operating normally
2	62	°C	Port link operating normally
3	62	°C	Port link operating normally
4	61	°C	Port link operating normally
5	62	°C	Port link operating normally
6	62	°C	Port link operating normally
7	62	°C	Port link operating normally
8	62	°C	Port link operating normally

Parameter descriptions:

Local Port : Indicates the list of physical Port.

Temperature : Shows the current chip temperature in degrees Celsius. **Note** The temperature means the MAC and PHY chipset's TA temperature not PSU device temperature or environment temperature.

Port Status : To display the Port status (includes link up or link down).

Buttons:

Auto-refresh : Click to automatically refresh the page every 3 seconds.

Refresh : Click to refresh the page information manually.

3-16 s-Flow Agent

The sFlow Collector configuration for the switch can be monitored and modified here. Up to one Collector is supported. This page allows for configuring sFlow collector IP type, sFlow collector IP Address, and Port Number for an sFlow Collector

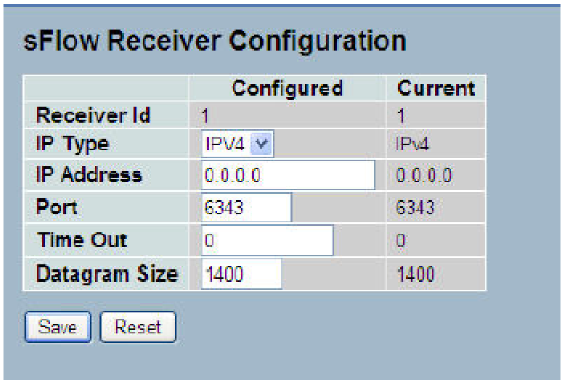
3-16.1 Collector

The "Current " field displays the currently configured sFlow Collector. The "Configured" field displays the new Collector Configuration.

To configure the sFlow Agent in the web UI:

1. Click Configuration, sFlow Agent, Collector.
2. Set the parameters.
3. Click the Save button to save the settings.
4. To cancel the settings click the Reset button to revert to previously saved values.

Figure 3-16.1: sFlow Receiver Configuration



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

Parameter descriptions:

Receiver Id : The "Receiver ID" field shows the ID of this particular sFlow Receiver. Currently one ID is supported as one collector is supported.

IP Type : A drop down list to select the type of IP of Collector is displayed. By default, IPv4 is the type of Collector IP type. You can use IPv4 or IPv6.

IP Address : 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(our switch). By default, the IP is set to 0.0.0.0, and a new entry must 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 must be typed into the text box. The value accepted is within the range of 1-65535. But an appropriate port number not used by other protocols must 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 the value is set before it expires. The value accepted is within the range of 0-2147483647. By default it is set to 0.

Datagram Size : The maximum UDP datagram size to send out the sFlow samples to the receiver. The value accepted is within the range of 200-1500 bytes. The default is 1400 bytes.

Buttons:

Save : Click to save changes.

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

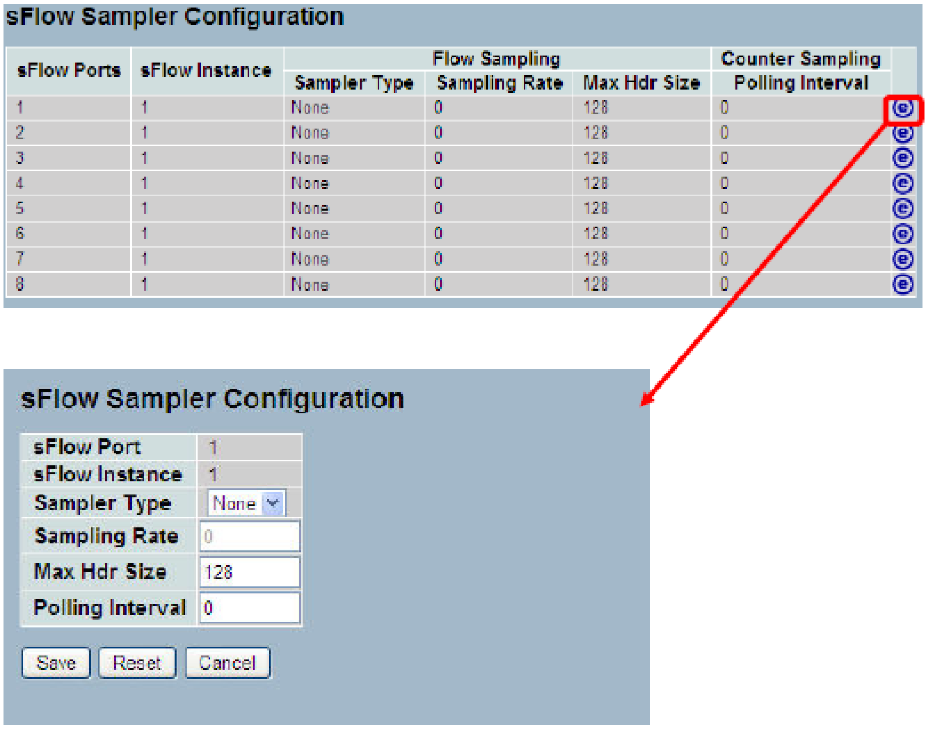
3-16.2 Sampler

This page lets you set and view sFlow Sampler parameters, based on a defined sampling rate, 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.

To configure the sFlow sampler in the web UI:

1. Click Configuration, sFlow Agent, Sampler.
2. Click the ⓔ icon to edit the sFlow sampler parameters.
3. Set the Sampler Type, Sampling Rate, Max Hdr Size, and Polling Interval.
4. Click the Save button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

Figure 3-16.2: sFlow sampler Configuration



sFlow Sampler Configuration

sFlow Ports	sFlow Instance	Flow Sampling			Counter Sampling	
		Sampler Type	Sampling Rate	Max Hdr Size	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	ⓔ
6	1	None	0	128	0	ⓔ
7	1	None	0	128	0	ⓔ
8	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

Parameter descriptions:

sFlow Ports : List of the port numbers on which sFlow is configured.

sFlow Instance : Configure sFlow instance for the port number.

Sampler Type : Configured sampler type on the port and can be ***None***, ***Rx***, ***Tx*** or ***All***. You can scroll to choice one for your sampler type. By default, the value is "None".

Sampling Rate : Configure the sampling rate on the ports.

Max Hdr Size : Configure the size of the header of the sampled frame.

Polling Interval : Configure the polling interval for the counter sampling.

Buttons:

ⓔ: Lets you edit the Data source sampler configuration.

Save : Click to save changes.

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

Cancel : Click to cancel to clear up what your setting.

Auto-refresh : Click to auto-refresh the page automatically every 3 seconds.

Refresh : Click to refresh the sFlow Sampler information manually.

3-17 Loop Protection

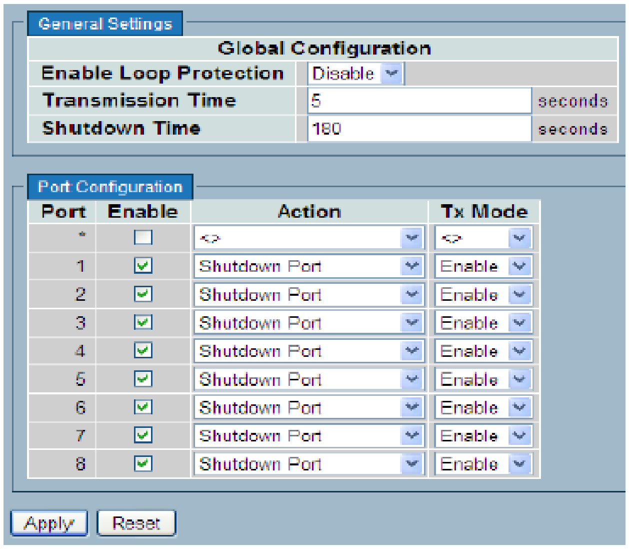
Loop detection is used to detect the presence of traffic. When the switch receives packet's (looping detection frame) MAC address the same as oneself from port, show Loop Protection happens. The port will be locked when it received the looping detection frames. If you want to resume the locked port, find and remove the looping path, then select the resume the locked port and click on "Resume" to turn on the locked ports.

3-17.1 Configuration

This page lets you set Loop Protection. To configure Loop Protection parameters in the web UI:

1. Click Configuration, Loop Protection, Configuration.
2. Enable or disable port loop protection.
3. Click the Save button to save the settings.
4. To cancel the settings click the Reset button to revert to previously saved values.

Figure 3-17.1: Loop Detection Configuration.



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

Parameter descriptions:

Enable Loop Protection: Controls whether loop protections is enabled (as a whole).

Transmission Time: The interval between each loop protection PDU sent on each port. Valid values are 1 – 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 shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart).

Port No: The switch port number of the port.

Enable : Controls whether loop protection is enabled on this switch port

Action: Configures the action performed when a loop is detected on a port. Valid values are Shutdown Port, Shutdown Port and Log or Log Only.

Tx Mode : Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

Buttons:

Save : Click to save changes.

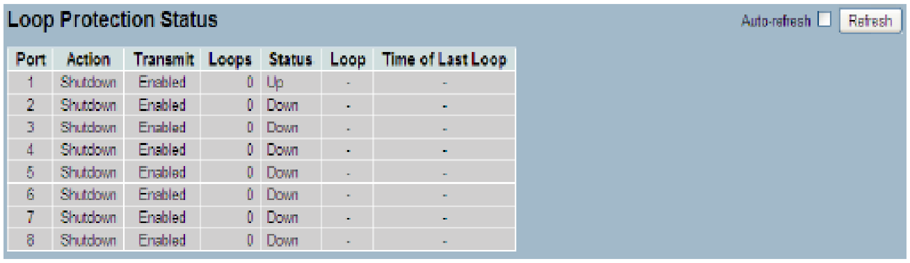
Reset : Click to undo any changes made locally and revert to previously saved values.

3-17.2 Status

This page displays Loop Protection status that is set on the switch. To display Loop protection parameters in the web UI:

1. Click Configuration, Loop protection, Status.
2. Select enable or disable Auto-refresh.
3. Click the Refresh button to clear or update the record of Loop protection.

Figure 3-17.2: Loop Protection Status.



Loop Protection Status

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	-	-

Parameter descriptions:

Port: The switch port number of the logical port.

Action: The currently configured port action.

Transmit: The currently configured port transmit mode (Enabled or Disabled).

Loops: The number of loops detected on this port.

Status: The current loop protection status of the port (Up or Down).

Loop: Whether a loop is currently detected on the port.

Time of Last Loop: The time of the last loop event detected.

Buttons:

Refresh –Click to refresh the page immediately.

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

3-18 Single IP

Single IP Management (SIM), a simple and useful method to optimize network utilities and management, 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:

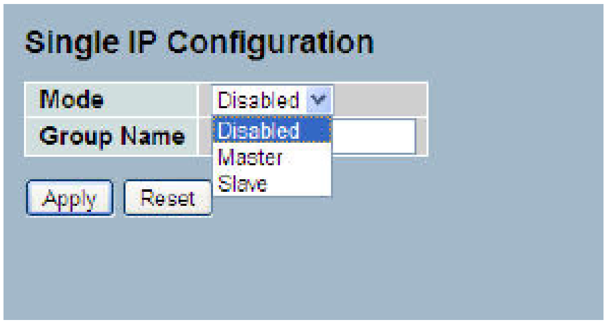
- Simplify management of small workgroups or wiring closets while scaling networks to handle increased bandwidth demand.
- Reduce the number of IP addresses needed on the network.
- Virtual stacking structure - Eliminate any specialized cables for stacking and remove the distance barriers that typically limit topology options when using other stacking technology.

3-18.1 Configuration

To configure Single IP in the web UI:

1. Click Configuration, Single IP
2. Set the page parameters.
3. Set the Role for what mode you want to set on the Single IP (Disable, or Master, or Slave).
4. Enter a Group name.
5. Click the Apply button to save the settings.
6. To cancel the settings click the Reset button to revert to previously saved values.

Figure 3-18.1: Single IP Configuration



Single IP Configuration

Mode	Disabled
Group Name	

Parameter descriptions:

Mode: The parameter lets you to disable the SIP function or set the device become a Master role or Slave role.

Master: The role is root. User connects to the Master and can control the Slaves in the same SIP group.

Slave: The role is slave. User connects to the switch what is a slave via Master management GUI.

Group name: The parameter lets you to set a group name what you want to make a Single IP management Group, the available value up to 64 characters describing group name.

Buttons:

Apply – Click to save changes.

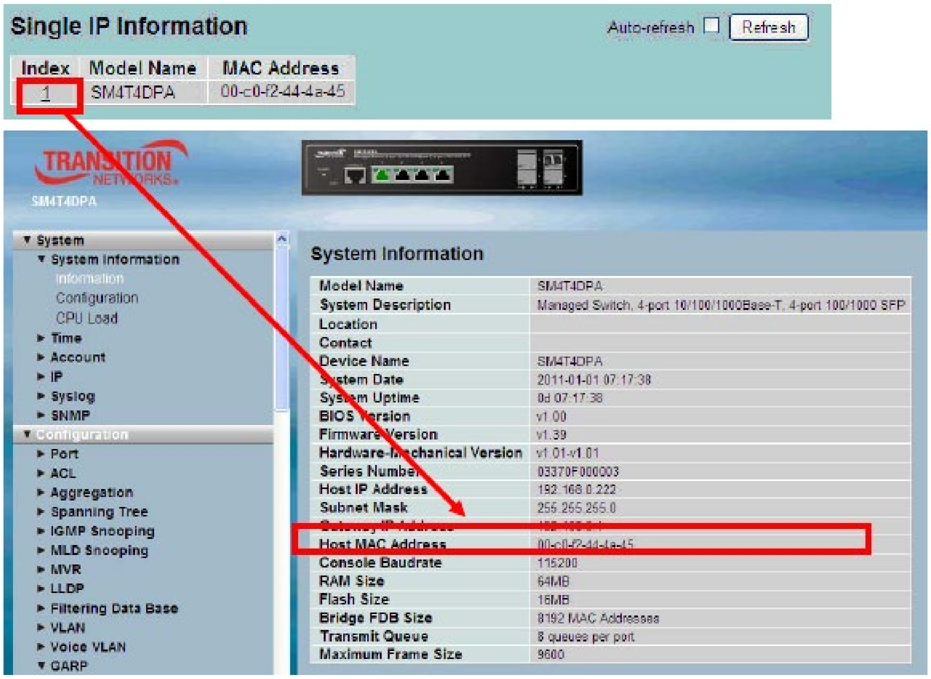
Reset- Click to undo any changes made locally and revert to previously saved values.

3-18.2 Information

This page displays the Single IP information currently set on the switch. To show Single IP information in the web UI:

1. Click Configuration, Single IP, and then information
2. Click refresh or evoke auto-refresh to automatic update information.

Figure 3-18.2: Single IP information



Single IP Information

Index	Model Name	MAC Address
1	SM4T4DPA	00-c0-f2-44-4a-45

System Information

Model Name	SM4T4DPA
System Description	Managed Switch, 4-port 10/100/1000Base-T, 4-port 100/1000 SFP
Location	
Contact	
Device Name	SM4T4DPA
System Date	2011-01-01 07:17:38
System Uptime	0d 07:17:38
BIOS Version	v1.00
Firmware Version	v1.39
Hardware-Mechanical Version	v1.01-v1.01
Series Number	03370F000003
Host IP Address	192.168.0.222
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.0.1
Host MAC Address	00-c0-f2-44-4a-45
Console Baudrate	115200
RAM Size	64MB
Flash Size	16MB
Bridge FDB Size	8192 MAC Addresses
Transmit Queue	8 queues per port
Maximum Frame Size	9600

Parameter descriptions:

Index: The parameter lets you know how many slave devices connect to the SIP group. **Note**: When you click the index you will redirect to the slave device and do the switch configuration or display/management the device.

Model name: The parameter lets you to know what kind of device is joined to this SIP group.

MAC Address: The parameter lets you to know what device's MAC address is joined to this SIP group.

Buttons:

Refresh : Click to refresh the page immediately.

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

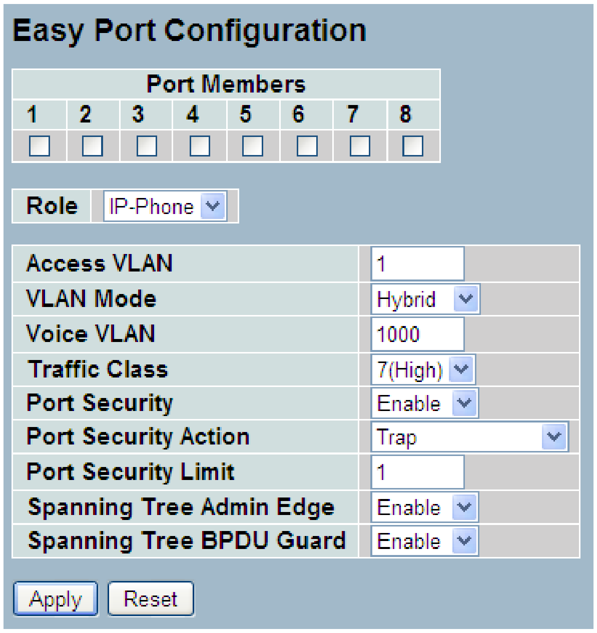
3-19 Easy Port

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. This makes it easy to implement Voice IP phones, Wireless Access Points, IP Cameras, etc. You can leverage a configuration to run a converged voice, video, and data network with quality of service (QoS), bandwidth, latency, and high performance.

To configure Easy Port in the web UI:

1. Click Configuration, Easy Port.
2. Set the parameters.
3. Set the Role for the kind of device you want the Easy Port to connect to.
4. Click the save to save the setting
5. To cancel the settings click the Reset button. It will revert to previously saved values.

Figure 3-19.1: Easy Port Configuration



Easy Port Configuration

Port Members							
1	2	3	4	5	6	7	8
□	□	□	□	□	□	□	□

Role	IP-Phone

Access VLAN	1
VLAN Mode	Hybrid
Voice VLAN	1000
Traffic Class	7(High)
Port Security	Enable
Port Security Action	Trap
Port Security Limit	1
Spanning Tree Admin Edge	Enable
Spanning Tree BPDU Guard	Enable

Parameter descriptions:

Port Members : Check to enable the Port(s) you want enable for the Easy Port function.

Role : Select what kind of device you want to connect and implement with this Easy Port setting.

Access VLAN : To set the Access VLAN ID, it means the switch port access VLAN ID (AVID).

VLAN Mode : Scroll to select the VLAN mode with Access, Trunk, or Hybrid.

Voice VLAN : If you connect the IP Phone you need to assign the Voice VLAN ID. The value of the port number must be typed into the text box.

Traffic Class : Scroll to 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 the highest priority then set the value to 7.

Port Security : Enable or disable the Port Security function on the Port. If you enable the function then you must set Port Security limit to allow how many devices can access the port (via MAC address).

Port Security Action : Select when the device won't allow access then switch action as trap, shutdown ,or trap & shutdown.

Port Security limit : Set the Port security limit (how many device MAC addresses will be allowed to access the port). The default is 1.

Spanning Tree Admin Edge : Scroll to enable or disable the Spanning Tree Admin Edge function on the Easy Port.

Spanning Tree BPDU Guard : Scroll to enable or disable the Spanning Tree BPDU Guard function on the Easy Port.

Buttons:

Save : Click to save changes.

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

3-20 Mirroring

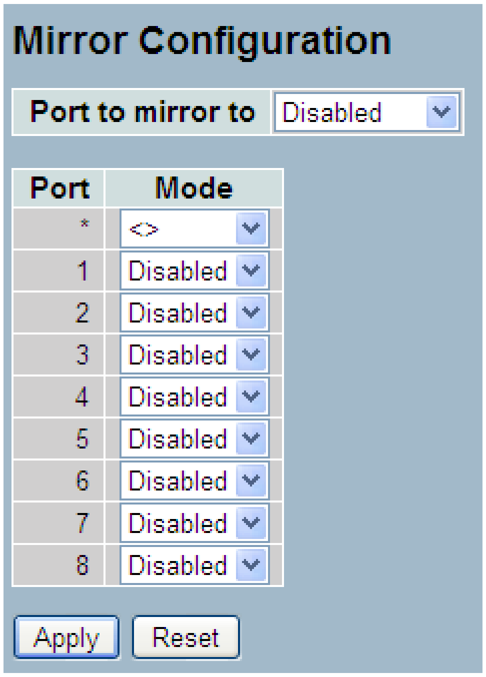
You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

Mirroring is used to monitor the traffic of the network. For example, assume that Port A and Port B are Monitoring Port and Monitored Port respectively, thus, the traffic received by Port B will be copied to Port A for monitoring.

To configure Mirroring in the web UI:

1. Click Configuration, Mirroring.
2. Scroll to select Port to mirror on which port
3. Scroll to disabled, enable, TX Only and RX Only to set the Port mirror mode
4. Click the save to save the settings.
5. To cancel the settings click the Reset button. It will revert to previously saved values.

Figure 3-20.1: Mirror Configuration



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

Parameter descriptions:

Port to mirror to : Port to mirror 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 disables mirroring.

Mirror Port Configuration

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

Mode : Select 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 nor frames 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. It is therefore not possible to mirror Tx frames on the mirror port. Because of this, mode for the selected mirror port is limited to Disabled or Rx only.

Buttons:

Apply : Click to save changes.

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

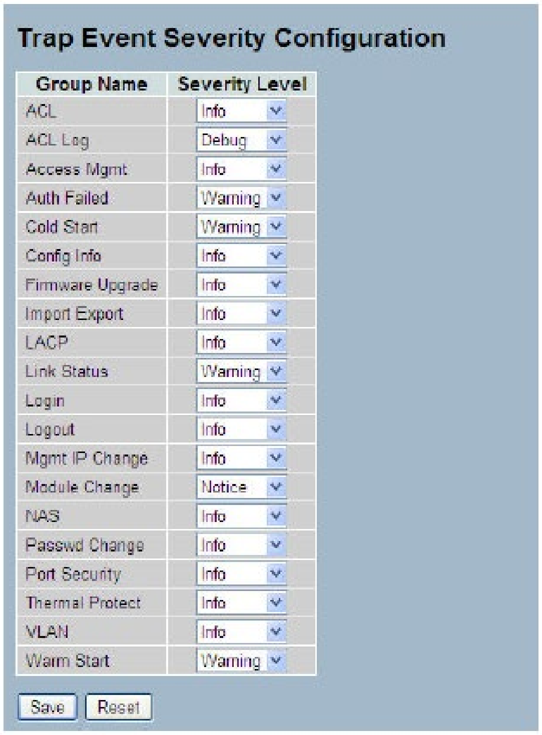
3-21 Trap Event Severity

This function is used to set an Alarm trap and get the Event log. The Trap Events Configuration function is used to enable the switch to send out the trap information when pre-defined trap events occur.

To configure Trap Event Severity in the web UI:

1. Click Configuration, Trap Event Severity Configuration
2. Scroll to select the Group name and Severity Level
3. Click the save to save the setting
4. To cancel the settings click the Reset button. It will revert to previously saved values.

Figure 3-21.1: Trap Event Severity Configuration



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
Mgmt IP Change	Info
Module Change	Notice
NAS	Info
Passwd Change	Info
Port Security	Info
Thermal Protect	Info
VLAN	Info
Warm Start	Warning

Parameter descriptions:

Group Name : The field describe the Trap Event definition.

Severity Level : Select the event type: Emerg, Alert, Crit, Error, Warming, Notice, Info and Debug.

Buttons:

Save – Click to save changes.

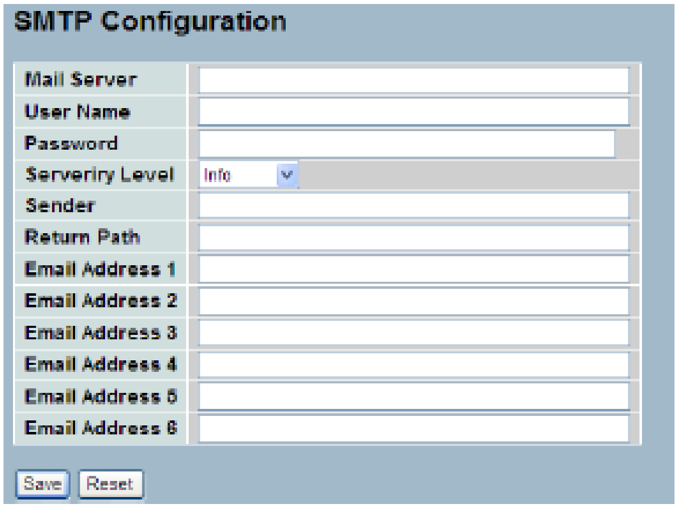
Reset- Click to undo any changes made locally and revert to previously saved values.

3-22 SMTP Configurations

The function is used to set an Alarm trap when the switch alarm then you could set the SMTP server to send you the alarm mail. To configure SMTP in the web UI:

1. Click Configuration, SMTP Configuration.
2. Select the Severity Level
3. Specify the parameters in each blank field.
4. Click the Save button to save the settings.
5. To cancel the settings click the Reset button. It will revert to previously saved values.

Figure 3-22.1: SMTP Configuration



SMTP Configuration

Mail Server	
User Name	
Password	
Serveriry Level	Info
Sender	
Return Path	
Email Address 1	
Email Address 2	
Email Address 3	
Email Address 4	
Email Address 5	
Email Address 6	

Parameter descriptions:

Mail Server : Specify the IP Address of the server transferring your email.

Username : Specify the username on the mail server.

Password : Specify the password on the mail server.

Sender : To set the mail sender name.

Return-Path : To set the mail return-path as sender mail address.

Email Address 1-6 : Email address that you want to receive the alarm message.

Buttons:

Save – Click to save changes.

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

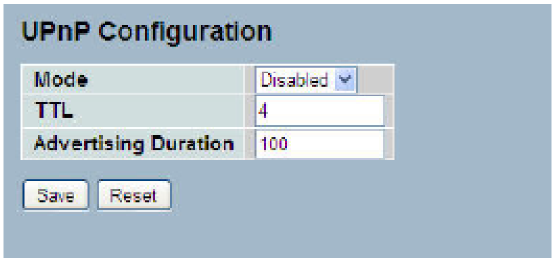
3-23 UPnP

UPnP (Universal Plug and Play) was promoted by the UPnP Forum to enable simple robust connectivity to stand-alone devices and PCs from over 800 vendors of consumer electronics, network computing, etc. UPnP has been managed by the Open Connectivity Foundation (OCF) since 2016.

To configure UPnP in the web UI:

1. Click Configuration, UPnP.
2. Select the mode (enable or disable).
3. Specify the parameters in each blank field.
4. Click the save to save the settings.
5. To cancel the settings click the Reset button. It will revert to previously saved values.

Figure 3-23.1: UPnP Configuration



UPnP Configuration

Mode	Disabled
TTL	4
Advertising Duration	100

Parameter descriptions:

Mode : Indicates the UPnP operation mode. Possible modes are:

Enabled: Enable UPnP mode operation.

Disabled: Disable UPnP mode operation.

When the mode is enabled, two ACEs are added automatically to trap UPNP related packets to CPU. The ACEs are automatically removed when the mode is disabled.

TTL : The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are 1 - 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, in the standard it is recommended that such refreshing of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are 100 - 86400.

Buttons:

Save : Click to save changes.

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

Chapter 4 - Security

This chapter describes the switch security configuration tasks to enhance the security of the local network including IP Source Guard, ARP Inspection, DHCP Snooping, AAA, etc.

4-1 IP Source Guard

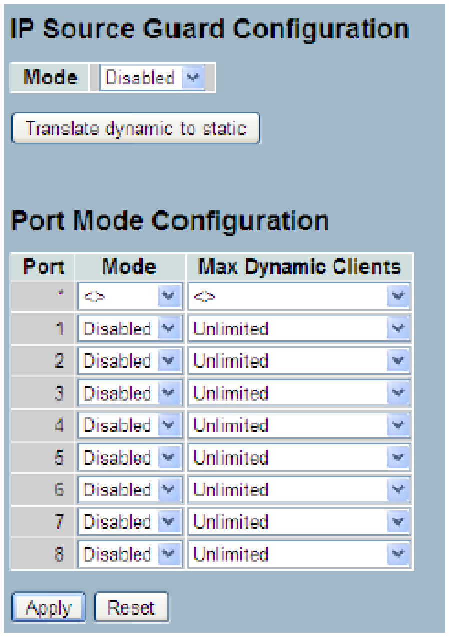
This page lets you configure IP Source Guard detail parameters on the switch. You can use IP Source Guard to enable or disable with each switch port.

4-1.1 Configuration

This section describes how to configure IP Source Guard setting including Mode and Maximum Dynamic Clients. To configure IP Source Guard in the web UI:

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 Maximum Dynamic Clients of the specific port in the Mode of Port Mode Configuration.
4. Click Save.

Figure 4-1.1: IP Source Guard Configuration



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

Parameter description:

IP Source Guard Configuration:

Mode : Check to enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.

Port Mode Configuration : Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.

Max Dynamic Clients : Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port.

Buttons:

Apply : Click to save changes.

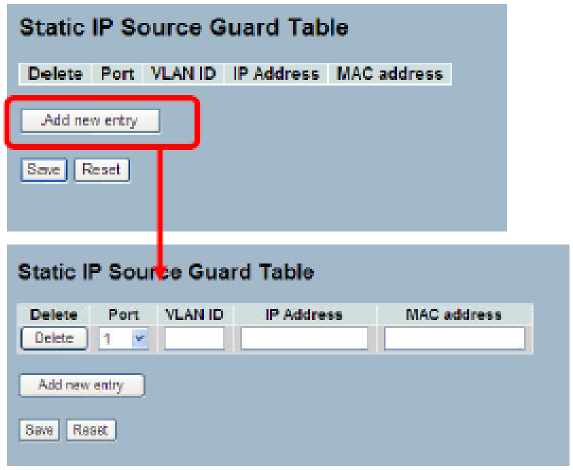
Reset : Click to undo any changes made locally and revert to previously saved values.

4-1.2 Static Table

This page lets you configure the Static IP Source Guard Table parameters of the switch. To configure Static IP Source Guard in the web UI:

1. Click “Add new entry”.
2. Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
3. Click Save.

Figure 4-1.2: Static IP Source Guard Table



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			

Parameter descriptions:

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

Port : The logical port for the settings.

VLAN ID : The vlan id for the settings.

IP Address : Allowed Source IP address.

IP Mask : It can be used for calculating the allowed network with IP address.

MAC address : Allowed Source MAC 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. Click "Save".

Buttons:

Save : Click to save changes.

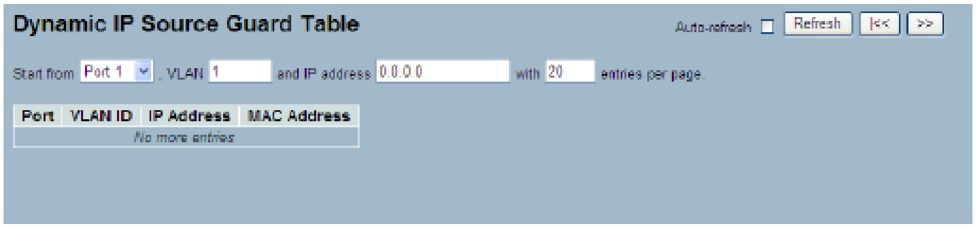
Reset : Click to undo any changes made locally and revert to previously saved values.

4-1.3 Dynamic Table

This page lets you configure and manage the Dynamic IP Source Guard Table parameters of the switch.
To configure Dynamic IP Source Guard Table parameters in the web UI:

1. Select Dynamic IP Source Guard Table.
2. Specify the Start from port, VLAN ID, IP Address, and entries per page.
3. Check "Auto-refresh" or click the Refresh button.

Figure 4-1.3: Dynamic IP Source Guird Table



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			

Parameter descriptions:

Port : Switch Port Number for which the entries are displayed.

VLAN ID : VLAN-ID in which the IP traffic is permitted.

IP Address : User IP address of the entry.

MAC Address : Source MAC address.

Buttons:

Auto-refresh : Check to auto-refresh the page information automatically.

Refresh : Click to refresh the Dynamic IP Source Guard Table manually.

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

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

4-2 ARP Inspection

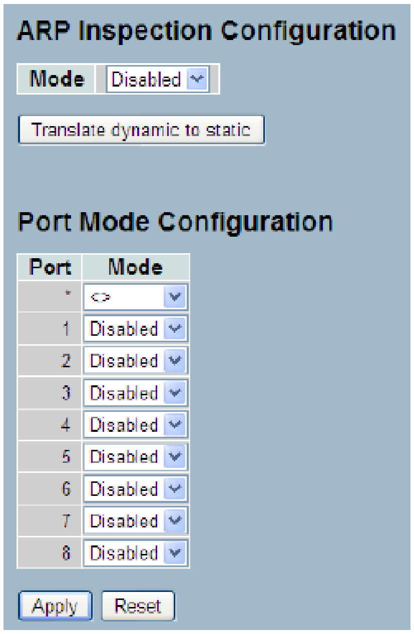
The section lets you configure and manage the ARP Inspection parameters of the switch.

4-2.1 Configuration

This page lets you configure ARP Inspection setting including Mode (Enabled and Disabled) and Port (Enabled and Disabled). To configure ARP Inspection in the web UI:

1. Select “Enabled” in the Mode of ARP Inspection Configuration.
2. Select “Enabled” of the specific port in the Mode of Port Mode Configuration.
3. Click Save.

Figure 4-2.1: ARP Inspection Configuration



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

Parameter descriptions:

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

Port Mode Configuration : Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port.

Buttons:

Apply : Click to save changes.

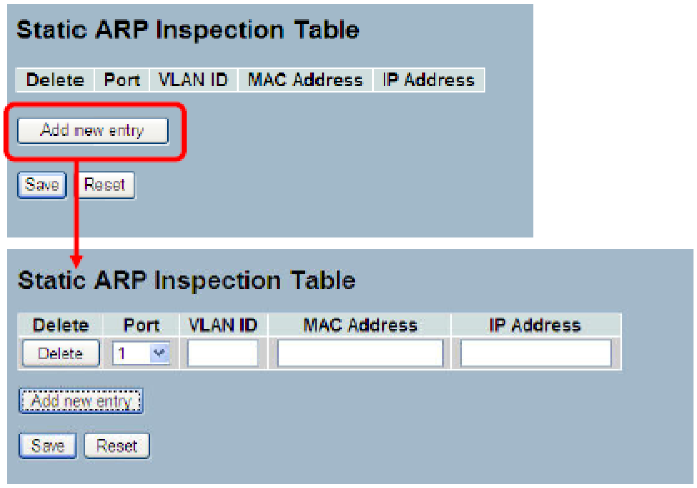
Reset : Click to undo any changes made locally and revert to previously saved values.

4-2.2 Static Table

This page lets you configure and manage Static ARP Inspection parameters of the switch. To configure Static ARP Inspection in the web UI:

1. Click “Add new entry”.
2. Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
3. Click Save.

Figure 4-2.2: Static ARP Inspection Table



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			

Parameter descriptions:

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

Port : Select the logical port for the settings.

VLAN ID : Enter the VLAN ID (VID) for the settings.

MAC Address : Enter an allowed Source MAC address in ARP request packets.

IP Address : Enter an allowed Source IP address in ARP request packets.

Buttons:

Add new entry : Click to add a new entry to the Static ARP Inspection table. Specify the parameters above for the each entry.

Save : Click to save changes.

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

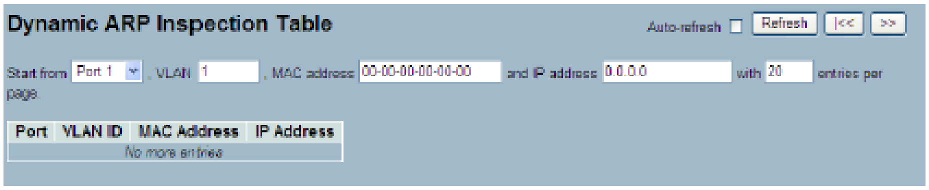
4-2.3 Dynamic Table

This page lets you configure Dynamic ARP Inspection parameters of the switch. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

To configure Dynamic ARP Inspection in the web UI:

1. Specify the Start from port, VLAN ID, MAC Address, IP Address, and entries per page.
2. Check "Auto-refresh".

Figure 4-2.3: Dynamic ARP Inspection Table



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			

Parameter descriptions:

Port : Switch Port Number for which the entries are displayed.

VLAN ID : VLAN-ID in which the ARP traffic is permitted.

MAC Address : User MAC address of the entry.

IP Address : User IP address of the entry.

Buttons:

Auto-refresh : Check the auto-refresh box to refresh the information automatically.

Refresh : Click to immediately refresh the page manually.

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

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

4-3 DHCP Snooping

The section describes how to configure the DHCP Snooping parameters of the switch. The DHCP Snooping can prevent attackers from adding their own DHCP servers to the network.

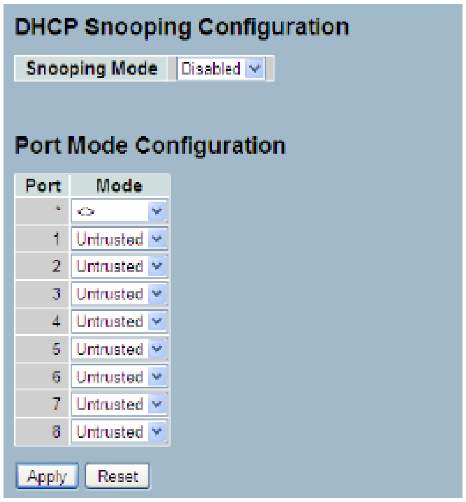
4-3.1 Configuration

This page lets you configure DHCP Snooping settings including Snooping Mode (Enabled and Disabled) and Port Mode Configuration (Trusted, Untrusted).

To configure DHCP Snooping in the web UI:

1. Select "Enabled" in the Mode of DHCP Snooping Configuration.
2. Select "Trusted" of the specific port in the Mode of Port Mode Configuration.
3. Click Save.

Figure 4-3.1: DHCP Snooping Configuration



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

Parameter descriptions:

Snooping Mode : Indicates the DHCP snooping mode operation. Possible modes are:

> ***Enabled***: Enable DHCP snooping mode operation. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.
>
> ***Disabled***: Disable DHCP snooping mode operation.

Port Mode : Indicates the DHCP snooping port mode. Possible port modes are:

> ***Trusted***: Configures the port as trusted source of the DHCP messages.
>
> ***Untrusted***: Configures the port as untrusted source of the DHCP messages.

Buttons:

Save : Click to save changes.

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

4-3.2 Statistics

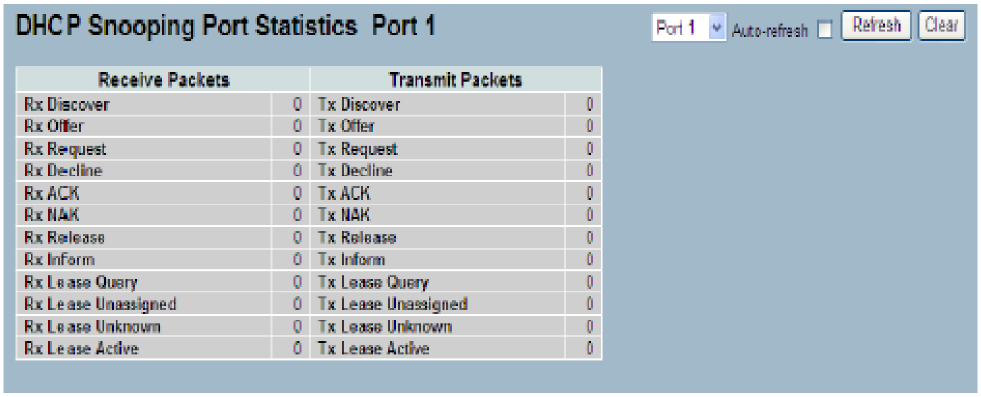
This page shows the DHCP Snooping Statistics information of the switch. The statistics show only packet counters when DHCP snooping mode is enabled and relay mode is disabled. And it doesn't count the DHCP packets for DHCP client.

To view DHCP Snooping Statistics in the web UI:

1. Specify the Port which you want to monitor.

2. Check “Auto-refresh” or click “Refresh” or “Clear”.

Figure 4-3.2: DHCP Snooping Port Statistics



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

Parameter descriptions:

Rx and Tx Discover : The number of discover (option 53 with value 1) packets received and transmitted.

Rx and Tx Offer : The number of offer (option 53 with value 2) packets received and transmitted.

Rx and Tx Request : The number of request (option 53 with value 3) packets received and transmitted.

Rx and Tx Decline : The number of decline (option 53 with value 4) packets received and transmitted.

Rx and Tx ACK : The number of ACK (option 53 with value 5) packets received and transmitted.

Rx and Tx NAK : The number of NAK (option 53 with value 6) packets received and transmitted.

Rx and Tx Release : The number of release (option 53 with value 7) packets received and transmitted.

Rx and Tx Inform : The number of inform (option 53 with value 8) packets received and transmitted.

Rx and Tx Lease Query : The number of lease query (option 53 with value 10) packets received and transmitted.

Rx and Tx Lease Unassigned : The number of lease unassigned (option 53 with value 11) packets received and transmitted.

Rx and Tx Lease Unknown : The number of lease unknown (option 53 with value 12) packets received and transmitted.

Rx and Tx Lease Active : The number of lease active (option 53 with value 13) packets received and transmitted.

Buttons:

Auto-refresh : Check to refresh page information automatically every 3 seconds.

Refresh : Click to immediately refresh Statistics manually.

Clear : Click to clear all entries.

4-4 DHCP Relay

This function sets the switch to forward DHCP requests to another specific DHCP servers via DHCP relay. The DHCP servers may be on another network.

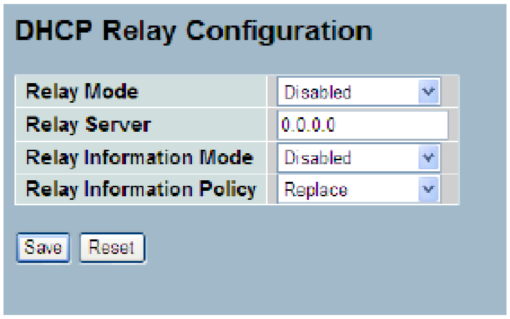
4-4.1 Configuration

This page lets you configure DHCP Relay setting including：Relay Mode (Enabled and Disabled), Relay Server IP setting, Relay Information Mode (Enabled and Disabled), and Relay Information Mode Policy (Replace, Keep and Drop).

To configure DHCP Relay in the web UI:

1. Select “Enabled” in the Relay Mode of DHCP Relay Configuration.
2. Specify Relay Server IP address.
3. Select “Enabled” in the Relay Information Mode of DHCP Relay Configuration.
4. Specify Relay (Replace, Keep and Drop) in the Relay Information Mode of DHCP Relay Configuration.
5. Click Save.

Figure 4-4.1: DHCP Relay Statistics



DHCP Relay Configuration

Relay Mode	Disabled
Relay Server	0.0.0.0
Relay Information Mode	Disabled
Relay Information Policy	Replace

Parameter descriptions:

Relay Mode : Indicates the DHCP relay mode operation. Possible modes are:

Enabled: Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.

Disabled: Disable DHCP relay mode operation.

Relay Server : Indicates the DHCP relay server IP address. 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 : Indicates the DHCP relay information mode option operation. Possible modes are:

Enabled: Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.

Disabled: Disable DHCP relay information mode operation.

Relay Information Policy : Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if agent receives a DHCP message that already contains relay agent information it will enforce the policy. And it only works under DHCP if relay information operation mode is enabled. Possible policies are:

Replace: Replace the original relay information when a DHCP message that already contains it is received.

Keep: Keep the original relay information when a DHCP message that already contains it is received.

Drop: Drop the package when a DHCP message that already contains relay information is received.

Buttons:

Save : Click to save changes.

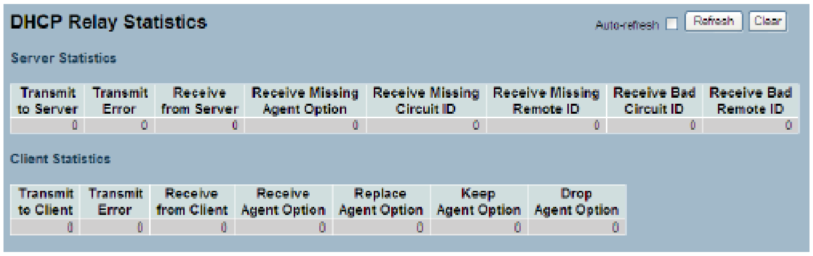
Reset : Click to undo any changes made locally and revert to previously saved values.

4-4.2 Statistics

This page shows DHCP Relay Statistics information of the switch. The statistics show both Server and Client packet counters when DHCP Relay mode is enabled. To view DHCP Snooping Statistics Configuration in the web UI:

1. Check “Auto-refresh”.

Figure 4-4.2: DHCP Relay Statistics



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

Parameter descriptions:

Server Statistics:

Transmit to Server : The number of packets that are relayed from client to server.

Transmit Error : The number of packets that resulted in errors while being sent to clients.

Receive from Server : The number of packets received from server.

Receive Missing Agent Option : The number of packets received without agent information options.

Receive Missing Circuit ID : The number of packets received with the Circuit ID option missing.

Receive Missing Remote ID : The number of packets received with the Remote ID option missing.

Receive Bad Circuit ID : The number of packets whose Circuit ID option did not match known circuit ID.

Receive Bad Remote ID : The number of packets whose Remote ID option did not match known Remote ID.

Client Statistics

Transmit to Client : The number of relayed packets from server to client.

Transmit Error : The number of packets that resulted in error while being sent to servers.

Receive from Client : The number of received packets from server.

Receive Agent Option : The number of received packets with relay agent information option.

Replace Agent Option : The number of packets which were replaced with relay agent information option.

Keep Agent Option : The number of packets whose relay agent information was retained.

Drop Agent Option : The number of packets that were dropped which were received with relay agent information.

Buttons:

Auto-refresh : Check to refresh page information automatically every 3 seconds.

Refresh : Click to manually refresh the DHCP Relay Statistics immediately.

Clear : Click to clear to the entries.

4-4 NAS

This section allows you to configure the NAS parameters of the switch. A 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.

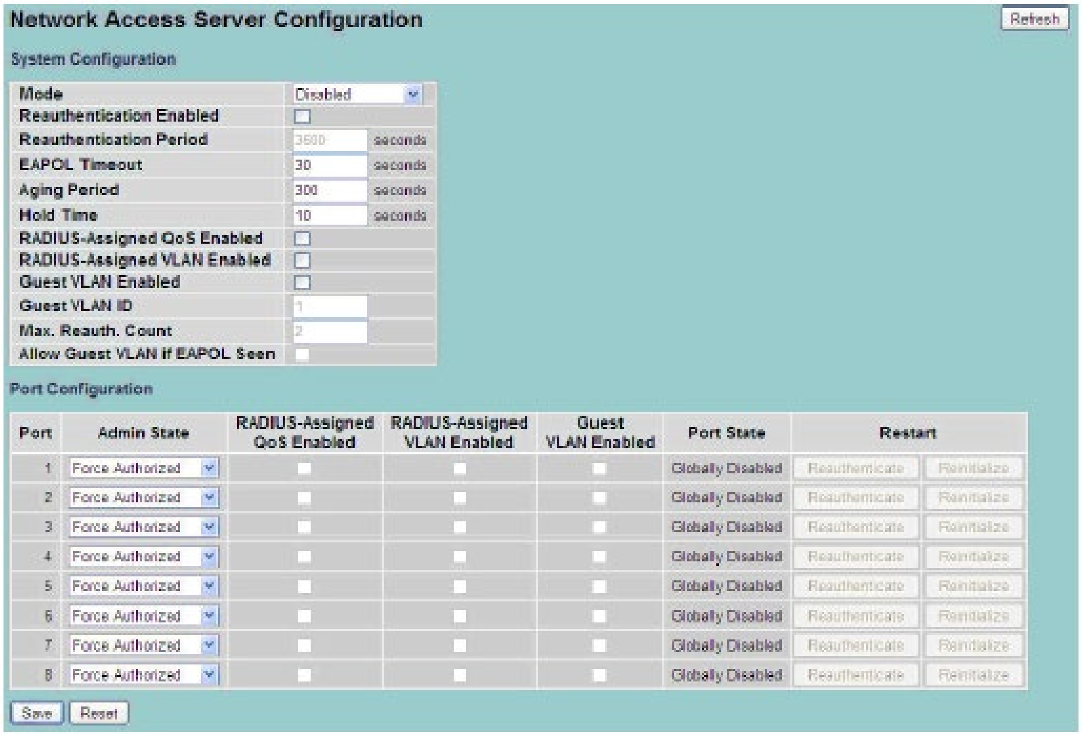
4-5.1 Configuration

This page lets you configure NAS settings of IEEE 802.1X, MAC-based authentication system, and port settings. The NAS configuration page has two sections, a system- and a port-wide.

To configure the System section in the web UI:

1. Select “Enabled” in the Mode of Network Access Server Configuration.
2. Checked Re-authentication Enabled.
3. Set Re-authentication Period (Default is 3600 seconds).
4. Set EAPOL Timeout (Default is 30 seconds).
5. Set Aging Period (Default is 300 seconds).
6. Set Hold Time (Default is 10 seconds).
7. Checked RADIUS-Assigned QoS Enabled.
8. Checked RADIUS-Assigned VLAN Enabled.
9. Checked Guest VLAN Enabled.
10. Specify Guest VLAN ID.
11. Specify Max. Reauth. Count.
12. Checked Allow Guest VLAN if EAPOL Seen.
13. Click Save.

Figure 4-5.1: Network Access Server Configuration



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	☐	

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

Parameter descriptions:

System Configuration section:

Mode : Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.

Reauthentication Enabled : If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached.

For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Aging Period below).

Re-authentication Period : Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.

EAPOL Timeout : Determine 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, i.e. modes using the Port Security functionality to secure MAC addresses:

- Single 802.1X
- Multi 802.1X
- MAC-Based Auth.

When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to 10 - 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, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.

Hold Time : This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:

- Single 802.1X
- Multi 802.1X
- MAC-Based Auth.

If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration > Security > AAA" page) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication.

In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time. The Hold Time can be set to a number between 10 and 1000000 seconds.

RADIUS-Assigned QoS Enabled : RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description)

The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.

RADIUS-Assigned VLAN Enabled : RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned VLAN Enabled below for a detailed description).

The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.

Guest VLAN Enabled : A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1Xunaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below.

The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.

Guest VLAN ID :

This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled. Valid values are 1 - 4095.

Max. Reauth. Count : The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled. Valid values are in the range [1; 255].

Allow Guest VLAN if EAPOL Seen : The switch remembers if an EAPOL frame has been received on the port for the 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 lifetime of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the 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 several columns:

Port : The port number for which the configuration below applies.

Admin State : If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:

> ***Force Authorized*** : In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.
>
> ***Force Unauthorized*** : In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.
>
> ***Port-based 802.1X*** : In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it. When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

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). Now, 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 on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And 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 port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really 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 port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really 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. Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module. In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port. The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.

MAC-based Auth.: Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xxxx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly. When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard. The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients 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 RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated.
If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class.
If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).
This option is only available for single-client modes, i.e.:

- Port-based 802.1X
- Single 802.1X

RADIUS attributes used in identifying a QoS Class:

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 IETF RFC 4675 forms the basis for identifying the QoS Class in an Access-Accept packet. Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:

- All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '3', which translates into the desired QoS Class in the range [0; 3].

RADIUS-Assigned VLAN Enabled : When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated.
If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID.
If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).
This option is only available for single-client modes, i.e.

- Port-based 802.1X
- Single 802.1X

For 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 fulfil the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag):
  - Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6).
  - Value of Tunnel-Type must be set to "VLAN" (ordinal 13).
  - Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].

Guest VLAN Enabled : When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below. This option is only available for EAPOL-based modes, i.e.:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

For 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 in the meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.
Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.
While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.

Port State : The current state of the port. It can undertake one of the following values:
Globally Disabled: NAS is globally disabled.
Link Down: NAS is globally enabled, but there is no link on the port.
Authorized: The port is in Force Authorized 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.
Re-authenticate*:* Schedules a re-authentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, re-authentication will be attempted immediately. The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.
Reinitialize: Forces a re-initialization 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.

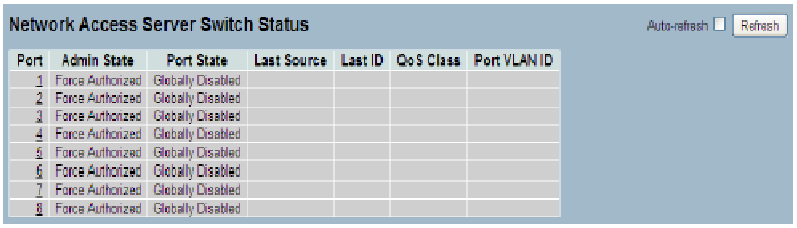
Buttons:
Save : Click to save changes.
Reset : Click to undo any changes made locally and revert to previously saved values.
Refresh : Click to refresh the NAS Configuration manually.

4-5.2 Switch Status

This page shows NAS status information for each port of the switch. The status includes Admin State Port State, Last Source, Last ID, QoS Class, and Port VLAN ID. To show NAS Switch Status Configuration in the web UI:

1. Navigate to the NAS Switch Status Configuration page.
1. Check “Auto-refresh”.

Figure 4-5.2: Network Access Server Switch Status



Network Access Server Switch Status

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled				
2	Force Authorized	Globally Disabled				
3	Force Authorized	Globally Disabled				
4	Force Authorized	Globally Disabled				
5	Force Authorized	Globally Disabled				
6	Force Authorized	Globally Disabled				
7	Force Authorized	Globally Disabled				
8	Force Authorized	Globally Disabled				

Parameter descriptions:

Port : The switch port number. Click to navigate to detailed NAS statistics for this port.

Admin State : The port's current administrative state. Refer to NAS Admin State for a description of possible values.

Port State : The current state of the port. Refer to NAS Port State for a description of the individual states.

Last Source : The source MAC address carried in the most recently received EAPOL frame for EAPOLbased authentication, and the most recently received frame from a new client for MACbased authentication.

Last ID : The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

QoS Class : QoS Class assigned to the port by the RADIUS server if enabled.

Port VLAN ID : The VLAN ID that NAS has put the port in. The field is blank if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.

Buttons:

Auto-refresh : Click to auto-refresh page information automatically.

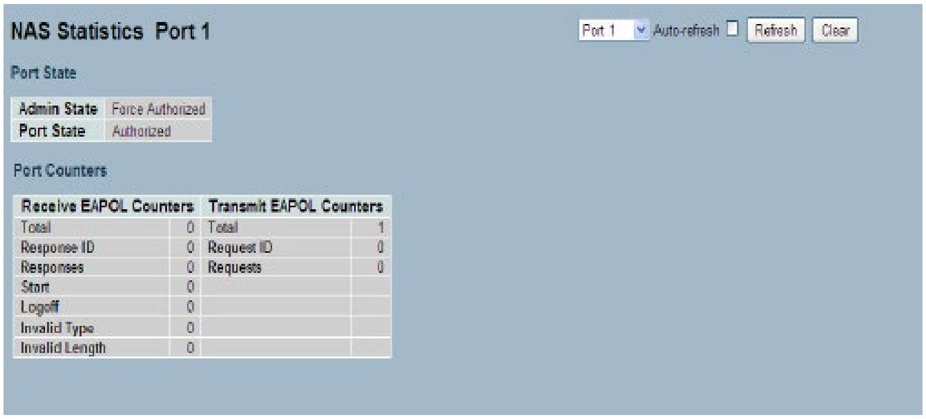
Refresh : Click to refresh the NAS Switch Status manually.

4-5.3 Port Status

This page provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. To view NAS Port Status in the web UI:

1. Specify the Port which you want to check.
2. Check “Auto-reflash” or “Refresh”.

Figure 4-5.3: NAS Statistics



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		

Parameter descriptions:

Port State

Admin State : The port's current administrative state. Refer to NAS Admin State for a description of possible values.

Port State : The current state of the port. Refer to NAS Port State for a description of the individual states.

QoS Class : The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.

Port VLAN ID : The VLAN ID that NAS has put the port in. The field is blank if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.

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 these admin states:

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

Last Supplicant/Client Info : 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 : 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 MACbased 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.

Buttons:

Last Authentication : Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

Auto-refresh : Click to refresh the information automatically every 3 seconds.

Refresh : Click to immediately refresh page information manually.

Clear : Click to clear all NAS Statistics entries.

4-6 AAA

This section shows you how to use an AAA (Authentication, Authorization, Accounting) server to provide access control to your 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 page lets you configure AAA setting of TACACS+ or RADIUS server. To configure a Common Configuration of AAA in the web UI:

1. Set Timeout (Default is 15 seconds).
2. Set Dead Time (Default is 300 seconds).

To configure TACACS+ Authorization and Accounting of AAA in the web UI:

1. Select “Enabled” in the Authorization.
2. Select “Enabled” in the Failback to Local Authorization.
3. Select “Enabled” in the Account.

To configure RADIUS Authentication Server Configuration of AAA in the web UI:

1. Check “Enabled”.
2. Specify IP address or Hostname for Radius Server.
3. Specify Authentication Port for Radius Server (Default is 1812).
4. Specify the Secret with Radius Server.

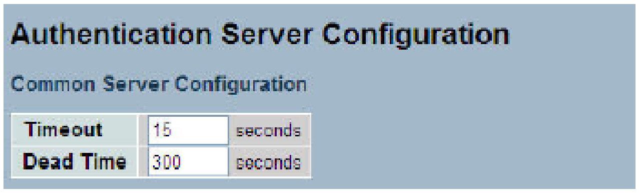
To configure RADIUS Accounting Server Configuration of AAA in the web UI:

1. Check “Enabled”.
2. Specify IP address or Hostname for Radius Server.
3. Specify Accounting Port for Radius Server (Default is 1813).
4. Specify the Secret with Radius Server.

To configure TACACS+ Authentication Server Configuration of AAA in the web interface:

1. Check “Enabled”.
2. Specify IP address or Hostname for TACACS+ Server.
3. Specify Authentication Port for TACACS+ Server (Default is 49).
4. Specify the Secret with TACACS+ Server.

Figure 4-5.3.1: Common Server Configuration

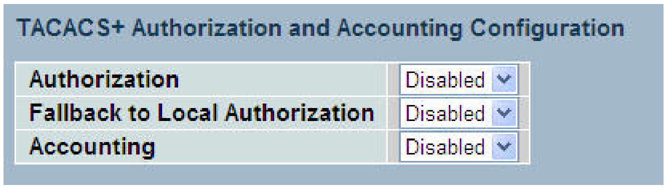


Authentication Server Configuration

Common Server Configuration

Timeout	15	seconds
Dead Time	300	seconds

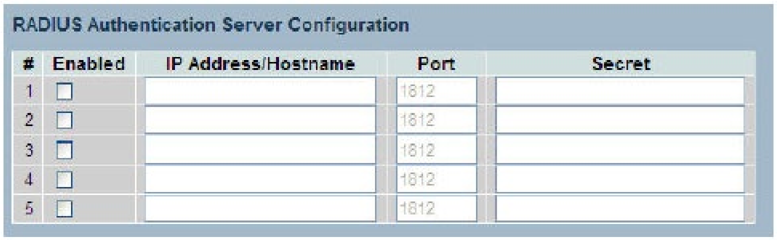
Figure 4-5.3.2: TACACS+ Accounting Configuration



TACACS+ Authorization and Accounting Configuration

Authorization	Disabled
Fallback to Local Authorization	Disabled
Accounting	Disabled

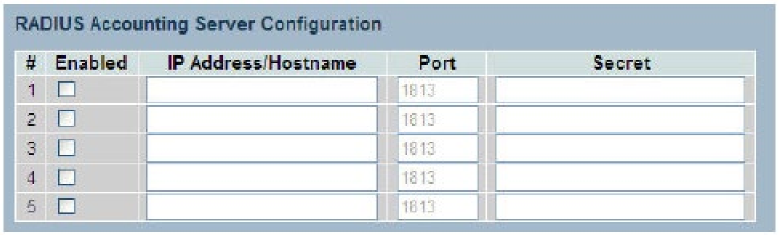
Figure 4-5.3.3: RADIUS Configuration



RADIUS Authentication Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	□		1812	
2	□		1812	
3	□		1812	
4	□		1812	
5	□		1812	

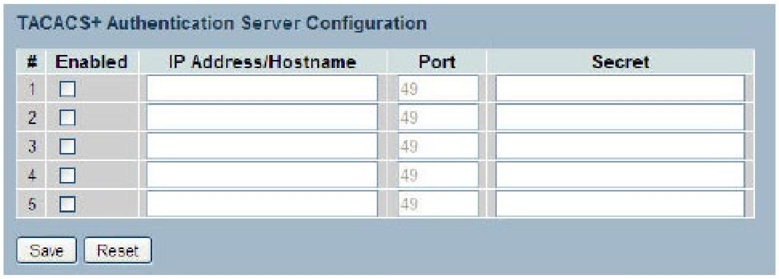
Figure 4-5.3.4: RADIUS Accounting Configuration



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: TACACS+ Authentication Configuration



TACACS+ Authentication Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	□		49	
2	□		49	
3	□		49	
4	□		49	
5	□		49	

Parameter descriptions:

Timeout : The Timeout, which can be set to a number between 3 and 3600 seconds, is the maximum time to wait for a reply from a server. 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, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

RADIUS Authentication Server Configuration: The table has one row for each RADIUS Authentication Server and a number of columns, which are:

:The RADIUS Authentication Server number for which the configuration below applies.

Enabled : Enable the RADIUS Authentication Server by checking this box.

IP Address/Hostname : The IP address or hostname of the RADIUS Authentication Server. IP address is expressed in dotted decimal notation.

Port : 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 : 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:

: The RADIUS Accounting Server number for which the configuration below applies.

Enabled : Enable the RADIUS Accounting Server by checking this box.

IP Address/Hostname : The IP address or hostname of the RADIUS Accounting Server. IP address is expressed in dotted decimal notation.

Port : 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 : 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:

: The TACACS+ Authentication Server number for which the configuration below applies.

Enabled : Enable the TACACS+ Authentication Server by checking this box.

IP Address/Hostname : The IP address or hostname of the TACACS+ Authentication Server. IP address is expressed in dotted decimal notation.

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

4-6.2 Radius Overview

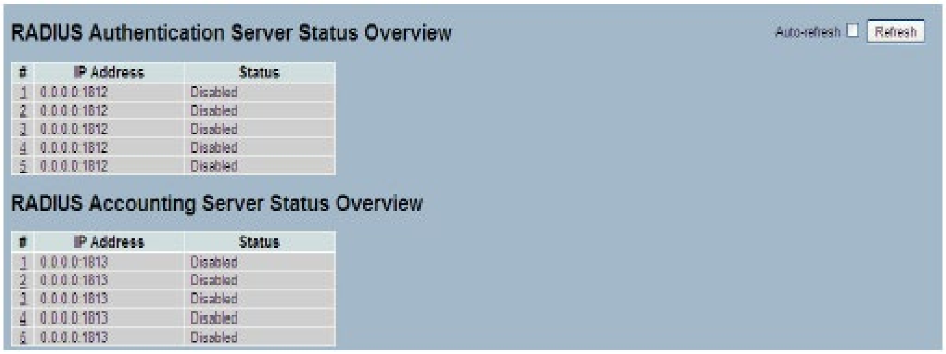
This section shows you an overview of the RADIUS Authentication and Accounting servers status to ensure the function is workable.

To view RADIUS Overview Configuration in the web UI:

1. Navigate to the RADIUS Overview Configuration page.

1. Check “Auto-refresh” or “Refresh”.

Figure 4-6.2: RADIUS Authentication Server Status Overview



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

Parameter descriptions:

RADIUS Authentication Servers

: The RADIUS server number. Click to navigate to detailed statistics for this server.

IP Address : The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

State : 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

: The RADIUS server number. Click to navigate to detailed statistics for this server.

IP Address : The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

State : 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 reenabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Buttons:

Auto-refresh : To evoke the auto-refresh icon then the device will refresh the information automatically.

Refresh : Click to refresh the RADIUS Status manually.

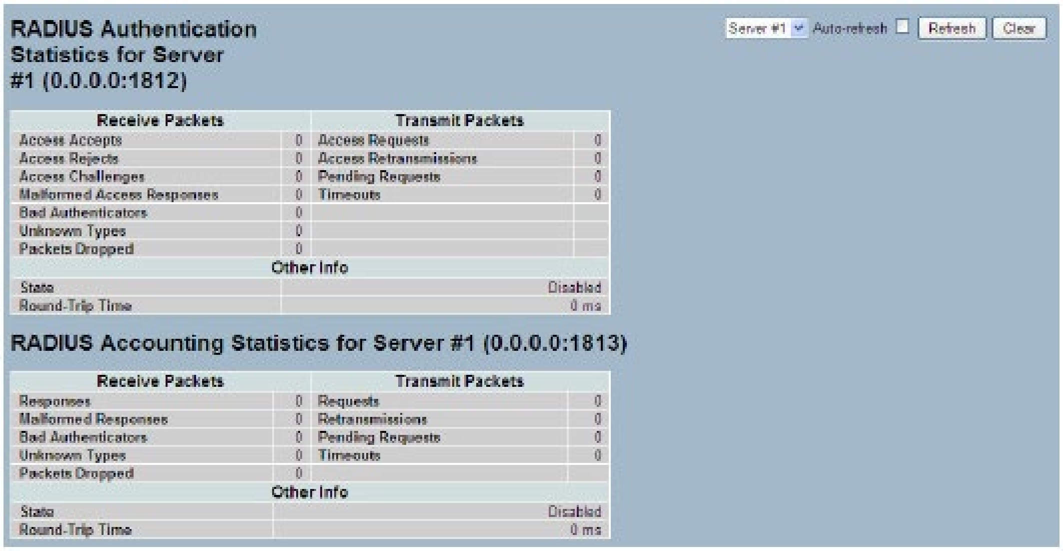
4-6.3 Radius Details

This page shows detailed statistics of the RADIUS Authentication and Accounting servers. The statistics map closely to those specified in IETF RFC 4668 - RADIUS Authentication Client MIB.

To view RADIUS Details in the web UI:

1. Specify which Server you want to check.
2. Check “Auto-refresh”, “Refresh” or “Clear”..

Figure 4-6.3: RADIUS Authentication Statistics Server



RADIUS Authentication Statistics for Server #1 (0.0.0.0:1812)

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			
State			Disabled
Round-Trip Time			0 ms

RADIUS Accounting Statistics for Server #1 (0.0.0.0:1813)

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			
State			Disabled
Round-Trip Time			0 ms

Parameter descriptions:

RADIUS Authentication Statistics for Server #x: For the selected RADIUS server, displays data on Receive Packets, Transit Packets, and Other Info.

RADIUS Accounting Statistics for Server #x: For the selected RADIUS server, displays data on Receive Packets, Transit Packets, and Other Info.

Buttons:

Auto-refresh : Click to refresh the information automatically.

Refresh : Click to immediately refresh the information manually.

Clear : Click to clear the RADIUS Statistics information.

4-7 Port Security

This section shows you to configure the Port Security settings of the Switch. You can use the Port Security feature to restrict input to an interface by limiting and identifying MAC addresses.

4-7.1 Limit Control

This page lets to configure the Port Security settings of the Switch. You can use the Port Security feature to restrict input to an interface by limiting and identifying MAC addresses.

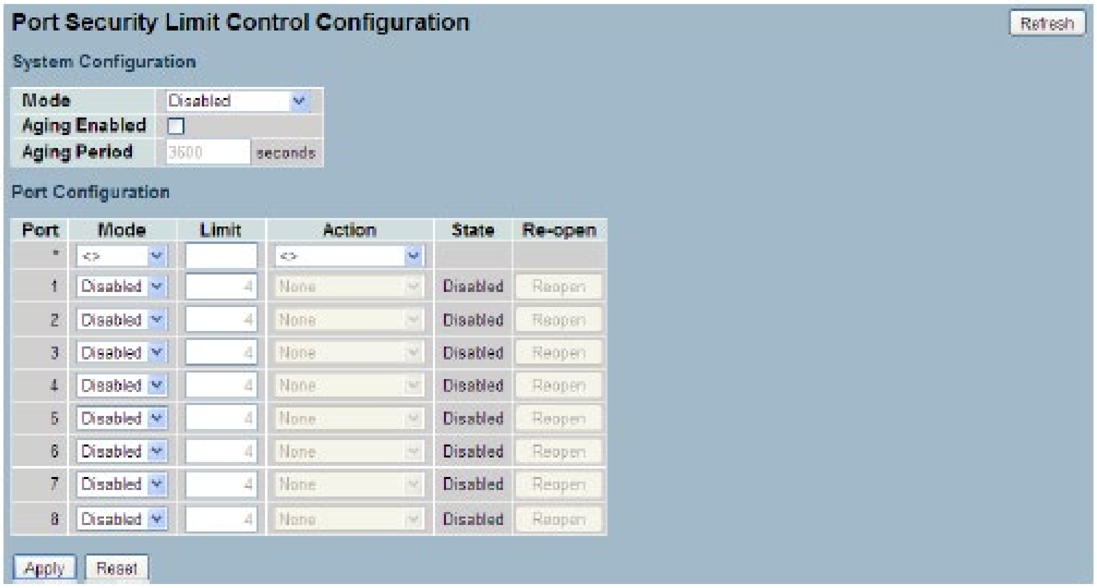
To configure System Configuration of Limit Control in the web UI:

1. Select "Enabled" in the Mode of System Configuration.
2. Checked Aging Enabled.
3. Set Aging Period (default is 3600 seconds).

To configure Port Configuration of Limit Control in the web UI:

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 Action (Trap, Shutdown, or Trap & Shutdown).
4. Click Save.

Figure 4-7.1: Port Security Limit Control Configuration



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

Parameter descriptions:

System Configuration

Mode : Indicated if Limit Control is globally enabled or disabled on the switch. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.

Aging Enabled : If checked, secured MAC addresses are subject to aging as discussed under Aging Period .

Aging Period : If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality.

The Aging Period can be set to a number between 10 and 10,000,000 seconds. To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Port Configuration: The table has one row for each port on the selected switch and a number of columns,

which are:

Port : The port number to which the configuration below applies.

Mode : Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.

Limit : The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken. The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

Action : If Limit is reached, the switch can take one of the following actions:

None: Do not allow more than Limit MAC addresses on the port, but take no further action.

Trap: If Limit + 1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded.

Shutdown: If Limit + 1 MAC addresses is seen on the port, shut 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 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: Limit Control is either globally disabled or disabled on the port.

Ready: The limit is not yet reached. This can be shown for all actions.

Limit Reached: Indicates that the limit is reached on this port. This state can only be shown if Action is set to None or Trap.

Shutdown: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap & Shutdown.

Buttons:

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

Refresh : Click to refresh the Port Security information manually.

Save : Click to save changes.

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

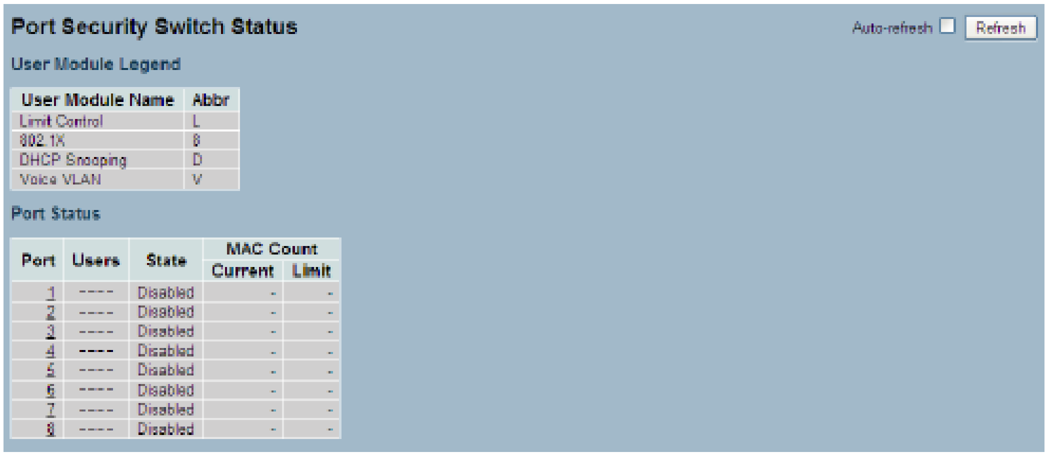
4-7.2 Switch Status

This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise. The status page is divided into two sections - one with a legend of user modules and one with the actual port status.

To view Port Security Switch Status in the web UI:

1. Navigate to the Port Security Switch Status webpage.
2. Check "Auto-reflash".

Figure 4-7.2: 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	-	-

Parameter descriptions:

User Module Legend : The legend shows all user modules that may request Port Security services.

User Module Name : The full name of a module that may request Port Security services.

Abbr : A one-letter abbreviation of the user module. This is used in the Users column in the port status table.

Port Status : The table has one row for each port on the selected switch and a number of columns, which are:

Port : The port number for which the status applies. Click the port number to see the status for this particular port.

Users : Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.

State : Shows the current state of the port, It can take one of four values:

Disabled: No user modules are currently using the Port Security service.

Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.

Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.

Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control Configuration webpage.

MAC Count (Current, Limit) : The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively. If no user modules are enabled on the port, the Current column will show a dash (-). If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-). Indicates the number of currently learned MAC addresses (forwarding as well as blocked) on the port. If no user modules are enabled on the port, a dash (-) will be shown.

Buttons:

Auto-refresh : Check the auto-refresh box automatically refresh page information.

Refresh : Click to immediately refresh page information manually.

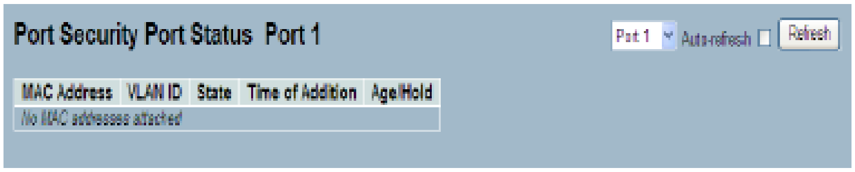
4-7.3 Port Status

This page shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

To view Port Security Switch Status in the web UI:

1. Specify the Port which you want to monitor.
2. Check “Auto-refresh”.

Figure 4-7.3: Port Security Port Status



Port Security Port Status Port 1

MAC Address	VLAN ID	State	Time of Addition	Age/Hold
No MAC addresses attached				

Parameter descriptions:

MAC Address & VLAN ID : The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.

State : Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.

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

Age/Hold : If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin. If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

Auto-refresh : Check the auto-refresh box to refresh page information automatically every 3 seconds.

Refresh : Click to immediately refresh the Port Security Port Status information manually.

4-8 Access Management

This section lets you configure the access management table of the Switch including HTTP/HTTPS, SNMP, and TELNET/SSH. You can manage the Switch over an Ethernet LAN, or over the Internet.

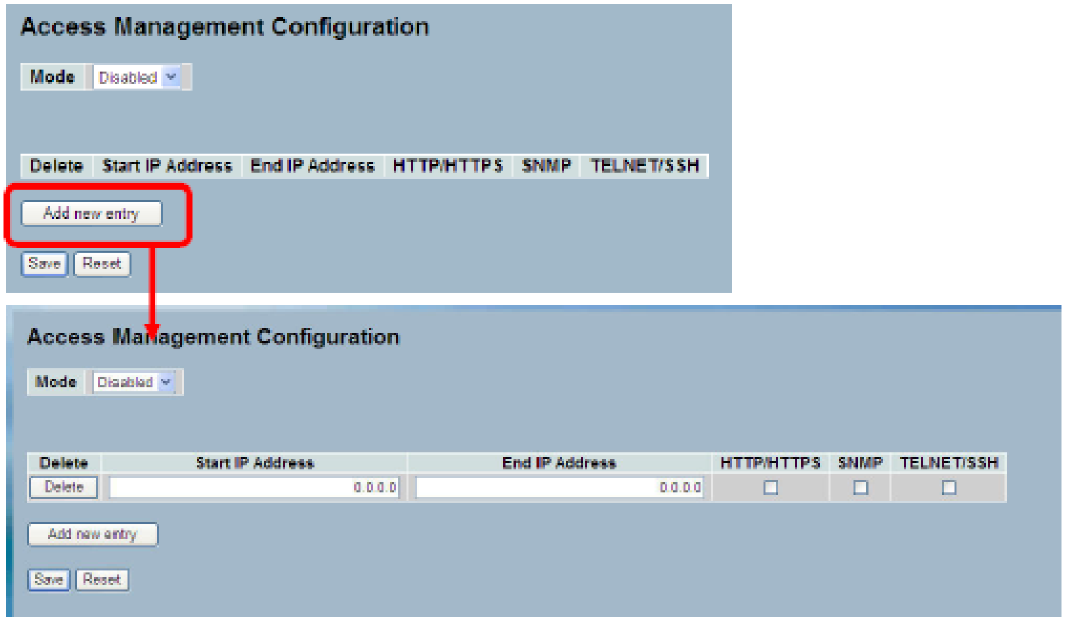
4-8.1 Configuration

This page lets you configure access management table of the Switch. 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.

To configure Access Management in the web UI:

1. Select “Enabled” in the Mode of Access Management Configuration.
2. Click “Add new entry”.
3. Specify the Start IP Address, End IP Address.
4. Checked Access Management method (HTTP/HTTPS, SNMP, and TELNET/SSH) in the entry.
5. Click Save.

Figure 4-8.1: Access Management Configuration



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	□	□	□

Parameter descriptions:

Mode : Indicate the access management mode operation. Possible modes are:

Enabled: Enable access management mode operation.

Disabled: Disable access management mode operation.

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

Start IP address : Indicate the start IP address for the access management entry.

End IP address : Indicate the end IP address for the access management entry.

HTTP/HTTPS : Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.

SNMP : Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.

TELNET/SSH : Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.

Buttons:

Add new entry: Click to add a new row to the table.

Save – Click to save changes.

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

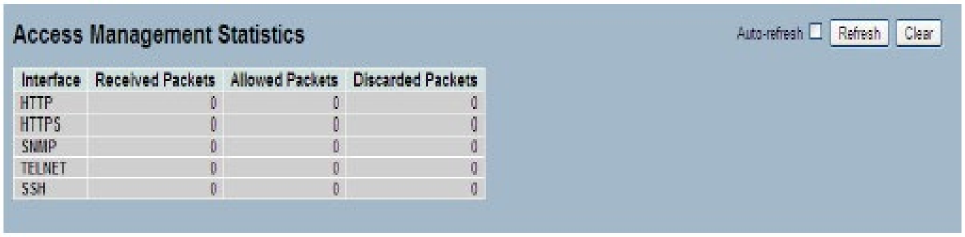
4-8.2 Statistics

This page shows detailed statistics of the Access Management including HTTP, HTTPS, SSH. TELNET, and SSH.

To view Access Management Statistics in the web UI:

1. Navigate to the Access Management Statistics page.
2. Check “Auto-refresh” or click “Refresh”.

Figure 4-8.2: Access Management Statistics



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

Parameter descriptions:

Interface : The interface type through which the remote host can access the switch.

Received Packets : Number of received packets from the interface when access management mode is enabled.

Allowed Packets : Number of allowed packets from the interface when access management mode is enabled.

Discarded Packets. : Number of discarded packets from the interface when access management mode is enabled.

Buttons:

Auto-refresh : Click to refresh page information automatically every 3 seconds.

Refresh : Click to immediately refresh the page manually.

Clear : Click to clear all entries.

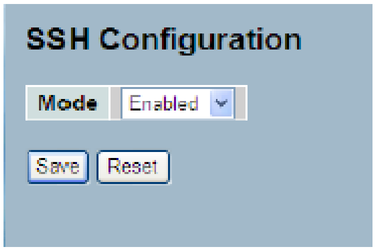
4-9 SSH

This page lets you use 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.

To configure SSH in the web UI:

1. Select "Enabled" in the Mode of SSH Configuration.
2. Click Save.

Figure 4-9.1: SSH Configuration



SSH Configuration

Mode: Enabled

Parameter descriptions:

Mode : Indicates the SSH mode operation. Possible modes are:

Enabled: Enable SSH mode operation.

Disabled: Disable SSH mode operation.

Buttons:

Save : Click to save changes.

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

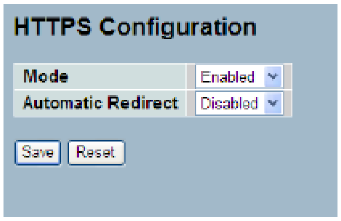
4-10 HTTPs

This page lets you use 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.

To configure HTTPS in the web UI:

1. Select “Enabled” in the Mode of HTTPS Configuration.
2. Select “Enabled” in the Automatic Redirect of HTTPS Configuration.
3. Click Save.

Figure 4-10.1: HTTPS Configuration



HTTPS Configuration

Mode	Enabled
Automatic Redirect	Disabled

Parameter descriptions:

Mode : Indicates the HTTPS mode operation. Possible modes are:

Enabled: Enable HTTPS mode operation.

Disabled: Disable HTTPS mode operation.

Automatic Redirect : Indicates the HTTPS redirect mode operation. Automatically redirect web browser to HTTPS when HTTPS mode is enabled. Possible modes are:

Enabled: Enable HTTPS redirect mode operation.

Disabled: Disable HTTPS redirect mode operation.

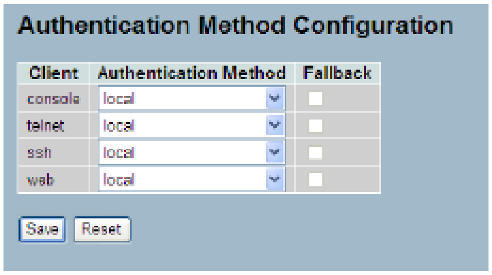
4-11 Auth Method

This page shows how to configure a user with authenticated when he logs into the switch via one of the management client interfaces.

To configure Authentication Method in the web UI:

1. Specify the Client (console, telnet, ssh, or web) which you want to monitor.
2. Specify the Authentication Method (none, local, radius, or tacacs+).
3. Checked Fallback.
4. Click Save.

Figure 4-11.1: HTTPS Configuration



Authentication Method Configuration

Client	Authentication Method	Fallback
console	local	□
telnet	local	□
ssh	local	□
web	local	□

Parameter descriptions:

Client : The management client for which the configuration below applies.

Authentication Method : The Authentication Method can be set to one of these values:

none : authentication is disabled and login is not possible.

local : use the local user database on the switch for authentication.

radius : use a remote RADIUS server for authentication.

tacacs+ : use a remote TACACS+ server for authentication.

Fallback : Enable fallback to local authentication by checking this box. 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 undo any changes made locally and revert to previously saved values.

Chapter 5. Maintenance

This chapter describes the switch Maintenance configuration tasks to enhance the performance of local network including Restart Device, Firmware upgrade, Save/Restore, Import/Export, and Diagnostics.

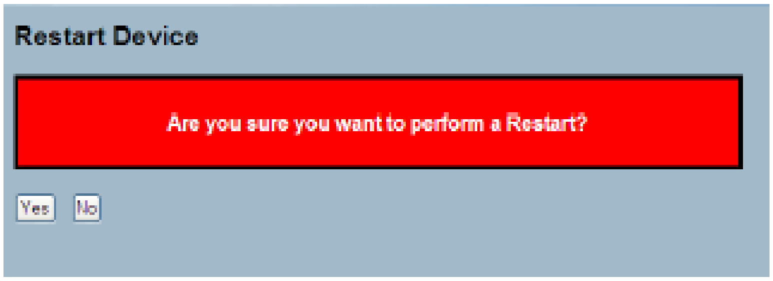
5-1 Restart Device

This section describes how to restart switch for any maintenance needs. Any configuration files or scripts that you saved in the switch should still be available afterwards.

To configure a Device Restart in the web UI:

1. Click Restart Device.
2. At the confirmation prompt click Yes.

Figure 5-1.1: Restart Device



Restart Device

Are you sure you want to perform a Restart?

Parameter descriptions:

Restart Device : Click to restart the switch. After restart, the switch will boot normally.

Buttons:

Yes : Click to restart the device.

No : Click to undo any restart action.

5-2 Firmware

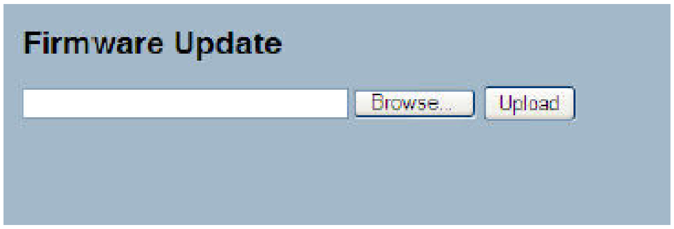
This section lets you upgrade the switch firmware and switch firmware versions.

5-2.1 Firmware Upgrade

This page lets you upgrade the switch firmware with more value-added functions. To upgrade switch firmware in the web UI:

1. Click the Browse… button and browse to and select a firmware file to upgrade the switch to.
2. Click the Upload button.

Figure 5-2.1: Firmware Update



Parameter descriptions:

Browse… : Click the button to search the firmware URL and filename.

Upload : Click the “Upload” button to start the firmware upload from the stored location on your PC or Server.

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

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

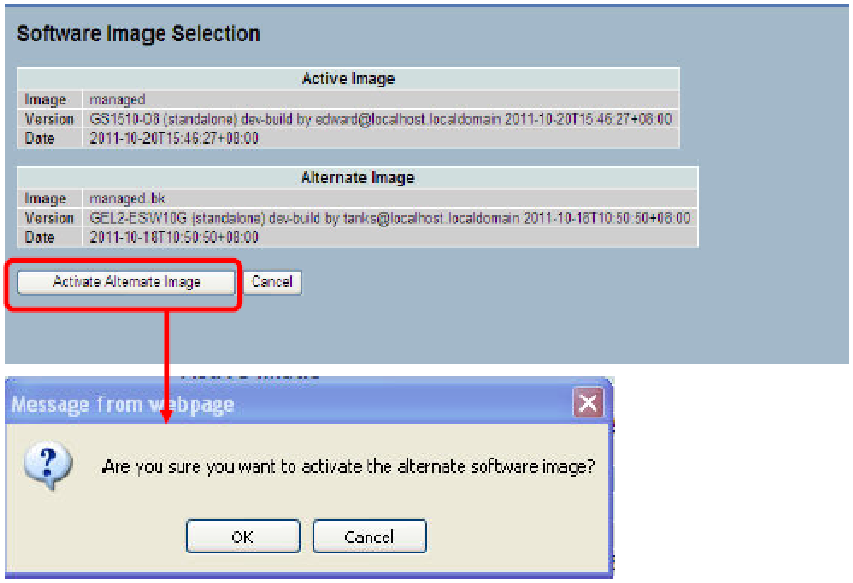
5-2.2 Firmware Selection

The switch supports dual images for firmware redundancy purposes. You can select which firmware image for your device's start firmware or operating firmware. This page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image.

To configure a Firmware Selection in the web UI:

1. Click Activate Alternate Image.
2. Click OK to complete firmware selection.

Figure 5-2.2: Firmware Selection



Software Image Selection

Active Image	
Image	managed
Version	GS1510-O8 (standalone) dev-build by edward@localhost.localdomain 2011-10-20T15:46:27+08:00
Date	2011-10-20T15:46:27+08:00

Alternate Image	
Image	managed.bk
Version	GEL2-ESW10G (standalone) dev-build by tanks@localhost.localdomain 2011-10-18T10:50:50+08:00
Date	2011-10-18T10:50:50+08:00

Message from webpage

Are you sure you want to activate the alternate software image?

Parameter descriptions:

Activate Alternate Image : Click to use the alternate image. This button may be disabled depending on system state.

Cancel: Click to cancel activating the backup image. Navigates away from this page.

Image : The flash index name of the firmware image. The name of primary (preferred) image is *image*, the alternate image is named *image.bk*.

Version : The version of the firmware image.

Date : The date where the firmware was produced.

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

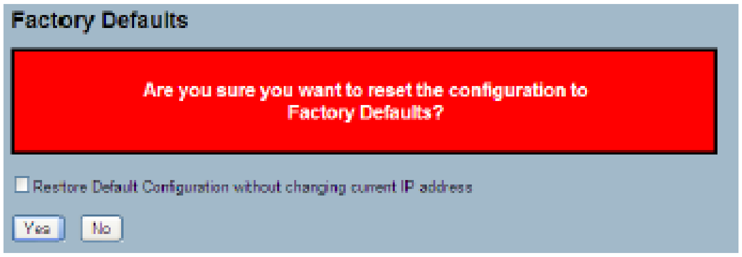
This section lets you save and restore the Switch configuration including reset to Factory Defaults, Save Start, Save Users, and Restore Users for any maintenance needs.

5-3.1 Factory Defaults

This page lets you reset the Switch configuration to Factory Defaults. Any configuration files or scripts will recover to factory default values. To perform a reset to factory defaults in the web UI:

1. Click Factory Defaults.
2. Click Yes.

Figure 5-3.1: Factory Defaults



Factory Defaults

Are you sure you want to reset the configuration to Factory Defaults?

□ Restore Default Configuration without changing current IP address

Parameter descriptions:

Buttons:

Yes : Click to “Yes” button to reset the configuration to Factory Defaults..

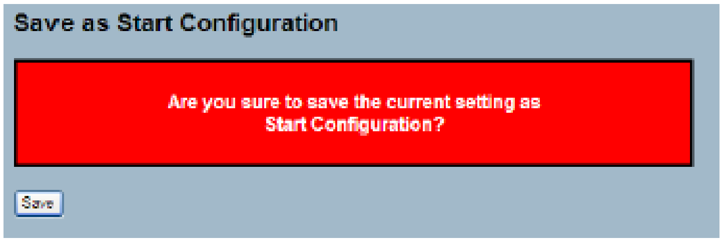
No : Click to return to the Port State page without resetting the configuration.

5-3.2 Save Start

This page lets you save the Switch Start configuration. Any current configuration files will be saved as XML format. To perform a Save Start Configuration in the web UI:

1. Click Save Start.
2. At the confirmation prompt click the Save button.

Figure 5-3.2: Save Start configuration



Save as Start Configuration

Are you sure to save the current setting as Start Configuration?

Parameter descriptions:

Buttons:

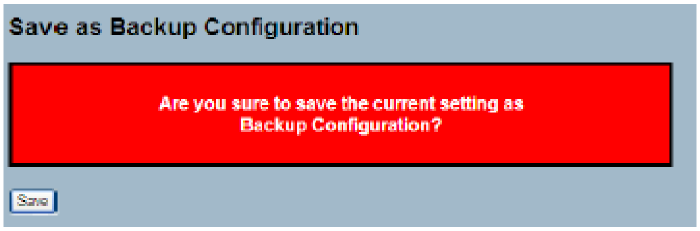
Save : Click the button to save current setting as Start Configuration.

5-3.3 Save User

This page lets you save users information. Any current configuration files will be saved in XML format. To perform a Save User operation in the web UI:

1. Click Save User.
2. Click Yes.

Figure 5-3.3: Save as Backup Configuration



Save as Backup Configuration

Are you sure to save the current setting as Backup Configuration?

Parameter descriptions:

Buttons:

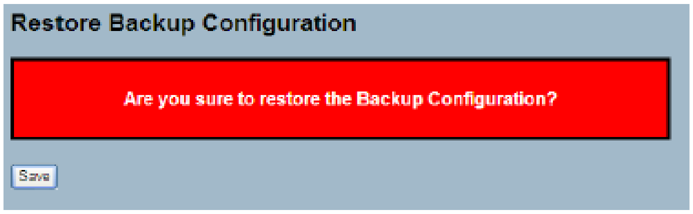
Save : Click the “Save” button to save current setting as Backup Configuration.

5-3.4 Restore User

This page lets you restore users information back to the switch. Any current configuration files will be restored via XML format. To perform a Restore User operation in the web UI:

1. Click Restore User.
2. Click Save.

Figure 5-3.4: Restore Backup Configuration



Restore Backup Configuration

Are you sure to restore the Backup Configuration?

Parameter descriptions:

Buttons:

Save : Click the “Save” button to restore the Backup Configuration to the switch.

5-4 Export / Import

This section describes how to export and import the Switch configuration. Any current configuration files will be exported in XML format.

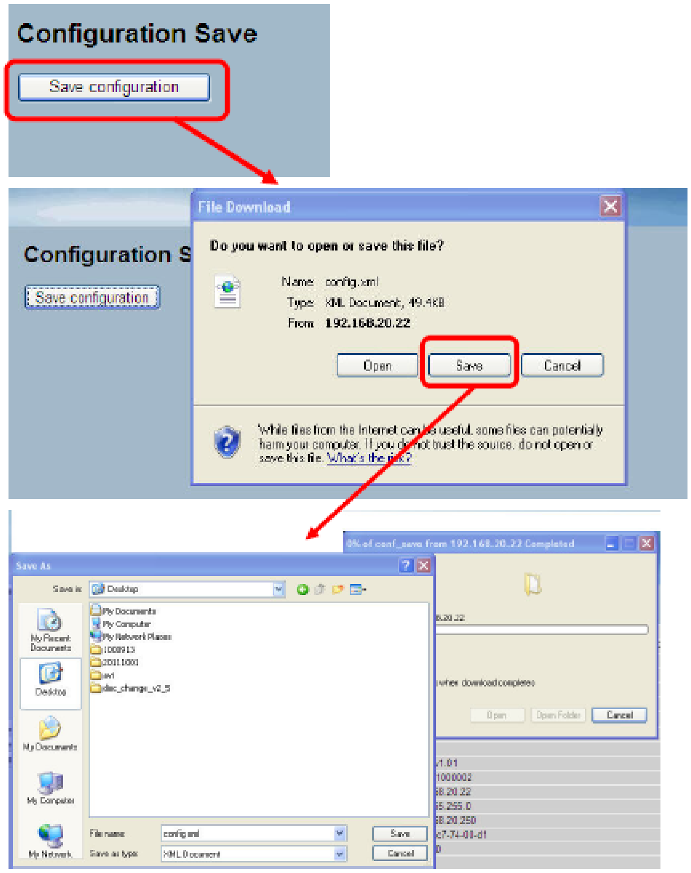
5-4.1 Export Config

This page lets you export the Switch configuration for maintenance needs. Any current configuration files will be exported in XML format.

To perform an Export Config operation in the web UI:

1. Click Save configuration.
2. Save the file in your device.

Figure 5-4.1: Restore the Backup Configuration



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?

File name: config.xml
Save as type: XML Document

Parameter descriptions:

Save : Click the “Save” button to store the Configuration to the PC or Server.

5-4.2 Import Config

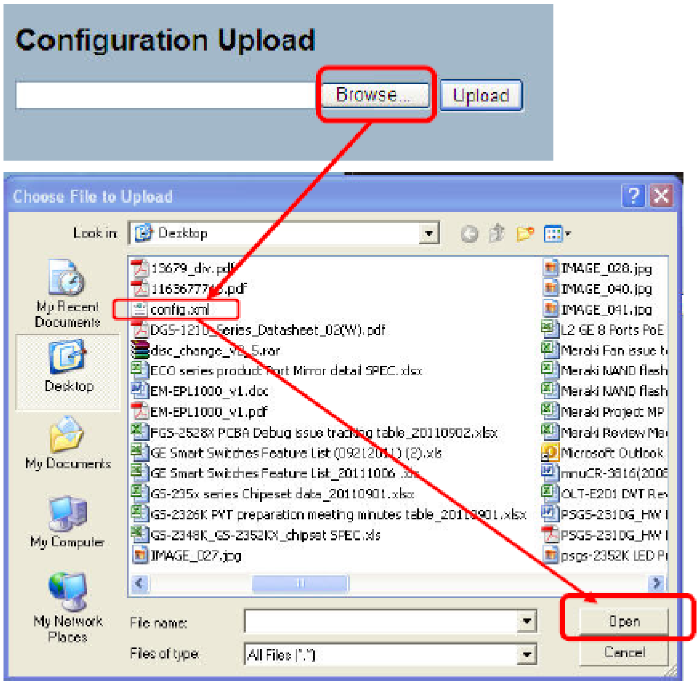
This page lets you import the Switch Configuration for maintenance needs. Any current configuration files will be exported in XML format.

Web Interface

To configure an Import Config Configuration in the web interface:

1. Click Browser to select the config file in your device.
2. Click Upload.

Figure 5-4.2: The Import Config



Parameter descriptions:

Browse : Click the “Browse...” button to search the Configuration URL and filename.

Upload : Click the “Upload” button then the switch will start to upload the configuration from the stored location in your PC or Server.

5-5 Diagnostics

This section provides a set of basic system diagnostics. It let users know whether the system is healthy or needs to be fixed. The basic system checks include ICMP Ping, ICMPv6, and VeriPHY Cable Diagnostics.

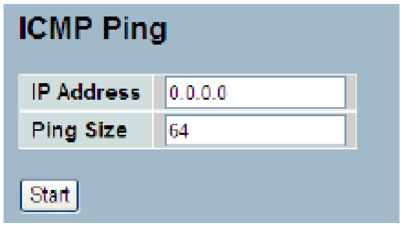
5-5.1 Ping

This page lets you issue ICMP PING packets to troubleshoot IPv6 connectivity issues.

To perform an ICMP PING operation in the web UI:

1. Specify ICMP PING IP Address.
2. Specify ICMP PING Size.
3. Click Start.

Figure 5-5.1: ICMP Ping



ICMP Ping

IP Address	0.0.0.0
Ping Size	64

Parameter descriptions:

IP Address : To set the IP Address of device what you want to ping it.

Ping Size: To set the ICMP Packet size to ping the other device.

Start: Click the "Start" button then the switch will start to ping the device using ICMP packet size that was set on the switch. After you press Start, five ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

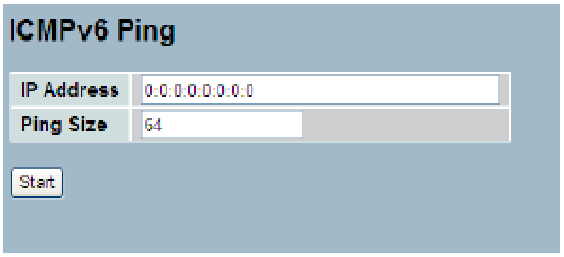
```
PING6 server ::10.10.132.20
64 bytes from ::10.10.132.20: icmp_seq=0, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=1, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=2, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

5-5.2 Ping6

This page lets you issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues. To perform an ICMPv6 PING operation in the web UI:

1. 1.Specify ICMPv6 PING IP Address.
2. 2.Specify ICMPv6 PING Size.
3. 3.Click Start.

Figure 5-5.2: ICMPv6 Ping



ICMPv6 Ping

IP Address	0:0:0:0:0:0:0:0
Ping Size	64

Parameter descriptions:

IP Address : The destination IP Address with IPv6

Ping Size : The payload size of the ICMP packet. Values range from 8 bytes to 1400 bytes.

Start: Click the “Start” button then the switch will start to ping the device using ICMPv6 packet size what set on the switch. After you press Start, 5 ICMPv6 packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

```
PING 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
```

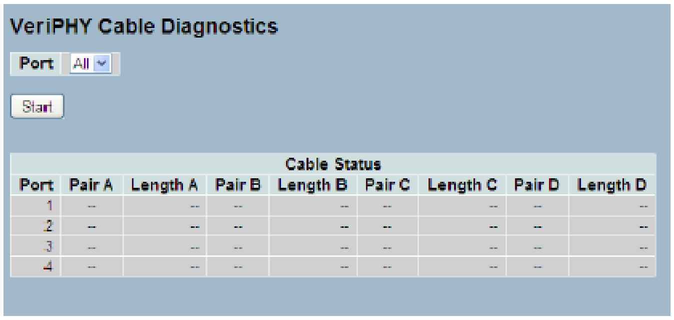
5-5.3 VeriPHY

This page lets you run the VeriPHY Cable Diagnostics. Press “Start” to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of length 7 -140 meters. Note that the 10 and 100 Mbps ports will be linked down while running VeriPHY. So running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

To perform a VeriPHY Cable Diagnostics operation in the web UI:

1. Specify the Port(s) which you want to check.
2. Click Start.

Figure 5-5.3: VeriPHY Cable Diagnostics



VeriPHY Cable Diagnostics

Port: All

Cable Status

Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	--	--	--	--	--	--	--	--
2	--	--	--	--	--	--	--	--
3	--	--	--	--	--	--	--	--
4	--	--	--	--	--	--	--	--

Parameter descriptions:

Port :The port where you are requesting VeriPHY Cable Diagnostics.

Cable Status :

Port: Port number.

Pair: The status of the cable pair.

Length: The length (in meters) of the cable pair.

Lantronix Corporate Headquarters
48 Discovery, Suite 250
Irvine, CA 92618, USA
Toll Free: 800-526-8766
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support
Online: https://www.lantronix.com/technical-support/

Sales Offices
For a current list of our domestic and international sales offices, go to the Lantronix web site at
www.lantronix.com/about/contact.